

Universidad Andina Simón Bolívar
Sede Ecuador

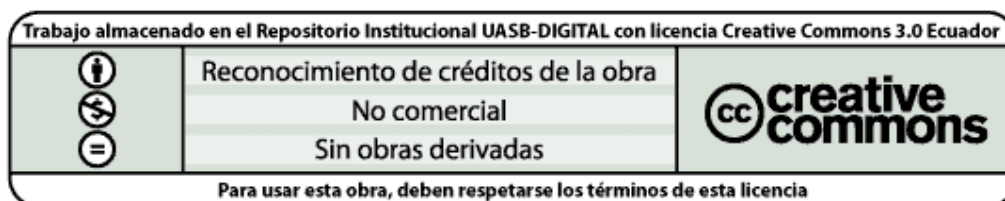
Área de Derecho

Programa de Doctorado en Derecho
Mención en Derecho Económico y de la Empresa

**EL CONTRATO DE PRESTACIÓN DE SERVICIOS
DE CERTIFICACIÓN RECONOCIDA
DE FIRMA ELECTRÓNICA**

Erwin Dotzauer Strampfer

2011



Al presentar esta tesis como uno de los requisitos previos para la obtención del grado de Doctor de la Universidad Andina Simón Bolívar, autorizo al centro de información o a la biblioteca de la universidad para que haga de esta tesis un documento disponible para su lectura según normas de la universidad.

Estoy de acuerdo en que se realice cualquier copia de esta tesis dentro de las regulaciones de la universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial.

Sin perjuicio de ejercer mi derecho de autor, autorizo a la Universidad Andina Simón Bolívar la publicación de esta tesis, o parte de ella, por una sola vez dentro de los treinta meses después de su aprobación.

.....
Erwin Dotzauer Strampfer
29 de junio de 2011

Universidad Andina Simón Bolívar
Sede Ecuador

Área de Derecho

Programa de Doctorado en Derecho
Mención en Derecho Económico y de la Empresa

**EL CONTRATO DE PRESTACIÓN DE SERVICIOS
DE CERTIFICACIÓN RECONOCIDA
DE FIRMA ELECTRÓNICA**

Doctorando:
Erwin Dotzauer Strampfer

Directora:
Prof. Dra. María del Rosario Valpuesta Fernández

Sevilla - España

2011

RESUMEN GENERAL (*Abstract*)

El objetivo primordial de la presente investigación, reside en identificar el régimen jurídico del contrato por el cual se modulan los servicios de certificación reconocida de firma electrónica entre empresarios, es decir, el titular de firma electrónica reconocida (Firmante/Suscriptor) y el prestador de servicios de certificación (PSC), de conformidad con la legislación española y comunitaria europea. A objeto de identificar sus características esenciales, la naturaleza jurídica, el contenido contractual así como la disciplina normativa que resulta aplicable a este negocio jurídico, nuestro estudio ha sido fragmentado en cinco Capítulos.

Iniciamos el *Capítulo Primero* exponiendo las nociones generales así como los antecedentes históricos, técnicos y legislativos que hacen al negocio jurídico objeto de estudio, pasando inmediatamente después a describir la función económica que éste cumple. Luego, en una aproximación preliminar bosquejaremos su definición inicial, diferenciándolo de otros contratos de certificación especiales, para culminar efectuando una descripción de la práctica habitual de la certificación reconocida, delimitando de entrada el contenido del contrato que se ha tomado en cuenta para nuestra investigación.

Posteriormente en el *Capítulo Segundo* concebimos el concepto del contrato que nos ocupa, identificando los caracteres particulares que denota, lo que finalmente nos permitirá establecer su naturaleza jurídica. A poco, nos detendremos en la tarea de identificar el marco legal en que se desenvuelve la certificación reconocida, determinando la normativa que le resulta aplicable y describiendo el modo en que se produce su integración en el contrato.

El *Capítulo Tercero* se ha destinado para el análisis de los elementos subjetivos (*determinando los requisitos de capacidad del PSC, Firmante/Suscriptor y el Usuario verificador del certificado reconocido*), los elementos objetivos (*Certificado reconocido, Datos y Dispositivos, tanto de creación como de verificación de firma electrónica*), para finalmente efectuar las consideraciones pertinentes con relación a los elementos formales del contrato.

Solventadas estas cuestiones en el *Capítulo Cuarto* revisaremos las distintas etapas el *iter* contractual, haciendo notar que las mismas se verifican unas veces en línea (*on line*) y otras fuera de línea (*off line*), desde la fase de formación o preparación del contrato, atravesando por el momento de su perfeccionamiento y desembocando finalmente en el período de ejecución del negocio jurídico, donde nos abocaremos al estudio detallado de su contenido, identificando el conjunto de obligaciones que atingen a cada uno de los sujetos involucrados en la certificación reconocida.

El *Capítulo Quinto* se ha reservado para efectuar un análisis de las hipótesis de responsabilidad civil del PSC derivadas de los servicios de certificación reconocida, identificando su origen (contractual o extracontractual), determinando su naturaleza (objetiva o subjetiva) y detectando los supuestos de limitación y/o exoneración a la responsabilidad del PSC. Para completar nuestro estudio, efectuamos un somero repaso de la responsabilidad civil emergente para el Firmante/Suscriptor.

Finalmente abordaremos las conclusiones generales que se desprenden de nuestra investigación, identificando una posible nueva clasificación del comercio electrónico atendiendo precisamente a la forma de contratación.

“La informática plantea al jurista el desafío de adecuar el cuerpo normativo y doctrinal a la evolución de la tecnología y de nuevas formas de producción y comercialización de bienes y servicios”

Carlos M. Correa

Agradecimientos:

A mi amado hijo Andrick, por todo su amor, infinita paciencia, entendimiento y colaboración a lo largo de estos años de investigación. Gracias por ser mi inspiración. Te amo.

A mis padres Julio, Silvia y mis hermanos, por su permanente e inagotable apoyo a lo largo de la vida.

A Rosario, por hacerme un espacio en medio de sus recargadas labores y tener la deferencia de aceptar dirigir mi trabajo con la paciencia y atención que hace a un comprometido docente universitario.

A José, por haber creído en mí desde un principio y ser el artífice de esta aventura académica apasionante.

A Claudia y Juan Ignacio, profesores y amigos entrañables que acompañaron mis pasos con su invaluable amistad.

A Ingrid, por las valiosas enseñanzas de vida asimiladas a lo largo de estos años, que me ayudaron a crecer y madurar.

Índice de contenido

**EL CONTRATO DE PRESTACIÓN DE SERVICIOS
DE CERTIFICACIÓN RECONOCIDA DE FIRMA ELECTRÓNICA**

Resumen General (<i>Abstract</i>)-.....	004
Agradecimientos.....	006
Índice de contenido.-.....	007
Abreviaturas.-.....	013
Introducción.-.....	015

CAPÍTULO PRIMERO

ORIGEN, JUSTIFICACIÓN ECONÓMICA Y PRÁCTICA COMERCIAL

I. Antecedentes y nociones generales.-.....	029
1.1. La Sociedad de la Información.-.....	029
1.2. El comercio electrónico.-.....	033
1.3. Problemática del comercio electrónico en sentido estricto.-.....	040
1.4. Firmas y certificados electrónicos.-.....	043
II. Delimitación geográfica del ámbito de estudio.-.....	051
2.1. Legislación española de firma electrónica.-.....	052
2.2. Marco jurídico de las firmas y los certificados electrónicos.-.....	054
2.3. Marco jurídico de los servicios de certificación.-.....	054
III. Circunscripción del objeto de estudio.-.....	056
IV. Función económica.-.....	059
V. Práctica comercial.-.....	068
5.1. Aproximación al concepto y definición inicial.-.....	068
5.2. Diferenciación de otros contratos de certificación.-.....	070
a) El contrato de certificación de sitios web.-.....	071
b) El contrato de firma de códigos.-.....	072
c) El contrato de visados electrónicos.-.....	072
5.3. Clasificación de la certificación electrónica.-.....	073
5.3.1. Por el destinatario de los servicios.-.....	073
a) Contratos de certificación con consumidores.-.....	073
b) Contratos de certificación con empresarios.-.....	074
5.3.2. Por la categoría de firma electrónica que contiene el certificado.-.....	074
a) Certificados de firmas electrónicas simples.-.....	075
b) Certificados de firmas electrónicas avanzadas.-.....	075
c) Certificados de firmas electrónicas reconocidas.-.....	075
5.3.3. Por la naturaleza del PSC que emite el certificado.-.....	075
a) Persona física o jurídica.-.....	076
b) Persona de derecho público o privado.-.....	076
c) PSC certificado o no certificado técnicamente.-.....	077
5.3.4. Por el ámbito territorial en que se presta el servicio.-.....	078
a) Nacional.-.....	078
b) Intracomunitario.-.....	078
c) Internacional.-.....	079
VI. Descripción general del contenido contractual.-.....	079
6.1. Descripción de las prestaciones propias del PSC.-.....	079
6.1.1. Obligación preliminar.-.....	079

6.1.2. Obligaciones principales.-	080
6.1.3. Obligaciones específicas para emitir certificados reconocidos.-	080
6.1.3.1. Previas a la emisión del certificado reconocido.-	080
6.1.3.2. A tiempo de emitir el certificado reconocido.-	081
6.1.4. Obligaciones adicionales.-	082
6.1.5. Obligaciones accesorias.-	083
6.2. Descripción de las obligaciones propias del Firmante/Suscriptor.-	084
6.2.1. Obligación principal.-	084
6.2.2. Obligaciones adicionales.-	084
VII. Sinopsis.-	086

CAPÍTULO SEGUNDO

CONCEPTO, CARACTERES Y NATURALEZA JURÍDICA

I. Concepto.-	088
II. Caracterización.-	093
2.1. Consensual.-	093
2.2. Mercantil.-	095
2.3. Bilateral sinalagmático.-	097
2.4. Oneroso - conmutativo.-	099
2.5. Relación obligatoria duradera de tracto continuo.-	100
2.6. Sujeto a condiciones generales, perfeccionado por adhesión.-	102
2.6.1. Concepto de adhesión.-	103
2.6.2. Concepto de Condiciones Generales de la Contratación.-	105
2.6.2.1. Régimen jurídico de las CGC en el Ordenamiento español.-	108
a) Validez de las CGC.-	111
b) Nulidad de las CGC.-	111
c) Sujetos de la contratación con CGC.-	112
d) Cláusulas abusivas.-	113
2.6.2.2. Régimen especial de interpretación de las CGC.-	115
2.6.3. Fundamento de la obligatoriedad de las CGC.-	116
2.6.4. La incorporación de las CGC al documento contractual.-	117
2.6.5. Las CGC en el contrato de certificación reconocida.-	118
2.7. Contrato obligatorio.-	119
2.8. No es <i>intuitu personae</i> .-	120
2.9. Sinopsis.-	120
III. Naturaleza jurídica.-	121
3.1.- Calificación del contrato.-	121
3.1.1.- La certificación reconocida en la órbita del contrato de mandato.-	129
3.1.2.- La certificación reconocida en la órbita del contrato de obra.-	134
3.1.3.- La certificación reconocida en la órbita del contrato de servicios.-	140
3.1.4.- La certificación reconocida como contrato que comprende la ejecución de una obra previa y la prestación de un servicio ulterior.-	151
3.1.5.- La certificación reconocida como contrato de actividad.-	153
3.1.6.- Inserción de la certificación reconocida en la genérica categoría del “ <i>contrato de servicios</i> ”.-	156
3.1.6.1.- Los servicios según los “ <i>Principios de Derecho Europeo</i> <i>Contratos de Servicios</i> ” en la elaboración del MCR.-	158
3.2.- El contrato de certificación reconocida como contrato atípico.-	160
IV. Marco jurídico.-	167
4.1.- Legislación aplicable.-	167
4.1.1.- Normativa española.-	167

4.1.2.- Normativa comunitaria europea.-	168
4.2.- Integración del contrato.-	169
4.2.1. La autorregulación del PSC en el contrato de certificación reconocida.-	171
a) Regulación sectorial.-	172
a.1.) Marcas basadas en normas o especificaciones.-	172
a.2.) Marcas basadas en códigos de conducta o guías.-	172
b) Regulación individual.-	173
b.1.) Contenido de la DPC y las PC.-	177
V.- Sinopsis.-	185

CAPÍTULO TERCERO ELEMENTOS DEL CONTRATO

I. Nociones previas.-	189
II. Elementos personales o subjetivos.-	192
2.1. El Prestador de Servicios de Certificación (PSC).-	192
2.1.1. Importancia de la cláusula de Mercado Interior.-	195
2.1.2. Incidencia de la “ <i>Directiva Servicios o Bolkestein</i> ”.-	199
2.1.3. Incidencia de la Ley 17/2009, de 23 de noviembre (LASE).-	205
2.2. Las Entidades de Registro (ER).-	207
2.3. El Firmante/Suscriptor y titular del certificado reconocido.-	209
2.4. El Usuario del certificado reconocido.-	215
III. La capacidad de las partes.-	217
3.1. La capacidad general de obrar.-	217
3.2. Capacidad del Prestador de Servicios de Certificación (PSC).-	218
a) Cuando es empresario mercantil individual.-	218
b) Cuando es empresario mercantil colectivo.-	219
3.3. Capacidad del Firmante/Suscriptor.-	221
a) Cuando es empresario mercantil individual.-	221
b) Cuando es empresario mercantil colectivo.-	221
IV. Elementos objetivos.-	221
4.1. El certificado reconocido.-	221
4.2. Datos y Dispositivos de creación de firma electrónica.-	225
4.2.1. Los datos de creación de firma.-	225
4.2.2. El dispositivo seguro de creación de firma.-	226
4.3. Datos y Dispositivos de verificación de firma electrónica.-	227
4.3.1. Los datos de verificación de firma.-	227
4.3.2. El dispositivo de verificación de firma.-	228
4.4. El dispositivo de generación de datos de creación de firma (de claves).-	228
V. Elementos formales.-	228

CAPÍTULO CUARTO FORMACIÓN, PERFECCIONAMIENTO Y CONTENIDO CONTRACTUAL

I. Discernimiento inicial.-	233
II. Formación del contrato.-	234
2.1. Procedimiento de solicitud del Certificado.-	237

2.1.1. (Etapa I) Obtención de información.-	238
2.1.2. (Etapa II) Obtención de elementos tecnológicos.-	238
2.1.3. (Etapa III) Presolicitud del certificado.-	240
2.2. Deberes de conducta en la preparación contractual.-	241
2.2.1. Principio-deber de buena fe.-	241
2.2.2. Deber de información sobre el contenido del contrato.-	247
2.2.3. Contenido de la información.-	249
i) Información sobre clausulados predisuestos y Prácticas de certificación.-	250
ii) Medidas de seguridad.-	250
iii) Método empleado para comprobar la identidad.-	251
iv) Condiciones y límites de empleo del certificado.-	252
v) Garantías.-	253
vi) Certificaciones obtenidas.-	253
vii) Procedimientos para resolución extrajudicial de conflictos.-	253
viii) Información sobre precios.-	254
ix) Otras informaciones.-	257
2.2.4. Oferta vinculante.-	259
2.2.5. Deberes de información y conducta del Solicitante.-	264
2.2.6. Responsabilidad pre-contractual.-	265
III. Perfeccionamiento y ejecución del contrato.-	266
3.1. (Etapa IV) Adhesión a cláusulas generales y Registro.-	266
3.2. (Etapa V) Envío de información al PSC.-	267
3.3. (Etapa VI) Emisión del certificado.-	267
3.4. (Etapa VII) Composición del nombre distintivo (DN) del Firmante/Suscriptor.-	267
3.5. (Etapa VIII) Publicación del certificado.-	268
3.6. (Etapa IX) Descarga e instalación del certificado.-	268
3.7. (Etapa X) Aceptación o rechazo del certificado.-	269
3.8. (Etapa XI) Empleo del certificado.-	269
3.9. (Etapa XII) Comprobación del estado del certificado.-	269
3.10. Ciclo vital del certificado.-	269
IV. Contenido del contrato de certificación reconocida.-	271
4.1. Parámetro de la obligación y diligencia profesional.-	272
4.2. Obligaciones del PSC.-	276
4.2.1. Obligaciones principales.-	276
i) Emisión y entrega del certificado reconocido.-	276
ii) Mantener un directorio y garantizar servicio de consulta de certificados.-	278
ii.1.) Generación y publicación de las Listas de Revocación de Certificados (LRC).-	278
ii.2.) Servicio de consulta y validación de Certificados mediante OCSP.-	279
4.2.2. Obligaciones específicas.-	283
4.2.2.1. Previas a la emisión del certificado reconocido.-	283
i) Comprobación de identidad de los solicitantes.-	283
ii) Asegurar exactitud de la información.-	288
iii) Cerciorarse la efectiva posesión del Firmante/Suscriptor del par de claves.-	289
iv) Garantizar complementariedad del juego de claves.-	290
4.2.2.2. A tiempo de emitir el certificado reconocido.-	290
i) Constituir un seguro.-	290
ii) Demostrar fiabilidad técnica.-	291
iii) Garantizar precisión temporal.-	292
iv) Emplear personal cualificado.-	295
v) Emplear procedimientos adecuados.-	296
vi) Utilizar recursos fiables.-	296
vii) Prevenir falsificaciones.-	297
viii) Asegurar confidencialidad de la clave privada.-	297
ix) Conservar información.-	298
x) Almacenar certificados de modo seguro.-	299

4.2.3. Obligaciones adicionales.-.....	300
i) Actuar de buena fe.-.....	301
ii) Administrar el ciclo vital del certificado reconocido.-.....	301
iii) Proporcionar información actualizada (DPC).-.....	304
iv) Protección de datos personales.-.....	304
v) No almacenar ni copiar los datos de creación de firma del Firmante/Suscriptor.-.....	306
vi) Comunicación del cese de actividades.-.....	308
4.2.4. Obligaciones accesorias.-.....	309
i) Provisión del dispositivo criptográfico y el software correspondiente.-.....	310
ii) Servicio de acuse de recibo.-.....	311
iii) Servicio de homologación de certificados.-.....	312
4.2.5. Obligaciones de la Entidad de Registro (ER).-.....	313
4.3. Obligaciones del Firmante/Suscriptor.-.....	315
4.3.1. Obligación principal.-.....	315
i) Pago del precio como contraprestación por el servicio.-.....	315
4.3.2. Obligaciones accesorias.-.....	319
i) Actuar de Buena fe.-.....	319
ii) Conservar diligentemente su clave privada.-.....	319
iii) Comunicar la puesta en peligro o pérdida de su clave privada.-.....	320
iv) Respetar las condiciones de empleo del certificado conforme la DPC.-.....	321
v) Respetar los límites de uso del certificado.-.....	322
vi) Respetar los límites de los importes que figuran en el certificado.-.....	323
vii) Comunicar los cambios de la información reflejada en el certificado.-.....	323
viii) Solicitar la suspensión o revocación del certificado oportunamente.-.....	324
ix) No utilizar la clave privada en caso de suspensión o extinción del certificado.-.....	325
V. Contexto de las obligaciones del Usuario.-.....	326
5.1. Obligaciones del Usuario previstas en la LFE.-.....	328
i) Observar y cumplir las disposiciones de la LFE.-.....	328
ii) Actuar de manera diligente.-.....	328
ii.1.) Comprobar la suspensión o extinción del certificado.-.....	329
ii.2.) Tener en cuenta los límites de uso del certificado.-.....	330
ii.3.) Tener en cuenta los límites de los importes del certificado.-.....	331
iii) Conocer y sujetarse a la DPC y las PC.-.....	333
5.2. Factibilidad de la contractualización de las obligaciones del Usuario.-.....	333
5.3. Criterios adversos a la contractualización.-.....	339
5.4. Conclusiones.-.....	341

CAPÍTULO QUINTO **RESPONSABILIDAD**

I. Consideraciones preliminares.....	343
II. Precisión terminológica, nociones básicas y aproximación al C.c. español.-.....	348
III. Régimen jurídico de la responsabilidad civil del PSC en la LFE.-.....	351
3.1. Supuestos de responsabilidad.-.....	355
a) Supuesto general de responsabilidad.-.....	355
b) Supuestos específicos de responsabilidad.-.....	356
3.2. Naturaleza de la responsabilidad: objetiva o subjetiva y carga de la prueba.-.....	356
3.3. Origen de la responsabilidad: contractual o extra-contractual.-.....	360
3.3.1. Responsabilidad frente al Firmante/Suscriptor.-.....	361
3.3.2. Responsabilidad frente al Usuario del certificado.-.....	363
3.3.3. Responsabilidad y resolución contractual.-.....	363

3.3.4. Responsabilidad frente a terceros <i>strictu sensu</i> .-.....	369
3.4. Cláusulas limitativas de responsabilidad contractual.-.....	370
3.5. Exoneración de responsabilidad.-.....	370
IV. Hipótesis de responsabilidad civil derivadas de los servicios de certificación reconocida.-.....	371
4.1. Hipótesis de responsabilidad previas o consustanciales a la emisión del certificado.-.....	372
4.1.1. Responsabilidad por generación del juego de claves.-.....	373
4.1.2. Responsabilidad por ausencia de emisión del certificado.-.....	374
4.2. Hipótesis de responsabilidad derivadas de la certificación.-.....	374
4.2.1. Responsabilidad por la inexactitud de los datos del certificado.-.....	375
a) Por circunstancias previas a la emisión del certificado.-.....	375
b) Por circunstancias posteriores a la emisión del certificado.-.....	379
4.2.2. Responsabilidad por la vulnerabilidad del directorio de certificados.....	382
4.2.3. Responsabilidad derivada de los servicios de extinción (revocación) y/o suspensión de los certificados.-.....	385
i) Primera fase.-.....	387
ii) Segunda fase.-.....	388
iii) Tercera fase.-.....	390
iv) Cuarta fase.-.....	391
4.2.3.1. Necesidad de un servicio de sellado temporal.-.....	392
4.2.4. Responsabilidad en caso de extinción (revocación) o suspensión de los certificados por causas atribuibles al PSC.-.....	394
a) Cese voluntario de las actividades del PSC.-.....	395
b) Cancelación las certificaciones técnicas obtenidas.-.....	396
c) Por causas técnicas.-.....	397
4.3. Hipótesis de responsabilidad derivadas del servicio de homologación.-.....	398
4.4. Hipótesis de responsabilidad por actuaciones de los auxiliares del PSC.-.....	400
V. Limitaciones a la responsabilidad del PSC contempladas en la LFE.-.....	402
5.1. Limitaciones intrínsecas al certificado.-.....	404
5.1.1. Limitaciones intrínsecas de carácter cualitativo.-.....	404
5.1.2. Limitaciones intrínsecas de carácter cuantitativo.-.....	404
5.1.3. Inobservancia a las condiciones de uso del certificado.-.....	405
5.2. Limitaciones extrínsecas al certificado.-.....	406
5.2.1. Provenientes de la actuación del Firmante/Suscriptor.-.....	406
5.2.2. Provenientes de la actuación del Usuario del certificado.-.....	407
5.2.3. Provenientes de la actuación del PSC.-.....	408
VI. Responsabilidad civil emergente para el Firmante/Suscriptor.-.....	409
6.1. Naturaleza de la responsabilidad: objetiva o subjetiva.-.....	410
6.2. Sujetos frente a los que responde el Firmante/Suscriptor.-.....	411
6.3. Origen de la responsabilidad: contractual o extra contractual.-.....	413
Conclusiones.-.....	415
Bibliografía.-.....	428
ANEXOS.-	
- Ley 59/2003, de 19 de diciembre, de firma electrónica.-.....	446
- 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.-.....	471
- Ley Modelo de la CNUDMI sobre las Firmas Electrónicas (2001).-.....	482

Abreviaturas

ABA	American Bar Association.
art.	Artículo
C.c.	Código Civil.
C.com.	Código de Comercio.
CE	Comercio electrónico.
CEC	Código Europeo de Contratos.
CGC	Condiciones Generales de la Contratación.
CNUDMI	Comisión de Naciones Unidas para el Derecho Mercantil Internacional.
C.p.	Código Penal.
CVCIM	Convención de Viena sobre Compraventa Internacional de Mercaderías (1980).
DCE	Directiva 2000/31/CE de 8 de junio, sobre Comercio Electrónico.
DFE	Directiva 1999/93/CE de 13 de diciembre, sobre Firma Electrónica.
DSMI	Directiva 2006/123/CE de 12 de diciembre, relativa a los servicios en el mercado interior.
DPC	Declaración de Prácticas y Políticas de Certificación.
EC	Entidades de Certificación.
EDI	Electronic Data Interchange.
EEE	Espacio Económico Europeo.
EF	Entidad Final.
EFD	Entidades de Fechado digital.
ER	Entidad de Registro.
ETSI	European Telecommunications Standards Institute.
FNMT-RCM	Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda.
ICP	Infraestructura de Clave Pública.
ins.	Inciso.
LASE	Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio.
LCGC	Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación (España).
LFE	Ley 59/2003, de 19 de diciembre, de firma electrónica (España).
LGDCU	Ley 26/1984, de 19 de julio, general para la defensa de los consumidores y usuarios (España).
LMISI	Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (España).
LMCE	Ley Modelo de la CNUDMI sobre Comercio Electrónico.
LMFE	Ley Modelo de la CNUDMI sobre Firma Electrónica.
LPDCP	Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (España).
LRC	Lista de Revocación de Certificados.
LSSI	Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (España).
NTIC	Nuevas Tecnologías de Información y las Comunicaciones.
OCDE	Organización de Cooperación y Desarrollo Económico.
OMC	Organización Mundial del Comercio.
PC	Políticas de Certificación.
PECL	Principles of European Contract Law / Principios del Derecho Europeo de los Contratos.
PEL-SC	Principles of European Law. Service Contracts / Principios de Derecho Europeo. Contratos de Servicios.
pfo.	Párrafo.
PSC	Prestador de Servicios de Certificación.
PUNIDROIT	Principios UNIDROIT sobre contratos comerciales internacionales.
RDL	Real Decreto-ley 14/1999, de 17 de septiembre, sobre firma electrónica (España).

RRM	Reglamento del Registro Mercantil.
s.	Siglo.
SSI	Servicios de la Sociedad de la Información.
SI	Sociedad de la Información.
SICC	Sociedad de la Información, Comunicación y el Conocimiento.
TCE	Tratado Constitutivo de la Comunidad Europea.
TIC	Tecnologías de Información y las Comunicaciones.
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 (España).
UNIDROIT	Instituto Internacional para la Unificación del Derecho Privado.
UE	Unión Europea.
UIT	Unión Internacional de Telecomunicaciones.
v.gr.	Verbigracia.

INTRODUCCIÓN

La mayoría de los investigadores sociales coinciden en señalar, que la evolución histórica de la sociedad humana se modula sobre la base de las tecnologías empleadas para producir y así satisfacer sus necesidades. Las distintas técnicas inventadas e incorporadas produjeron cambios no sólo en las tecnologías empleadas en sí mismas, sino que paralelamente aparejaron una serie de transformaciones sociales en todos los ámbitos.

De modo que la sociedad habría transitado - o debería hacerlo teóricamente - por tres grandes etapas, idea que constituye la base de autores como Daniel Bell, Peter Drucker, Marshall McLuhan, Manuel Castells y particularmente Alvin Toffler, quien en su libro “La Tercera Ola” (The Third Wave, 1980), apunta que en el desarrollo evolutivo de la sociedad humana se identifican tres grandes momentos históricos, u olas como las denomina el autor, las cuales corresponderían a la era agraria o *Sociedad Preindustrial*, que engendra la aparición de la *Sociedad Industrial*, en la que en determinado momento la producción de bienes cede en importancia a la prestación de servicios, surgiendo por consiguiente la *Sociedad Post-industrial*.

En esta última predomina el sector terciario de producción, se caracteriza por el desarrollo de la cibernética y un alto grado de automatización, lo que repercute en la economía, en la cual como se tiene dicho, el sector primario y el secundario son sustituidos por el terciario, es decir, por los servicios.

Cuando se logra la automatización de los servicios respecto de un bien inmaterial e ilimitado el sistema económico vuelve a reorganizarse y, por ende, el modelo social sufre otra profunda transformación: es el inicio de la *Sociedad de la Información* (SI) la cual apunta finalmente hacia la consolidación de la *Sociedad del Conocimiento*, en la cual el saber y el conocimiento son determinantes como “valor añadido”, en la nueva economía.

Evidentemente la evolución de los adelantos científicos especialmente a partir de la segunda mitad del s. XX, posibilitó particularmente en el ámbito de las comunicaciones el surgimiento de nuevas tecnologías, las que han venido a denominarse por la generalidad de los autores y uniformemente reconocidas por la doctrina como: Nuevas Tecnologías de Información y Comunicaciones (NTIC), las que junto con las no tan nuevas tecnologías se integran bajo la concepción generalizadora de TIC.

En ese sentido, el desarrollo de la Ciencia informática gracias al aporte de la cibernética y de la Teoría General de los Sistemas, posibilitó el surgimiento precisamente de una de esas nuevas tecnologías a las que hacemos referencia, nos referimos a “Internet”, la cual desde su difusión al público en 1983 y su apertura comercial en 1994, no ha parado de crecer y desarrollarse a pasos agigantados en una especie de ebullición permanente.

De tal modo que en el “*Ciberespacio*”, la materia prima que transita por estas tecnologías y sirve para trabajar sobre ella misma es la información - que puede devenir en conocimiento - constituyendo el “nuevo capital” que transforma los procesos de producción material e inmaterial de acumulación de las riquezas.

Autores como Antonio E. Pérez Luño indican que la evolución tecnológica ha supuesto para la economía una auténtica “*segunda revolución industrial*”, en la que los sectores primario (agropecuario) y secundario (industrial) así como el sector terciario (servicios), están dejando paso al creciente protagonismo del *sector cuaternario* constituido por la información, de modo que la creación y tratamiento automatizado de la información ha pasado a ser el recurso económico básico de la sociedad Post-industrial.

La revolución tecnológica posibilita la aparición de una nueva economía basada en la red de inteligencia humana. El canadiense Donald Tapscott ya puso de manifiesto que “*En una economía digital, individuos y empresas crean riqueza aplicando conocimiento, inteligencia humana en red y esfuerzos en las áreas de producción, agricultura y servicios.*”

En la frontera digital de esa economía, los participantes, la dinámica, las reglas y las exigencias de supervivencia y éxito están cambiando todo.”¹

En el caso del análisis de Internet, la cual constituye una de las tecnologías principales de la novedosa SI, los distintos autores afirman que genera fundamentalmente un nuevo y gran mercado donde podría materializarse, al fin, un espacio de imperio del libre comercio.

Lester Thurow en su libro *Construir Riqueza*, postula que por primera vez en la historia es posible una economía global donde el conocimiento es la nueva base de riqueza, la información es uno de los nuevos insumos utilizados para construir una economía diferente, poblada de productos y servicios muy distintos.

De manera que la diferencia con la sociedad post-industrial radica, no sólo en que la prestación de servicios crece mucho en relación a la producción de bienes, sino que se trata en definitiva, de bienes y servicios vinculados a la información.

Resulta evidente que la actual economía presenta un perfil nuevo, lo que ahora caracteriza al movimiento comercial es el acceso a una amplia gama de servicios a través de las extensas redes comerciales que se desarrollan en el ciberespacio, encaminándose a convertirse en uno de los hiper-sectores de la nueva estructura económica.

Por consiguiente, debemos observar que nos encontramos en medio de una transición económica que implica el cambio de la economía industrial a la electrónica. El comercio electrónico esta creando un consumidor con mayores poderes de decisión, tomando en cuenta las ofertas que recibe y la manera en que los productos llegan hasta él.

La Sociedad de la Información y el Derecho.-

Como se tiene dicho, el desarrollo acelerado de tecnologías ha introducido cambios en costumbres y hábitos en el entorno privado y público del hombre de fines del siglo XX. La economía, las relaciones humanas, la cultura, la política y las ciencias sociales, todas se ven

¹ Donald Tapscott, *Economía Digital. Promessa e Perigo na era da inteligencia em rede*, Sao Paulo, Makron Books do Brasil Editoria Limitada, 1997, p. 54 y ss.

influenciadas por las TIC, el gran motor de cambio de nuestra sociedad. Esta circunstancia obliga al legislador a adaptar el ordenamiento jurídico a la nueva realidad que origina la introducción de los avances tecnológicos en la vida cotidiana del ciudadano común, la cual no está exenta de incertidumbres en el mundo de la Ciencia Jurídica.

En ese entendido, la ciencia del Derecho no puede permanecer ajena al cambio tecnológico, ésta debe ser capaz de crear mecanismos necesarios para regular adecuadamente las actuales relaciones surgidas del empleo de las TIC; en consecuencia el legislador se halla comprometido a una observación correcta de los inéditos fenómenos surgidos por este uso, a objeto que sean reconocidos y normados mediante una legislación oportuna, efectiva, clara y útil.

Precisamente el impresionante desarrollo de la tecnología y la democratización de los medios han obligado a las comunicaciones a utilizar mecanismos cada vez más rigurosos en términos de seguridad y eficiencia. En el contexto de las actividades comerciales, las firmas y los certificados electrónicos - junto a los demás servicios conexos de autenticación de datos - se han convertido en un recurso imprescindible para las actuales contrataciones y transacciones electrónicas mercantiles.

Por ende la firma electrónica es utilizada en infinidad de escenarios y circunstancias con diferentes propósitos y beneficios, dando lugar a una gran variedad de servicios accesorios.

El paradigma del documento escrito con firmas manuscritas está siendo relegado por el uso del documento digital con o sin firma electrónica sobre el mensaje. El Derecho debe brindar las respuestas adecuadas para facilitar la transición del medio físico al mundo virtual, a fin que todos los actos jurídicos que tengan lugar en el mundo virtual posean idénticas consecuencias en el mundo físico, y que además, cualquier relación jurídica que se desplace entre ambos espacios goce de idénticos efectos legales.

Si bien Internet se ha desarrollado con sus propios códigos y normas técnicas de conducta (lo cual brinda un apreciable nivel de seguridad desde el punto de vista tecnológico) teniendo en algunos aspectos el reconocimiento del Derecho tradicional, no se puede dejar de reconocer que la legislación tiene que proporcionar en el mundo virtual la debida seguridad jurídica a los distintos agentes económicos (empresarios, clientes, usuarios, terceras partes, etc.), para que puedan realizar sus operaciones comerciales en un marco de certeza, no solo técnica sino también y fundamentalmente legal, de manera que cada uno de los actores en la SI posea un régimen jurídico claro y eficaz, en cuanto a sus derechos, obligaciones, garantías y responsabilidades.

Para el desarrollo de los Servicios de la Sociedad de la Información (SSI) y particularmente el comercio electrónico, es imprescindible la creación de instrumentos jurídicos que permitan a los consumidores y a las empresas intercambiar información, contratar y comerciar electrónicamente de una forma segura.

Para satisfacer estas necesidades, en el ámbito normativo podemos destacar la Ley Modelo sobre Comercio electrónico de la CNUDMI, la cual inspiró a varios legisladores a nivel mundial para abordar la temática. Así por ejemplo, a nivel del derecho comunitario europeo contamos con la Directiva sobre Comercio Electrónico (DCE) y, en el ámbito nacional español, la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI).

Dentro este contexto conforme sostiene la Directiva de Firma Electrónica (DFE), el estímulo de la prestación de servicios de certificación de firma electrónica en competencia a través de entornos abiertos de comunicación (v.gr. Internet) resulta prioritario. Para que los medios de certificación electrónica sean verdaderamente efectivos y produzcan los efectos deseados sobre la seguridad del tráfico electrónico, es esencial que se les provea del reconocimiento adecuado por el ordenamiento jurídico.

En cuanto a la legislación que hace a las firmas electrónicas, debemos destacar que a partir de la Ley sobre firma digital del Estado de Utah (1995), se desató en el concierto internacional una verdadera carrera por sancionar leyes sobre firma electrónica. Para nuestro estudio resultan relevantes además de la DFE antes mencionada; la Ley Modelo sobre firmas electrónicas de la CNUDMI y la Ley 59/2003, de 19 de diciembre, de firma electrónica (LFE) española.

En el escenario descrito y al amparo de la legislación sobre firma electrónica, han surgido los Prestadores de Servicios de Certificación de firma electrónica (PSC), cuya finalidad no se limita a la emisión y gestión de certificados de identificación, sino que incluyen también una serie de diversos servicios relacionados a la firma electrónica, como por ejemplo: homologación de certificados; certificación de sitios web; firma de códigos; visados electrónicos; servicios de directorio y verificación de certificados; registro de firmantes; suspensión, revocación y extinción de certificados, así como guías de usuarios y asesoría en general.

La persona física o jurídica que desee ser titular de una firma electrónica (el Firmante/Suscriptor) para autenticar su identidad en redes abiertas de comunicación, a objeto de llevar a cabo transacciones seguras de comercio electrónico en sentido estricto con sus potenciales clientes (los Usuarios del certificado), dotándoles el mismo valor jurídico-probatorio que la ley otorga a los documentos y firmas tradicionales, requiere contar previamente con un certificado reconocido emitido por un PSC legalmente constituido. La certificación reconocida constituye por consiguiente el sustentáculo de un específico servicio de la Sociedad de la Información.

Por la importancia que reviste la materia, desde la aparición misma de las primeras legislaciones sobre comercio y firmas electrónicas en el mundo, los estudiosos del Derecho se han abocado al análisis de la temática, lo que dado lugar al surgimiento de una cuantiosa y

hoy en día prácticamente inagotable bibliografía, en la que se procura explicar a la par de los componentes que hacen al funcionamiento tecnológico de estos novedosos instrumentos, los aspectos jurídicos respecto de la eficacia de los documentos, las firmas y los certificados electrónicos, describiendo el conjunto de actividades que ocupan al PSC a momento de acometer su labor certificadora, así también, respecto de las conductas que deben observar a su turno el Firmante/Suscriptor y el Usuario verificador de certificados electrónicos, pero limitándose a señalar que la prestación de dichos servicios se formaliza mediante un contrato celebrado entre el PSC y el Firmante/Suscriptor, sin que existan mayores referencias que profundicen el análisis del negocio jurídico en concreto.

En otras palabras, la mayor parte de la literatura especializada - salvo un par de honrosas excepciones de coetánea publicación a momento de efectuar la presente tesis - se limita en anunciar la existencia de esta relación contractual, pero no profundiza sobre el estudio del contrato en sí mismo, con lo cual, sobrevienen una serie de dudas y cuestionamientos, por ejemplo con relación sus características particulares, la naturaleza jurídica o el contenido de este contrato, entre otros aspectos. Asimismo, deviene la interrogante respecto a la posición jurídica que ocupa el Usuario verificador del certificado, quien en principio ocupa la posición de verdadero tercero ajeno al contrato celebrado entre el PSC y el Firmante.

Estas carencias son igualmente sentidas en el ámbito jurisdiccional, toda vez que la jurisprudencia con relación a este contrato es prácticamente inexistente, dada la inclusión en tales contratos de cláusulas arbitrales así como la acusada tendencia a resolver los conflictos entre las partes por medio de la transacción.

Los mencionados vacíos son precisamente los que nos han motivado a desarrollar la presente investigación. El reto justamente ha consistido en desentrañar el régimen jurídico que hace al referido contrato, considerando que, no obstante que la LFE explicita algunas

obligaciones del PSC, regula su responsabilidad fijando los límites a la misma, y de esta última se infieren ciertas obligaciones del Firmante-Suscriptor y el Usuario del certificado, podemos afirmar que no existe un tratamiento legal acabado del negocio objeto de estudio.

Por las razones expuestas nuestra investigación se centra en el análisis del contrato, mismo que habitualmente se viene nominando en el tráfico como “*Contrato de certificación reconocida*”. Para cumplir nuestro cometido se ha delimitado el objeto de estudio del modo siguiente: nuestra investigación se circunscribe fundamentalmente al derecho de obligaciones y contratos, partiendo del supuesto en que ambas partes contractuales revisten la condición de empresarios. Asimismo, desde el punto de vista geográfico nos abocaremos al ámbito de la legislación española y comunitaria europea, por considerar que al presente se configura en la normativa con mayor desarrollo; desde el punto de vista tecnológico nos concentraremos en Infraestructura de Clave Pública (ICP), ya que hoy en día constituye la tecnología más difundida en el mercado de la certificación.

Procuramos aportar soluciones a los diversos conflictos que pueden suscitarse, desde el momento de formación hasta la etapa de ejecución del contrato, que podemos definir atendiendo a su contenido esencial, como aquel en virtud del cual una de las partes contratantes, el PSC, se obliga a emitir y poner a disposición un certificado reconocido a favor de su cliente, el Firmante/Suscriptor, estando obligado el PSC además a publicar el certificado manteniendo un directorio actualizado que refleje su estado (vigente, suspendido o extinguido), garantizando un servicio de consulta y/o verificación pública del mismo; en tanto que la contraparte contractual, el Firmante/Suscriptor, se obliga a pagar un precio como contraprestación por el servicio recibido.

La modalidad de investigación es de tipo teórica o documental, toda vez que permite definir, sistematizar y evaluar nuestro objeto de estudio conforme el criterio principal de la coherencia. La metodología implementada combina adecuadamente los métodos deductivo,

jurídico-dogmático o constructivo, analógico, comparativo, analítico-sintético, interpretativo y descriptivo.

Asimismo se aplicaron técnicas de investigación bibliográfica y documental, las cuales comprendieron la revisión de la doctrina, jurisprudencia, la legislación española y la legislación comparada (particularmente la proveniente de la Unión Europea y Organismos Internacionales: OMC, CNUDMI, OCDE, etc.) y tuvo por objeto profundizar el análisis de los principios y régimen jurídico aplicable al comercio y firmas electrónicas así como a la prestación de servicios de la Sociedad de la Información, cuyas normas fueron debidamente interpretadas y sistematizadas.

De igual modo, la investigación demandó la elaboración de resúmenes, fichas y ficheros, toma de notas y la organización de la información en carpetas adecuadamente ordenadas por temática y capítulos en el ordenador. Finalmente inferimos nuestras conclusiones, que se encuentran respaldadas y sustentadas conforme el *método jurídico-dogmático*, a fin de garantizar la credibilidad, seriedad así como utilidad de nuestra investigación.

En cuanto a la distribución del trabajo, para su mejor asimilación ha sido parcelado en cinco Capítulos conforme se pasa a explicar a continuación.

En el *Capítulo Primero* efectuaremos una somera descripción de los antecedentes y nociones generales que hacen a la presente investigación, procediendo luego a efectuar las correspondientes demarcaciones de nuestro objeto de estudio.

Así, nos detendremos en el discernimiento del objeto y contenido general de la legislación española sobre firma electrónica (LFE). Se resaltarán los aspectos más destacados de la referida normativa, haciendo notar que sus disposiciones se aplican: i) en comunidades que han celebrado acuerdos previos para el empleo de firmas electrónicas o sin ellos; ii) sea que se trate de entornos cerrados o abiertos de comunicación; iii) tanto a las actividades de

comercio electrónico en sentido amplio como en sentido estricto. Finalmente, se describe el marco jurídico en el que se desenvuelven tanto las firmas y certificados electrónicos, como los servicios de certificación, conforme se encuentra previsto en la LFE.

A continuación se establece la función económica del contrato, que consiste en la identificación en - sentido amplio - de los operadores económicos en el tráfico virtual, como requisito imprescindible para generar un entorno seguro, de manera que tanto los consumidores como las empresas puedan tener confianza en que sus transacciones no serán interceptadas, ni modificadas y se tenga la certeza que tanto el comprador y vendedor (emisor y receptor de un mensaje de datos) son efectivamente quienes dicen ser.

Posteriormente se destacarán los elementos que hacen a la práctica comercial del contrato de certificación reconocida, proporcionando inicialmente una aproximación al concepto para luego efectuar su diferenciación de otros contratos de certificación especiales.

De ese modo es que se efectúa una descripción del supuesto contractual desde un punto de vista práctico, a tal fin partimos de un principio de definición de carácter descriptivo que nos permitirá identificar los supuestos de esta realidad contractual, diferenciando al efecto diversas modalidades de certificación reconocida en función de los destinatarios a los que va dirigida habitualmente.

Acto seguido se describe que los servicios de certificación electrónica se pueden clasificar atendiendo ya sea: al destinatario de los servicios (consumidor o empresario), a la categoría de firma electrónica que contiene el certificado; según la naturaleza del PSC que emite el certificado y por último según el ámbito territorial en que se presta el servicio.

Finalmente nos ocuparemos en esta parte, de efectuar una enumeración descriptiva, global y general de las prestaciones más habituales del contrato de certificación reconocida, atendiendo a las cláusulas que más frecuentemente se incluyen en el tráfico, estableciendo las

obligaciones principales, específicas, adicionales y accesorias tanto del PSC como del Firmante/Suscriptor, que serán tomadas en cuenta para nuestro estudio.

En el *Capítulo Segundo* determinaremos las características fundamentales del contrato de certificación reconocida, atendiendo a las categorías más frecuentemente utilizadas por la doctrina para la clasificación de los contratos. De igual manera nos hemos cuestionado respecto de su naturaleza jurídica; para solventar esta cuestión, acudimos al propósito contractual concreto del mismo y analizamos si éste coincide con el de los contratos de mandato, arrendamientos de obra y de servicios.

En efecto, como ponemos de manifiesto en nuestro trabajo, la doctrina que se ha ocupado de la materia ha asemejado la certificación con alguno de estos tres tipos contractuales. Partiendo de estos supuestos, determinaremos si la legislación prevista para los contratos mencionados puede ser aplicada al que es objeto de nuestro estudio, acudiendo al recurso de la analogía.

Es en este sector de nuestro trabajo donde identificaremos precisamente, el conjunto de normas jurídicas que resultan de aplicación a la certificación reconocida, tanto las procedentes del ordenamiento español como aquellas que devienen del ámbito comunitario europeo, así como las normas que rigen su contenido tal como han dispuesto las partes, determinando el modo en que se integran al contrato.

El *Capítulo Tercero* se ha destinado para el análisis de los elementos subjetivos (*determinando los requisitos de capacidad del PSC y del Firmante/Suscriptor*), los elementos objetivos (*Certificado reconocido, Datos y Dispositivos tanto de creación como de verificación de firma electrónica*), para finalmente efectuar las consideraciones pertinentes con relación a los elementos formales del contrato.

Denotaremos respecto de estos últimos la peculiaridad manifiesta, en sentido que si bien la certificación reconocida constituye un contrato consensual, es posible observar que en

la práctica reviste la característica de contrato *formalizado*, en el que la exigencia de forma se establece con el alcance que normalmente se le da en materia de contratos, es decir, como una exigencia *ab probationem*.

Solventadas estas cuestiones en el *Capítulo Cuarto* revisaremos las distintas etapas del *iter* contractual, desde la fase de formación o preparación del contrato, atravesando por el momento de su perfeccionamiento y desembocando finalmente en el período de ejecución del negocio jurídico, haciendo notar que las referidas etapas se verifican unas veces en línea (*on line*) y otras fuera de línea (*off line*).

Lo anterior nos lleva a su vez a considerar una serie particularizada de cuestiones que se encuentran ubicadas en su debido orden y lugar, al interior de los distintos períodos descritos precedentemente, así, repararemos respecto: i) de las disposiciones que hacen a la información sobre el contenido del contrato y oferta vinculante; ii) se describirá el procedimiento de solicitud y obtención del certificado electrónico; iii) asimismo, nos detendremos a indagar la posible existencia de responsabilidades pre-contractuales.

Poco después será nuestro objetivo analizar minuciosamente el contenido contractual, delimitando el conjunto de derechos y obligaciones que atingen a los distintos sujetos implicados en las actividades de certificación: el PSC, el Solicitante y Firmante/Suscriptor así como el Usuario del certificado reconocido.

Respecto de este último, haremos notar que si bien constituye un tercero respecto del contrato de certificación reconocida celebrado entre el PSC - Firmante/Suscriptor, y cuyas obligaciones en consecuencia devienen en principio de la ley, nos cuestionaremos sobre la factibilidad de que dichos deberes se formalicen con el PSC mediante la celebración de un nuevo contrato.

El *Capítulo Quinto* se ha reservado para determinar el régimen jurídico de responsabilidades emergentes para el PSC, a cuyo efecto y de manera introductoria a la

temática brindaremos algunas nociones básicas, aproximándonos a las disposiciones generales contenidas en la legislación civil española y las particulares previstas por la LFE.

De conformidad con estas últimas observaremos la previsión legal de un supuesto universal de responsabilidad civil del PSC, el cual resulta exigible de conformidad con las normas generales sobre la culpa contractual o extra-contractual, según proceda, con una inversión de la carga de la prueba por la cual y a efectos liberatorios, corresponde en todo caso al PSC demostrar que actuó con la diligencia profesional que le resulta exigible. Paralelamente se detectarán los hechos que generan la responsabilidad general del PSC, para finalmente considerar los supuestos específicos de responsabilidad que le atingen.

De ese modo se efectúa un análisis de las distintas hipótesis de responsabilidad civil derivadas de los servicios de certificación reconocida, determinando los hechos que pueden producir daños. Éstas se encuentran clasificadas en cuatro grandes grupos, a saber: i) aquellas que son previas o consustanciales a la emisión del certificado; ii) las derivadas de la certificación propiamente tal; iii) las que sobrevienen del servicio de homologación; y iv) las que devienen por las actuaciones de los auxiliares del PSC.

Coronamos esta parte detectando asimismo los supuestos de limitación y/o exoneración a la responsabilidad del PSC, las cuales han sido agrupadas en dos categorías, a saber: i) limitaciones intrínsecas al certificado, que se subdividen en limitaciones cuantitativas y cualitativas; ii) limitaciones extrínsecas al certificado, que admiten a su vez tres variantes, las provenientes de la actuación: del Firmante/Suscriptor; del Usuario del certificado; y del propio PSC.

Para completar nuestro análisis, procuraremos inferir de manera general las responsabilidades que emergen para el Firmante/Suscriptor, determinando por un lado su naturaleza (objetiva o subjetiva); identificando los sujetos frente a los que responde en caso

de producirse daños o perjuicios; y por último, establecer su origen (contractual o extracontractual).

Todo ello desembocará finalmente, en la exposición de las conclusiones generales a las que hemos abordado y que se desprenden de nuestra investigación.

CAPÍTULO PRIMERO

ORIGEN, JUSTIFICACIÓN ECONÓMICA Y PRÁCTICA COMERCIAL

I. Antecedentes y nociones generales.-

1.1. La Sociedad de la Información.-

En la actualidad se viene dando un proceso acelerado de transformación de la civilización humana, que es el paso de la Sociedad Industrial a la Sociedad del Conocimiento, lo cual incide directamente en su forma de interacción y se apoya fundamentalmente en el uso y apropiación de las Tecnologías de Información y las Comunicaciones (TIC) en la vida diaria.² En el avance entre las dos etapas mencionadas se aprecia una fase intermedia que se ha venido a denominar Sociedad de la Información (SI), la cual corresponde a un periodo de transición entre ambas y coincidiría con el momento que se vive en el presente.³

² Las TIC comprenden: a) las tecnologías físicas relativas al ordenador y a las telecomunicaciones (v.gr. televisión, radio, fax, teléfono, télex y más recientemente la Internet); b) las tecnologías inmateriales: sistemas operativos y programas informáticos que contienen (software); c) así como a los bienes y servicios que son capaces de suministrar (v.gr. dinero electrónico, multimedia, video juegos, etc.). Carlos Ferreyros Soto y Audilio Gonzales Aguilar, “*Tendencias de las Nuevas Tecnologías de la Información*”, Montpellier, 2005, ubicado en <http://www.ieid.org/congreso/ponencias/Ferreyros%20Soto.%20Carlos%20-%20Gonzales%20Aguilar.%20Audilio.pdf> // Se define desde su inicio a las TIC como instrumentos y procesos utilizados para recuperar, almacenar, organizar, manejar, producir, presentar e intercambiar información por medios electrónicos y automáticos. Ejemplos: los equipos físicos y programas informáticos, material de telecomunicaciones en forma de computadoras personales, *scanner*'s, cámaras digitales, asistentes personales digitales, teléfonos, facsímiles, *modem*'s, tocadiscos, grabadoras de CD y DVD, radio y televisión, además de programas como bases de datos y aplicaciones multimedia. En resumen, las TIC son aquellas tecnologías que permiten transmitir, procesar y difundir información de manera instantánea. Son consideradas la base para reducir la Brecha Digital sobre la que se tiene que construir una Sociedad de la Información y una Economía del Conocimiento. Las TIC pueden ser tanto tradicionales, como la radio, la televisión y los medios impresos, como nuevas, un conjunto de medios y herramientas como los satélites, la computadora, la Internet, el correo electrónico, los celulares, los robots, entre otros. // Al respecto, Reusser indica que el auge de la SI está indisolublemente ligado al florecimiento de las llamadas Nuevas Tecnologías que irrumpieron con fuerza en la década de los 80 del s.XX y que actúan sobre los procesos técnico-económicos, como es el caso de la nanotecnología, la robótica, la inteligencia artificial, la biotecnología, el láser, las telecomunicaciones, la informática, los superconductores, etc. y en general los avances de la técnica que rompen y cambian la forma tradicional de comprender los conceptos de tiempo y espacio. Precisa que lo de “Nuevas Tecnologías” no ha sido una terminología pacífica, en atención de que se argumenta que es connatural a la existencia humana la evolución en sus múltiples facetas, entre ellas las tecnológicas, y cada época tiene sus propias innovaciones y la velocidad de los cambios hace que lo “nuevo” de ayer, hoy se encuentre tecnológicamente desfasado. Carlos Patricio Reusser Monsálvez, “¿Qué es la Sociedad de la Información?”, en *REDI: Revista Electrónica de Derecho Informático*, No. 61, Santiago, Alfa-Redi, agosto/2003, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1307>

³ El Informe de la Conferencia Ministerial Regional preparatoria de América latina y el Caribe para la Cumbre Mundial de la Sociedad de la Información realizada en Bávaro, República Dominicana, del 29 al 31 de enero de 2003, afirma:

“1. a) El progreso social y económico de los países, así como el bienestar de las personas y de las comunidades, deben ocupar un lugar preponderante en las actividades destinadas a construir una sociedad de la información. El uso y aprovechamiento de las tecnologías de información y comunicación (TIC) son indispensables para satisfacer las necesidades de los individuos, de las comunidades y de la sociedad en general.

1. c) La sociedad de la información debe servir al interés público y al bienestar social, mediante su contribución a la erradicación de la pobreza, la generación de la riqueza, la promoción y el realce del desarrollo social, la participación democrática, la diversidad lingüística y la identidad cultural, asegurando al mismo tiempo iguales oportunidades de acceso a las tecnologías de información y comunicación, ateniéndose siempre al principio de legalidad para asegurar su uso eficiente y ordenado.

2. b) Promover la expansión de las infraestructuras de las tecnologías de información y comunicación y la innovación tecnológica. Las políticas de acceso universal deben promover la mejor conectividad posible a un costo razonable a las regiones subatendidas (...)”

Sin embargo es necesario hacer notar que las distintas naciones del planeta atraviesan de la Sociedad Industrial a la Sociedad del Conocimiento a ritmos dispares.⁴ Así, los países desarrollados que se ubican fundamentalmente en el hemisferio norte, viven ese “presente” de la SI de un modo mucho más avanzado y acelerado que los países en vías de desarrollo, los cuales se ubican básicamente en el hemisferio sur.⁵ Por lo tanto, el fenómeno de la SI y su nivel de inserción en las distintas sociedades presenta diversos matices y niveles de penetración desiguales.⁶

A pesar de todas las dificultades y limitaciones los países en vías de desarrollo han comenzado a tomar conciencia de la integración de las TIC como herramientas estratégicas para su desarrollo social, económico y cultural, buscando vías y mecanismos para permitir que todos los estratos de la sociedad puedan acceder a estas herramientas y las hagan parte de su quehacer diario.⁷ No obstante, la difusión de tecnologías avanzadas en los países desarrollados y en los sectores de alto poder adquisitivo en los países en vías de desarrollo, ha

⁴ El Programa de Naciones Unidas para el Desarrollo (PNUD) afirma que Internet y la el fenómeno de la Globalización están provocando las mayores desigualdades de la historia a todos los niveles. Así, el 20% más rico de la población mundial acapara el 93,3% de los accesos a Internet frente al 20% más pobre que apenas tiene el 0,2%. Este mismo 20% posee el 86% del PIB mundial, mientras el más pobre tiene un 1%. De igual manera, este 20% más rico gana 74 veces más que el 20% más pobre. T. Corcobado Cartes, “*Donde el aire da la vuelta: Sociedad de la Información y exclusión social. El papel de la educación*”, Universidad de Extremadura., 1998, ubicado en <http://www.launion.edu.pe/info99-4.htm>

⁵ Las TIC son los cimientos de un cambio radical que, desde las definiciones industriales/postindustriales de desarrollo, dará origen a un nuevo paradigma basado en el modelo de las Sociedades de la Información. “7. *Es importante advertir que esta evolución es también muy promisorio en lo que respecta al desarrollo económico, sociopolítico y cultural de los pueblos del Sur. Estos países no pueden seguir percibiendo las tecnologías de la información y la comunicación como un lujo exclusivamente reservado a los ricos. La creciente conciencia de esta realidad se ha traducido en la pugna de numerosos países en desarrollo por alcanzar a los países industrializados en términos de acceso a esas tecnologías. Hoy en día, los países en desarrollo no se interrogan tanto sobre la conveniencia de otorgar máximo prioridad a su participación en la estructura mundial y nacional de información como sobre la forma adecuada de aplicar al desarrollo las tecnologías de la información para reducir más que incrementar la distancia que separa a los “poseedores” de los “desposeídos” de información. Semejante estrategia, sin embargo, abre varios interrogantes*”. (las negrillas son nuestras). Tomado del documento de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura: UNESCO (1996): “*Las tecnologías de la información y la comunicación en el desarrollo. Reflexiones de la UNESCO*”, ubicado en <http://infofac.ucoj.mx/documentos/tecnologia.html>

⁶ Para Del Alamo, a pesar de estas aportaciones no existe aún una definición concreta y operacional que consensualice exactamente en qué consiste el fenómeno de la sociedad de la información. Esto provoca que sea difícil determinar con exactitud cuáles son las sociedades o países que ya han alcanzado un *status* determinado para hallarse en la sociedad de la información. Indica que algunos autores como Jan Steyard o Nick Gould plantean una propuesta que si bien esencial y un tanto ambigua, podría determinar las bases que caracterizan los rasgos principales de lo que actualmente podemos entender por Sociedad de la Información: más información, más nivel tecnológico y un progresivo crecimiento del conjunto de actividades y servicios que se desarrollan en la economía del tercer sector. Oscar Del Alamo, “Construyendo la Sociedad de la información”, en *REDI: Revista Electrónica de Derecho Informático*, No. 49, Madrid, Alfa-Redi, agosto/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1464>

⁷ “La realidad contemporánea está marcada por la profunda disparidad existente en el acceso a la informática entre los países del Sur, que recién despiertan a este fenómeno, y los del Norte, principales beneficiarios de aquélla. Ésta es, tal vez, una de las asimetrías más dramáticas de la historia contemporánea. La informática es, en rigor, un dominio de los países industrializados. ...”. Carlos M. Correa y otros, *Derecho Informático*, 1ª reimp., Buenos Aires, Depalma, 1994, pp. 8-9.

ido creando desafortunadamente lo que se conoce como « *barrera o brecha digital* » de acceso a la información y al conocimiento.⁸

De modo que cuando se aborda el difícil tema de definir qué es la SI, son recurrentes las opiniones que afirman que se trata de una sociedad en formación en que las nociones de información, comunicación y TIC se integran, aunque también es usual que se eluda conceptualizar directamente, dando una explicación en base a las características más notables e indiscutidas, pues no es menos cierto, que el trasfondo del asunto es que se trata de un concepto complejo cuyo nivel de desarrollo es incipiente.

De hecho muchas de las tentativas de conceptualizar han devenido en obsolescencia, pero dentro de las que se encuentran vigentes están la de Masuda, quien nos dice desde una óptica humanista que se trata de una sociedad “*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*”.⁹

Bastante más descriptiva resulta la definición proporcionada en el *Libro Verde sobre la Sociedad de la Información en Portugal* (1997), que señala que “*se refiere a una forma de desarrollo económico y social en el que 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 actividad económica, en la creación de riqueza y en la definición de la calidad de vida y las prácticas culturales de los ciudadanos*”.¹⁰

Podríamos esbozar muchas otras definiciones, pero en general son variaciones de las ya señaladas, aunque si es de interés el sello de política pública que desarrollo el Gobierno

⁸ Herrera sostiene que las desigualdades y exclusiones se han acentuado con el *tecnopartheid* representado en lo que hoy se conoce como brecha digital, divisoria/división digital o, bautizada de modo positivo, oportunidad digital. Karina M. Herrera Millar, “Comunicación y Desarrollo en la Sociedad de la Información, Contextos discursivos neodesarrollistas y tecnoinformacionales”, en Erick R. Torrico, comp., *Comunicación, Nuevos Escenarios y Conflictos Sociales*, La Paz, EDOBOL, 2005, pp. 84-93.

⁹ Yoneji Masuda., *La Sociedad Informatizada como Sociedad Post-Industrial*, Madrid, Fundesco Tecnos, 1984.

¹⁰ El Libro Verde fue elaborado por la Comisión de la Sociedad de la Información del Ministerio de Ciencias de Portugal y aprobado por el Consejo de Ministros de Portugal, abril/1997, ubicado en <http://www.missao-si.mct.pt/>.

Vasco en su *Plan para el Desarrollo de la Sociedad de la Información para el Periodo 2000 – 2003*, al entenderla como “*aquella comunidad que utiliza extensivamente y de forma optimizada las oportunidades que ofrecen las tecnologías de la información y las comunicaciones como medio para el desarrollo personal y profesional de sus ciudadanos miembros*”.

Es evidente que la SI es un fenómeno complejo, cuyo análisis es abordado por los investigadores desde múltiples puntos de vista así como desde diversos ámbitos de estudio. Como es posible apreciar, cada una de estas conceptualizaciones responde a cosmovisiones diferentes y explican el fenómeno desde una particular perspectiva; y cada una de ellas será más o menos aplicable dependiendo del ámbito específico al cual tratemos de aplicar el concepto.¹¹

Desde nuestro punto de vista la SI mas allá de los planteamientos filosófico-teóricos sobre su existencia o no, dejando de lado los complejos análisis históricos, económicos, políticos y sociológicos sobre el grado de desarrollo en la que se encontraría, es a todas luces una realidad en el mundo actual, prueba de ello lo constituye la celebración de la Cumbre Mundial sobre la Sociedad de la Información (CMSI)¹² efectuada en dos fases - Ginebra 2003 y Túnez 2005 -, donde estuvieron representados prácticamente todos los países y ciudadanos del globo terráqueo, hecho que denota de forma rotunda la presencia e importancia que la SI cobra para todos los agentes y representantes de la sociedad, tales como administraciones

¹¹ Al respecto, Petrisans hace notar que es necesario realizar una precisión. En general - opina - se puede observar que se usan indistintamente las denominaciones de “Sociedad de la Información” y de “Sociedad del Conocimiento”, pero aclara que una etapa previa al arribo de la Sociedad del Conocimiento, lo constituye el tránsito hacia una Sociedad de la Información. Ricardo Petrisans Aguilar, “El Futuro y La Sociedad Tecnológica. La necesidad de una reflexión”, en *REDI: Revista Electrónica de Derecho Informático*, No. 33, Montevideo, Alfa-Redi, abril/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=655>

¹² Reconociendo la importancia de la revolución de las TIC como instrumento para conformar el futuro del planeta y conseguir los Objetivos de Desarrollo del Milenio fijados en la “*Declaración del Milenio*” (New York-2000), los líderes mundiales decidieron que se necesitaba una visión y diálogo global para instaurar el marco de una SI integradora y justa. De ese modo la Cumbre de Ginebra (2003), puso los cimientos con la *Declaración de Principios* y el *Plan de Acción* y en la Cumbre de Túnez (2005), se emitió el *Compromiso de Túnez* y aprobó la *Agenda de Túnez para la Sociedad de la Información*, que incluye directrices para la implementación y seguimiento de la CMSI. Esta última incluye capítulos sobre mecanismos de financiación, el Gobierno de Internet y la implementación y seguimiento. Los cuatro documentos pueden ser consultados en: Naciones Unidas, *Cumbre Mundial sobre la Sociedad de la Información - Documentos finales Ginebra 2003-Túnez 2005*, Ginebra, Unión Internacional de Telecomunicaciones, 2006, disponible en <http://www.itu.int/wsis/outcome/booklet-es.pdf>

públicas, organizaciones del sector privado, empresas, organizaciones no gubernamentales, organismos internacionales y en general a todos los ciudadanos de la Aldea Global.¹³

Este es el estado de la cuestión, habrá que estar atentos al seguimiento que se haga sobre los objetivos trazados haciendo votos porque los principios aprobados en las dos fases de la CMSI, no pasen de ser meros enunciados teóricos y buenas intenciones, sino que la práctica acompañe el desarrollo de la SI hasta el año 2015, que es cuando las naciones y ciudadanos del mundo se reunirán nuevamente para efectuar una evaluación sobre los compromisos y desafíos que asumieron en Ginebra y Túnez.

1.2. El comercio electrónico.-

Como se ha venido sosteniendo, la revolución tecnológica producida durante la segunda mitad del s.XX significó el surgimiento de la denominada Sociedad de la Información, en la que hoy en día millones de personas alrededor de todo el planeta emplean medios de comunicación electrónicos ya sea: para la búsqueda e intercambio de todo tipo de información y/o a efectos de realizar transacciones estrictamente comerciales.¹⁴ Precisamente la tecnología más difundida hoy en día para dichos propósitos es la Internet.¹⁵

Las referidas transferencias de información se verifican en cuatro niveles: i) el ámbito privado: entre empresas y/o con clientes; ii) el ámbito público: entre entidades públicas y/o con el ciudadano; iii) entre ambos sectores: público y privado; iv) en el ámbito tanto nacional como internacional; las cuales se llevan a cabo mediante los denominados “*Mensajes de*

¹³ Fue MacLuhan quien acuñó el término “Aldea Global”.

¹⁴ Apòl-Lónia Martínez Nadal, *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, Civitas, 2001, 3ª ed., p. 29 y ss.

¹⁵ Fernández especifica que el término Internet, constituye la contracción de *inter-network*, o sea, “entre redes” y su origen y desarrollo -sustenta- lo podemos encontrar en los EEUU en la segunda mitad del siglo XX. Horacio Fernández Delpech, *Internet: su problemática jurídica*, Buenos Aires, Abeledo Perrot, 2000, p. 11 // Para mayores referencias sobre el surgimiento y evolución de Internet consultar: Stephen Segaller, *Nerds 2.0.1. A Brief History of the Internet*, New Cork, TvBooks Inc., ISBN 9781575000886, 1999. // También se sugiere revisar la tesis doctoral de Andreu Veà Baró, *Historia, Sociedad, Tecnología y Crecimiento de la Red. Una aproximación divulgativa a la realidad más desconocida de Internet*, 2002, disponible en http://www.tdx.cesca.es/TESIS_URL/AVAILABLE/TDX-1104104-101718//Index.htm // El “*Federal Networking Council*” (FNC) de los Estados Unidos, en octubre de 1995 ha definido a Internet de la siguiente manera: “*Internet se refiere al sistema global de información que: 1) está lógicamente unido por un espacio global único de dirección basado en el protocolo de Internet TCP/IP o sus extensiones/continuaciones subsecuentes; 2) es capaz de soportar comunicaciones usando la serie de protocolos Transmission Control Protocol/Internet Protocol (TCP/IP) y sus extensiones/continuaciones subsecuentes; y/u otros protocolos IP-compatibles; y 3) ofrece, usa o hace accesibles, ya sea pública o privadamente, servicios de alto nivel soportados en las comunicaciones e infraestructura relacionada descripta aquí*”. Traducción no oficial del informe del 24-X-1995 del FNC de los Estados Unidos; citado por (H. Fernández, 2000: 12).

Datos”,¹⁶ naciendo de ese modo el fenómeno del Comercio Electrónico, el cual posee diversas modalidades¹⁷ y definiciones en la literatura especializada.¹⁸

El concepto de comercio electrónico presenta dos acepciones, una amplia y otra estricta. La primera engloba todo intercambio de datos (o información) a través de medios electrónicos, ya sea que se encuentre relacionado o no con la actividad estrictamente comercial.¹⁹ Por otra parte, la definición estricta supone únicamente las transacciones comerciales electrónicas, es decir de compra venta de bienes o prestación de servicios.²⁰ En uno y otro caso las transferencias de información se valen de los beneficios que ofrecen las TIC, como por ejemplo: el correo electrónico o la World Wide Web (www), ambas

¹⁶ Las Leyes Modelo de la CNUDMI sobre Firmas y Comercio electrónico, ambas definen al mensaje de datos en sus arts. 2, incisos c) y a) respectivamente, del modo siguiente: Por “mensaje de datos” se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax.

¹⁷ Por la orientación de la gestión comercial el comercio electrónico presenta tres modalidades elementales, a saber: i) Business to Customer (B2C) entre el productor y el consumidor (v.gr. tiendas virtuales); ii) Business to Business (B2B) entre empresas (es el sector de mayor crecimiento) y iii) Customer to Customer (C2C) de consumidor a consumidor (v.gr. intercambio de música). A estas tres categorías básicas, se añaden muchas otras variantes, como se encarga de resaltar Fernández, entre ellos por ejemplo: *Business to government* B2G (empresa-administración); *Government to citizen* G2C (administración-ciudadano), etc. (H. Fernández, 2000: 274).

¹⁸ Fernández define el comercio electrónico, como cualquier intercambio de datos relacionados directa o indirectamente con la compra y venta de bienes y servicios por medios electrónicos (H. Fernández, 2000: 273) // Por su parte, Domínguez sostiene que en sentido amplio, el comercio electrónico abarca todo tipo de transacciones comerciales electrónicas, fundamentalmente compraventa de bienes y prestación de servicios, pero igualmente engloba las actividades y negociaciones previas y otras actividades posteriores relacionadas con las mismas como los pagos electrónicos, cuya particularidad radica en que se desarrollan a través de los mecanismos que proporcionan las nuevas tecnologías de la comunicación, como el correo electrónico, u otras aplicaciones de Internet, como los sitios *web*. Andrés Domínguez Luelmo, “La contratación electrónica y la defensa del consumidor”, en Joseba A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, 2001, Edisofer S.L., p.31 // A fin de obtener mayores nociones sobre el comercio electrónico, examinar: Pablo Palazzi y Julian Peña, “Comercio Electrónico y MERCOSUR”, en *REDI: Revista Electrónica de Derecho Informático*, No. 05, Buenos Aires, Alfa-Redi, diciembre/1998, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=193> // Danilo Hernández Cortés, “Aspectos Legales del Comercio y la Contratación Electrónica en Cuba”, en *REDI: Revista Electrónica de Derecho Informático*, No. 95, Cuba, Alfa-Redi, junio/2006, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=6218> // Alejandro Loredo A., “Contratos Telemáticos. Naturaleza Jurídica en la Legislación Mexicana”, en *REDI: Revista Electrónica de Derecho Informático*, No. 98, México, Alfa-Redi, septiembre/2006, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=7176> // (H. Fernández, 2000: 273-293).

¹⁹ Para la noción amplia de comercio electrónico, en criterio de Martínez, debieran utilizarse otros términos, como por ejemplo: *Intercambio, Transmisión o Comunicación Electrónica de Datos* - género - reservando únicamente para la noción estricta, es decir cuando se efectúan transacciones con fines eminentemente comerciales, la expresión de Comercio Electrónico - especie - (A. Martínez, 2001: 30).

²⁰ El comercio electrónico en sentido estricto, consiste en el intercambio de valor entre un vendedor y un consumidor por bienes y servicios, efectuado vía electrónica (v.gr. Internet, EDI, u otro tipo de tecnología). Los bienes y servicios pueden ser: i) enviados físicamente al comprador; ii) vía red (download); o iii) ser disfrutados directamente en línea (on-line). La literatura especializada lo clasifica en seis categorías, a saber: **i) Indirecto.**- Se refiere a aquella actividad comercial en la cual el pedido electrónico está referido a bienes materiales, los cuales son entregados al comprador, por medio de canales tradicionales de distribución, como el correo postal o los servicios de mensajería; **ii) Directo.**- En este caso el pedido electrónico está referido a bienes y servicios inmateriales, situación en la que tanto el pedido, el pago y la entrega de los mismos se efectúa en línea (on-line), ya sea bajando su contenido de la red (download) o disfrutando del mismo en la propia red; **iii) Cerrado.**- Consiste en la realización de transacciones comerciales de forma automatizada, con el intercambio, en formato normalizado o estandarizado de órdenes de compra, venta y pago realizadas de ordenador a ordenador, dentro de comunicaciones sectoriales por medio de redes cerradas, más conocidas como Value-Added Networks (VAN), cuyo uso -previo pago- es proporcionado por los correspondientes proveedores de servicios. Constituye ejemplo típico de este modo de operación, el *close EDI* o EDI cerrado, que en su vertiente comercial surgió en los años 80; **iv) Abierto.**- Consiste en la realización de transacciones comerciales mediante las aplicaciones de Internet, como por ejemplo el correo electrónico o la World Wide Web (www o simplemente Web), mediante la cuales es posible efectuar una transacción electrónica de bienes o servicios, por medio de procedimientos de almacenamiento y reenvío de un mensaje a través de los denominados agentes de transferencia de mensajes (caso del e-mail), o de modo prácticamente interactivo y en línea (caso del Web); **v) Completo.**- Se refiere a aquella actividad comercial en la cual tanto la transacción como el pago por el bien o servicio, se realiza mediante el sistema electrónico (v.gr. tarjeta de crédito, dinero electrónico, etc.); **vi) Incompleto.**- Se refiere a aquella actividad comercial en la cual sólo la transacción utiliza el medio electrónico, pero el pago se efectúa fuera del sistema por medios tradicionales (v.gr. dinero efectivo, cheque de banco, etc.). Erwin Dotzauer Strampfer, *Aspectos Jurídicos y Tecnológicos del Comercio, Firmas y Documentos Electrónicos. Estudio del Proyecto de Ley boliviano*; Santa Cruz, El País, 2009, p. 23 y ss.

aplicaciones de Internet; así como también el EDI (*Electronic Data Interchange*)²¹ en su esfera comercial o el SET (*Secure Electronic Translations*).²²

Todo ello, conforme reflexiona Martínez “*sin perjuicio de que la problemática planteada por toda comunicación electrónica de datos, sea o no de naturaleza comercial la relación de fondo, sean esencialmente idénticos y, por consecuencia, lo sean también sustancialmente, las respuestas jurídicas y técnicas aplicables*”.²³

En cualquiera de los dos supuestos la consecuencia principal reside en que las transferencias de información que tradicionalmente se han venido efectuando en soporte papel, trasuntan a procesos digitales en los que documentos y firmas manuscritas son reemplazados por sus equivalentes funcionales: los documentos y firmas electrónicas.²⁴

Muy pronto, varios empresarios de distintos rubros comprendieron las ventajas que ofrecía el nuevo entorno electrónico y buscaron emplear las TIC con el objetivo de trasuntar las transacciones comerciales que venían efectuando por mecanismos tradicionales, registrándolas por medio de los denominados *Mensajes de Datos* en las redes de comunicaciones, surgiendo de esa manera el comercio electrónico en sentido estricto.

No obstante, las transacciones efectuadas en redes electrónicas debido a las inseguridades que posee el medio requerían de la satisfacción de algunas necesidades legales y técnicas. Desde el punto de vista jurídico, resultaba prioritario asegurar:

- a) Que el contenido del mensaje no fue modificado en el trayecto (inalterabilidad);
- b) Que provenía efectivamente del remitente (identificación indubitada);
- c) Que tanto el remitente como el receptor del mensaje no puedan negar su envío y recepción respectivamente (no rechazo tanto en origen como destino);
- d) Garantizar que el mensaje conservó su confidencialidad (privacidad).

²¹ En español: *Intercambio Electrónico de Datos*.

²² En español: *Transacción Electrónica Segura*, aplicada en el sector bancario.

²³ (A. Martínez, 2001: 30).

²⁴ (A. Martínez, 2001: 30) // Para ampliar los conceptos de documento y firma electrónica, nos remitimos a: (H. Fernández, 2000: 251-271) // También consultar: Ricardo L. Lorenzetti, *Comercio electrónico*, Buenos Aires, Abeledo Perrot, 2001, pp. 55-91.

El cumplimiento de los requerimientos legales descritos se logra gracias a la introducción de una serie de soluciones técnicas, que configuran verdaderas asistencias de seguridad. Nos referimos a los servicios de integridad, autenticación, no repudio y confidencialidad respectivamente, los cuales son proporcionados por la firma electrónica conforme analizaremos más adelante.²⁵

En procura de dar respuesta a las necesidades de seguridad apuntadas, a principios de la década de los años 80 del siglo pasado surgió la tecnología denominada EDI, concebida como “*el intercambio de datos en un formato normalizado entre los sistemas informáticos de quienes participan en las transacciones comerciales con reducción al mínimo de la intervención manual*”.²⁶ El EDI se proyectó en consecuencia, para que el intercambio de datos a fines comerciales se efectúe dentro de sistemas o entornos cerrados de comunicación.²⁷

Los empresarios que desean hacer uso de las bondades del EDI deberán vincularse - a objeto de efectuar transacciones comerciales electrónicas - por medio de convenios previos denominados “*Acuerdos de intercambio*”, en el que se establecen las normas jurídicas y técnicas a las que se sujetarán sus relaciones comerciales por medios electrónicos,²⁸ debiendo quedar claramente estipulados los pasos a seguir entre la fase de formación o preparación y la fase de ejecución del contrato electrónico.²⁹ Por consiguiente, especial importancia revisten

²⁵ (A. Martínez, 2001: 37-38).

²⁶ Definición contenida en el siguiente documento preparado por la Comisión Europea: *Presentación del EDI (Electronic data Interchange)* EUR 11883 ES. Comisión de las Comunidades Europeas, 1989, p. 12.

²⁷ No obstante lo indicado, como hace notar Echebarría, también es posible hoy en día transmitir mensajes en formato EDI y crear comunidades de comunicaciones limitadas, utilizando redes abiertas como Internet, dado que los protocolos de comunicación TCP/IP o los modelos OSI no son incompatibles con los formatos EDI. Estos además -apunta la autora- pueden transmitirse a través de redes abiertas debidamente encriptados o codificados. Joseba Aitor Echebarría Sáenz, “El comercio electrónico entre empresarios”, en Joseba A. Echebarría Sáenz, comp., *El comercio electrónico*, Edisofer S.L., Madrid, 2001, p. 27. Por lo tanto, añadimos nosotros, que el EDI posee dos versiones: el *close EDI* o EDI cerrado conforme fue concebido inicialmente, y el reciente *open EDI* o EDI abierto, que permite actuar en Internet.

²⁸ Con base en el principio de autonomía de la voluntad, reconocido en el artículo 1.255 del Código civil español, Juliá explica que las partes pueden dotarse en los acuerdos de intercambio de cláusulas que faciliten la contratación electrónica, supliendo así los supuestos en que la ley aplicable a los contratos electrónicos presenta ambigüedades. De todas formas, la referida autora considera que no se debe considerar al contrato como la herramienta perfecta para cubrir las deficiencias de la ley, toda vez que por un lado, algunas materias no son *ius dispositionis* y, por otro, porque los contratos vinculan solo a las partes contratantes y no a terceros. Rosa Julià Barceló, *Comercio electrónico entre empresarios. La formación y prueba del contrato electrónico (EDI)*, Valencia, Tirant Lo Blanch, 2000, p. 455.

²⁹ Domínguez sostiene al respecto, que las transacciones vía EDI requieren generalmente de una larga fase de preparación y negociación entre las partes implicadas, para establecer los protocolos técnicos y administrativos, así como los acuerdos que les serán aplicables, por ello - indica - unas relaciones comerciales duraderas, a largo plazo, con un cierto volumen de operaciones, entre partes próximas, que son

las reglas que deben acordar respecto del modo en que se imputaran las declaraciones de voluntad.

Para la década de los años 80 cuando surge el EDI, las tecnologías de firma electrónica basadas en criptografía³⁰ de cifrado simétrico (de clave única o privada)³¹ y asimétrico (de doble clave o clave pública, que permiten generar firmas digitales)³² ya se encontraban muy desarrolladas, de manera que los empresarios tenían la posibilidad de intercambiar entre si las claves criptográficas con las cuales firman sus distintas transacciones,³³ de conformidad con los procedimientos y pactos previos que mutuamente acuerden.³⁴

No obstante, es indudable que el modo de distribuir las claves entre las partes resultaba muy poco seguro, por esta razón fue imprescindible la constitución de las

empresas mutua y recíprocamente conocidas y dignas de confianza, pues solo este tipo de relación justifica los altos costes de puesta en funcionamiento del EDI (A. Domínguez, 2001: 32).

³⁰ Las técnicas criptográficas son las principales herramientas empleadas para conseguir la confidencialidad de la información enviada. El elemento fundamental de las técnicas criptográficas es el algoritmo de encriptado o cifrado, el cual es aplicado a la información que se quiere mantener confidencial. El sistema de encriptado transforma esta información mediante una clave en información cifrada la cual es en teoría, y dependiendo del algoritmo de cifrado utilizado y la longitud de la clave, muy difícil de descifrar. El funcionamiento de las técnicas criptográficas, es analizado en una sintética pero aclaradora exposición por (R. Lorenzetti, 2001: 69-72) // Sobre la misma temática Miguel Ángel Gallardo Ortiz, "Garantías criptológicas de las firmas electrónicas", en *Actualidad Informática Arazandi*, N° 6, 1993, pp. 5-6 // José María Molina Mateos, "Libertad informática y criptología", en *Informática y Derecho*, N° 12-15, 2000, pp. 971 y ss. // José Fernando Irabien Chedraui, "Key Management y Certificación Digital", en *REDI: Revista Electrónica de Derecho Informático*, No. 52, México, Alfa-Redi, noviembre/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1411> // Alfredo Reyes Krafft, "Criptografía: ciencia de la seguridad. Sus antecedentes", disponible en <http://www.alambre.info/2003/12/22/criptografia-ciencia-de-la-seguridad/>

³¹ Conforme pormenoriza Fernández, la moderna criptografía utiliza generalmente un algoritmo matemático para cifrar datos, haciéndolos ininteligibles para el que no posea cierta información secreta -clave criptográfica- necesaria para el descifrado del mensaje. Dentro de la criptografía basada en algoritmos matemáticos encontramos hoy en día dos sistemas: i) simétricos y ii) asimétricos. Cuando la clave de cifrado es la misma que la de descifrado (y, por tanto, los algoritmos de cifrado y de descifrado coinciden) se habla de algoritmo de cifrado simétrico, el cual ha dominado la historia de la criptografía hasta hace un par de décadas, también denominado de "clave privada" o "clave única", mediante el cual quien envía un mensaje lo encripta con una clave privada secreta, y quien recibe el mensaje lo desencripta con esa misma clave. El sistema simétrico si bien permite el cifrado de textos para hacerlos ilegibles, pero no posibilita firmar digitalmente los mensajes y consecuentemente no garantiza la autenticidad y el no repudio (H. Fernández, 2000: 255-256).

³² En 1976 Witfield Diffie y Martín Hellman, publican un trabajo sobre un método de intercambio de mensajes secretos sin necesidad de intercambiar claves secretas. Estas ideas fueron luego desarrolladas, llegándose así a los *sistemas asimétricos* o de "criptografía de clave pública", en los cuales existen dos claves que son complementarias entre sí. En la criptografía de clave pública se utilizan dos claves diferentes, una para el cifrado y otra para el descifrado. La clave de cifrado es pública, esto es, conocida por todo el mundo mientras que la de descifrado (clave privada) solamente es conocida por su propietario. Ambas constituyen lo que se llama un "par de claves" (H. Fernández, 2000: 256) // El esquema descrito evita los peligros de enviar la clave por un conducto inseguro; de hecho la clave pública puede (y debe) ser diseminada (por ejemplo en una pagina web) igual que un número de teléfono o una dirección postal sin incurrir en riesgos de seguridad. Nótese en consecuencia que la criptografía de clave pública se asemeja a un buzón de correos, cualquiera puede introducir una carta en el buzón, pero solamente el poseedor de la llave del buzón podrá abrirlo para acceder a su contenido. Mediante estos sistemas es posible simultáneamente cifrar el mensaje y crear una firma digital, dando posibilidad al receptor del mensaje de verificar tanto la integridad del mismo como la firma del emisor. // A mayor abundamiento sobre la temática consultar el trabajo de Carolina Díaz Levano y Laura María Peraza Adarve, "La Criptografía: Una guerra de Piratas y Corsarios", en *REDI: Revista Electrónica de Derecho Informático*, No. 82, Colombia, Alfa-Redi, mayo/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=950> // Del mismo modo la investigación de Alfredo Reyes Krafft, "¿Qué son los algoritmos de encriptación? Estándares y su aplicación", *Ciber-leyes*, ubicado en <http://www.alambre.info/2003/12/29/que-son-los-algoritmos-de-encriptacion/>

³³ Así por ejemplo, la clave única puede ser intercambiada en una carta en sobre cerrado por medios seguros de entrega; en tanto que la clave pública puede ser intercambiada a través de disquetes, cd's u otros soportes digitales.

³⁴ Estos acuerdos no obstante adolecen de inconvenientes: por un lado, que únicamente son válidos en grupos cerrados y con pocos participantes; de otro, que las partes deberán reunirse nuevamente en la eventualidad de la incorporación de un socio nuevo, o cuando acontezca el cambio de clave de uno de los socios (v.gr. pérdida o robo de la clave).

denominadas “*terceras partes de confianza*” cuyo propósito es el de distribuir la clave pública, especialmente en los casos en que los empresarios se ubican geográficamente dispersos o alejados.³⁵

De esa manera la solución consistió en la prestación de un servicio a través del cual se verifica a la persona titular de la clave pública y se certifica la correspondiente titularidad. El mencionado servicio lleva el nombre de “*Servicio de Soporte*” y el sujeto que lo brinda fue conocido en un inicio como “*Autoridad de Certificación*”.³⁶

Constituye precisamente el *Contrato de Servicio de Soporte* (concebido para brindar servicios de certificación al interior de las redes cerradas de comunicación) el antecedente directo de nuestro objeto de estudio: el *Contrato de Prestación de Servicios de Certificación Reconocida* de las firmas electrónicas que operan en entornos abiertos. En tanto que la entidad que brinda el Servicio de Soporte, denominada *Autoridad de Certificación*, se configura como el antecesor inmediato del Prestador de Servicios de Certificación que opera en redes abiertas de comunicación.

Con el correr del tiempo la irrupción de Internet significó que el comercio electrónico, cada vez más, se lleve a cabo en redes abiertas en lugar de redes cerradas de comunicación en el denominado comúnmente como “Espacio virtual”.³⁷

En el nuevo medio abierto ya no resultan satisfactorios los *Acuerdos de intercambio y Contratos de Servicios de Soporte*, ello debido a que es muy probable que las partes

³⁵ En el caso del cifrado asimétrico, además de constituir un problema de seguridad, la distribución de la clave pública reviste un problema de falta de practicidad, toda vez que por definición, la clave pública es y debe ser conocida por todos, no sólo por las partes contratantes sino inclusive por terceros que puedan verse afectados o perjudicados.

³⁶ El servicio de soporte fue desarrollado por la Recomendación X.509 del CCITT, organismo creado en 1988. CCITT son las siglas del Comité Consultivo Internacional Telegráfico y Telefónico (*Consultative Committee for International Telegraphy and Telephony - Comité Consultatif International Télégraphique et Téléphonique*), antiguo nombre -hasta 1992- del Comité de Normalización de las Telecomunicaciones dentro de la UIT (Unión Internacional de Telecomunicaciones) ahora conocido como UIT-T.

³⁷ La red ARPANET del Departamento de Defensa de los Estados Unidos (precursora de la actual Internet) y la mayoría de las otras redes académicas que habían formado equipo con éste, recibían financiamiento de *Nacional Science Foundation* (NSF), que prohibió el tráfico de redes comerciales en sus redes, hasta que en 1994, se suspendió dicha restricción definitivamente. Gary P. Schneider, *Comercio electrónico*, México, Internacional Thomson Editores, 3ª ed., 2003, p. 29 // Dado que en 1994 se eliminan las restricciones de uso comercial de Internet y el gobierno de EE.UU. deja de controlar la información de la red, el año 1995 se considera el gran despegue de Internet, nace la red comercial, desarrollándose definitivamente el comercio electrónico efectuado por redes abiertas de comunicación, lo que conllevó la necesidad que los Estados aborden legislativamente la materia, sancionando normas jurídicas que regulen las complejas actividades de las autoridades de certificación, denominación que finalmente fue superada por las de: Entidades de Certificación, Entidad Certificadora, Proveedor o Prestador de Servicios de Certificación (PSC) o simplemente Certificador, en atención a que el término “*Autoridad*” se daba a confusión con los organismos que hacen a la función pública o con las autoridades de orden público.

contratantes no se conozcan, lo que implica la ausencia de confianza entre sí.³⁸ En comunidades abiertas de comunicación electrónica en consecuencia, es imprescindible por razones prácticas pero sobre todo de seguridad, poseer un mecanismo para la distribución de las claves públicas muy fiable, de manera que se asegure su indubitable vinculación con el titular de la clave privada.³⁹

En el nuevo entorno por consiguiente es imperiosa la necesidad de acudir a terceras partes confiables que certifiquen las firmas digitales de quienes efectúan transacciones en la red. El modelo de confianza basado en *terceras partes confiables* constituye la base de la definición de la tecnología de Infraestructura de Clave Pública (ICP).⁴⁰ La ICP no es otra cosa que un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública; se encuentra compuesta por distintas terceras partes en las que todos los demás usuarios de la infraestructura confían, a saber: Entidades de Certificación o Prestadores de Servicios de Certificación (PSC); Entidades de Registro (ER) y otras terceras partes confiables, como por ejemplo las Entidades de Fechado Digital (EFD).

³⁸ Fernández al respecto, explica que es de destacar que Internet es una red abierta, pero que existen también redes cerradas a las que se ha denominado redes LAN (*Local Area Network*), cuya interconectividad está limitada a un edificio (*intranets*), o a varios edificios o a varias empresas (*extranets*). En ellas el acceso está restringido a los autorizados o habilitados a tal fin, y funcionan normalmente dentro de empresas, grupos de empresas, o instituciones (públicas o privadas complementamos nosotros). A contrario de lo que ocurre con las redes cerradas -aclara Fernández- al ser Internet una red abierta o pública tiene por característica que nadie puede ser impedido de acceder a ella, con lo cual, la red Internet permite hoy en día el intercambio de datos entre los cinco continentes, posibilitando el acceso a toda clase de contenidos así como su transmisión, entre cualquier usuario del mundo conectado a la red. (H. Fernández, 2000: 12).

³⁹ Martínez igualmente remarca que este nuevo contexto del comercio electrónico, basado en Internet, es conocido como comercio electrónico abierto, y se caracteriza por ser un comercio, a diferencia del EDI, sin necesidad de acuerdos bilaterales previa y largamente negociados y entre partes que no necesariamente mantienen relaciones estables. De esta forma, Internet facilita relaciones ocasionales o a corto plazo entre las partes negociales, sin necesidad de acuerdos o contactos previos. Martínez asimismo alega, que si hasta hace poco el comercio electrónico se limitaba a relaciones inter-empresariales a través de redes propias (cerradas), hoy día se está ampliando y convirtiendo rápidamente en una compleja malla de actividades a nivel mundial entre participantes (empresas, y particulares, conocidos y desconocidos), que utilizan redes abiertas de ámbito mundial y cuyo número no deja de crecer (A. Martínez, 2001: 32-33).

⁴⁰ Los servicios ofrecidos por una ICP (también conocida por sus siglas inglesas como PKI - *Public Key Infrastructure*) se pueden clasificar en: servicios esenciales (v.gr. emisión, revocación, suspensión y renovación de certificados de clave pública); complementarios (v.gr. fabricación y distribución de dispositivos seguros de creación y verificación de firma electrónica); y avanzados (v.gr. servicios de fechado digital). Para mayor abundamiento en el estudio de la ICP consultar: Miguel Ángel Davara Rodríguez, "Firma electrónica y autoridades de certificación: el notario electrónico", en Juan José Martín-Casallo López, comp., *Problemática jurídica en torno al fenómeno de Internet*, Madrid, Consejo General del Poder Judicial, 2000, pp.147 y ss. // Rafael Bonardell Lenzano, "Los certificados de firma electrónica. Los prestadores de servicios de certificación", en Susana García Santa Cecilia, comp., *Firma Electrónica*, Madrid, 2000; en Estudios Jurídicos. Secretarías Judiciales, IV-2000, Madrid, Solana e Hijos A.G., S.A., 2000, pp. 359-377 // Agustín Madrid Parra, "Seguridad en el comercio electrónico", en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003; pp. 136-144 // Sobre modelos de confianza adoptados por una ICP, consultar la Tesis de Grado de Héctor José Gracia Santiago, "Seguridad en el Comercio Electrónico", Álvaro Andrés Motta, dir., Bogotá, Pontificia Universidad Javeriana - Facultad de Derecho, 2004, pp. 114-168 // Un estudio sobre la distribución de riesgos en una ICP, puede ser consultado en Leonor Guini, "Introducción a la Normativa de firma digital y a su régimen de aplicación", en *REDI: Revista Electrónica de Derecho Informático*, No. 82, Buenos Aires, Alfa-Redi, mayo/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=947>

El servicio principal que brinda el PSC a través de la ICP, consiste en la emisión de certificados digitales, constituyendo su propósito central avalar sin margen a dubitación el vínculo entre la clave pública y el titular de la clave privada.⁴¹

1.3. Problemática del comercio electrónico en sentido estricto.-

Uno de las características propias del comercio electrónico es la ausencia de una relación física directa entre las partes contratantes. La innovación fundamental que conlleva Internet reside precisamente en la facilidad a la hora de contratar, ya que no es necesario que las partes estén presentes para que el contrato o el acuerdo a que lleguen tengan plena validez y eficacia jurídicas.⁴² A diferencia de lo que ha ocurrido en el pasado, los negocios y la contratación electrónica ahora tiene lugar sin la presencia física simultánea de las partes.⁴³

En definitiva, el modo de contratación masivo existente en la actualidad requiere de una forma y de una dinámica contractual que permita, facilite y que al mismo tiempo asegure de manera razonable la validación jurídica de las transacciones realizadas por las partes a través de Internet.⁴⁴

Todas estas circunstancias deben tener como consecuencia una variación de los esquemas contractuales que, tradicionalmente, han sostenido el derecho de los contratos en lo referente a la prestación del consentimiento y al momento en el que se entiende perfeccionado el contrato.⁴⁵ Adicionalmente, es necesario considerar que los esquemas

⁴¹ Organismos internacionales como la OCDE, han comprendido que una aplicación muy importante de la criptografía de clave pública es la “firma digital” que se puede usar para verificar la integridad de los datos o la autenticidad del remitente de los datos; por ello publicó en 1997 su política criptográfica en un documento denominado “*The OECD Cryptography Policy Guidelines and the Report on Background and Issues of Cryptography Policy*”, disponible en <http://www.srekcach.org/~utashiro/profile/mirror/OECD-GD97-204.html>

⁴² García hace notar no obstante, que en ningún caso debemos entender que el comercio electrónico se limita únicamente a las transacciones económicas que tienen lugar a través de Internet, sino que, en el sentido de lo que mantiene la OMC, este concepto tiene un ámbito más amplio si consideramos aquellas transacciones económicas que se realizan utilizando medios tales como el fax, teléfono, televisión (pago por visión), sistemas de pago electrónico, el EDI u otros mecanismos similares. Rafael García Del Poyo, “Aspectos mercantiles y fiscales del e-business”, en Joseba A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001, pp.491-492.

⁴³ Las características jurídicamente relevantes de Internet, pueden ser estudiadas en (R. Lorenzetti, 2001: 11-12).

⁴⁴ Al respecto, Oliver sostiene que la contratación electrónica en entornos abiertos, como Internet, a través de las páginas Web y utilizando como medio de pago la tarjeta de crédito, supone otra perspectiva del comercio electrónico, desde luego mucho más universal. Aunque -hace notar- con los inconvenientes de la falta de estandarización en relación con los aspectos técnicos, jurídicos y de protección. No obstante -enfatisa- son cada día más habituales en Internet los métodos de encriptado y los certificados de autenticación, que resuelven algunos de los problemas relativos a estos aspectos. Rafael Oliver Cuello, *Tributación del comercio electrónico*, Valencia, Tirant Lo Blanch, 1999, p.15.

⁴⁵ Un estudio bastante completo sobre los temas que hacen a la contratación electrónica, particularmente respecto al momento del perfeccionamiento del contrato, lugar de celebración, ley aplicable y jurisdicción competente, puede ser analizado en (A. Domínguez, 2001: 33-79) // Igualmente examinar el trabajo de Joseba Aitor Echebarría Sáenz, “El comercio electrónico entre empresarios”, en Joseba A.

contractuales previstos en los Códigos Civiles y en los Códigos de Comercio sistematizados dentro de la familia jurídica romano-germánica de derechos,⁴⁶ tienen como referencia estructural la cercanía espacial y temporal de las partes contratantes.⁴⁷

Conforme se ha reconocido en la Unión Europea (UE) a través de la Directiva sobre comercio electrónico (DCE)⁴⁸, la actividad comercial constituye la base del tráfico en Internet y es el mecanismo principal para financiar los Servicios de la Sociedad de la Información (SSI), de esa manera la UE postula que en provecho de los consumidores y en favor de la probidad de las transacciones, la contratación en Internet debe respetar ciertos parámetros de transparencia y seguridad que deben regularse en la normativa específica sobre la temática.⁴⁹

La DCE postula en sentido que el estímulo de la contratación por medios electrónicos, parte por el desarrollo y adopción de un marco jurídico claro, que contribuya a garantizar la

Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, 2001, Edisofer S.L., pp.101-140 // En idéntico sentido la obra de Rafael Illescas Ortiz, *Derecho de la contratación electrónica*, Madrid, Civitas, 2001, pp. 17 y ss. // Jesús Ignacio Fernández Domingo, “Algunas notas acerca de la contratación y el comercio electrónico”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003; pp. 240-265 // Javier Plaza Penades, “Contratación electrónica y pago electrónico (en el derecho nacional e internacional)”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003; pp. 403-475 // Emilio José Ruiz López, “Contratación bancaria electrónica a través de internet”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003; pp. 477-485 // Rosa Laguna Quiroz, “El Trabajo en la Era Digital: Análisis de la Relación Contractual”, en *REDI: Revista Electrónica de Derecho Informático*, No. 78, Bolivia, Alfa-Redi, enero/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=986> // Carlos Alberto Soto Coaguila, “El Comercio Electrónico en el Derecho Peruano”, en *REDI: Revista Electrónica de Derecho Informático*, No. 41, Lima, Alfa-Redi, diciembre/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1015> // Claudio Magliona, “Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico”, en *REDI: Revista Electrónica de Derecho Informático*, No. 34, Santiago, Alfa-Redi, mayo/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=681> // La estructura problemática del contrato electrónico es abordada asimismo por (R. Lorenzetti, 2001: 163-216).

⁴⁶ Conforme la clasificación propuesta por el comparatista Rene David, en su mundialmente famosa obra “Los Grandes Sistemas Jurídicos Contemporáneos”, los diversos derechos nacionales, pueden ser agrupados en cuatro grandes familias jurídicas a saber: a) la familia del common law; b) la de los Derechos socialistas; c) los sistemas filosóficos o religiosos y d) la familia romano-germánica (civil law). A esta última pertenecen, los derechos de los países en los que la ciencia jurídica se ha constituido sobre la base del Derecho romano. Rene David, *Les Grands Systèmes de Droit Contemporains (Droit compare)*, Paris, Libraire Dalloz, 1964, p. 25 y ss.

⁴⁷ Lorenzetti postula que la mayoría de los autores y de los precedentes jurisprudenciales aplican las reglas generales de los contratos para solucionar los casos en los que hay empleo de medios electrónicos. Esta práctica, basada en la analogía -esgrime- no debe ocultar la complejidad de los temas que se plantean, que abarcan un enorme espectro de cuestiones que exceden las “reglas generales”. Se trata de un fenómeno que puede subsumirse dentro del estudio general del impacto de la tecnología en la contratación civil y comercial, pero que, en opinión suya, no se limita a examinar un nuevo supuesto de hecho a regular con los conceptos y normas disponibles, ya que la influencia es más contundente: es un nuevo supuesto de hecho, que obliga a remodelar los conceptos y normas existentes (R. Lorenzetti, 2001: 162-163).

⁴⁸ 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. La DCE es profusamente examinada en Juan María Díaz Fraile, “Aspectos jurídicos más relevantes de la directiva y del proyecto de ley español de comercio electrónico”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003; pp. 75-121 // Mayores consideraciones sobre el propósito de la DCE son abordados por: Francisco Javier García Más, “Análisis de la proposición de Directiva del Parlamento Europeo y del Consejo 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 Comercio Electrónico)”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000; pp. 139-183 // Javier Maestre y Carlos Sánchez Almeida, “Análisis de la Directiva sobre Comercio Electrónico (Servicios de la Sociedad de la Información)”, en *REDI: Revista Electrónica de Derecho Informático*, No. 35, España, Alfa-Redi, junio/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=692> // Gema Ma. Campillos González, “El comercio electrónico en el marco jurídico de la Sociedad de la Información”, Ministerio de Ciencia y Tecnología, Madrid, disponible en <http://www.ieid.org/congreso/ponencias/Campillos,%20Gema.pdf> // Miquel Peguera Poch, “Servicios de la Sociedad de la Información: Su caracterización Legal en Europa”, en *REDI: Revista Electrónica de Derecho Informático*, No. 100, Chile, Alfa-Redi, noviembre/2006, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=7842>

⁴⁹ Extraído y desarrollado en base al Considerando 29 de la DCE.

seguridad jurídica, asegurando su compatibilidad con las normas vigentes a escala mundial, de manera que la competitividad de la industria de todos los Estados involucrados no resulte perturbada, al mismo tiempo que no se generen trabas innecesarias para la ejecución de medidas novedosas en ese contexto.⁵⁰

Aparentemente la legislación en una Ley Marco - que es el modelo seguido precisamente por la UE - sobre los *servicios de la sociedad de la información*, resulta el modo más apropiado de abordar la temática a efectos de garantizar un tratamiento coherente y con criterios uniformes, toda vez que se abordan materias altamente técnicas y muy especializadas. Cualquier normativa en este ámbito, debe establecer las obligaciones que se impongan a los prestadores de servicios así como también debe determinar las normas mínimas aplicables a la contratación electrónica, delimitando finalmente las características implícitas que hacen a las relaciones entre los prestadores de servicios y sus clientes.

Dicha normativa básica en consecuencia, debe facilitar los elementos que faculden a los diversos agentes involucrados a estar en conocimiento pleno: respecto de la información mínima a la que los usuarios de esos servicios deben acceder, los efectos de contratar haciendo uso de medios electrónicos, la legislación que norma esos contratos, así como los derechos y obligaciones de cada uno de ellos.

Pero debemos reparar en el hecho que la contratación electrónica para ser totalmente eficaz y operativa requiere de normas que regulen los efectos de la firma electrónica, por la cual se instituya de modo claro los requisitos que una firma electrónica debe cumplir a objeto de equipararse a la firma manuscrita. Por consecuencia, se debe igualmente regular las actividades de los Prestadores de Servicios de Certificación de firma electrónica (PSC), detallando las diversas categorías de firma electrónica que pueden existir así como sus específicos efectos, contemplando normas que regulen la participación voluntaria de los PSC

⁵⁰ Extraído y desarrollado en base al Considerando 60 de la DCE.

en sistemas de acreditación o certificación técnica, lo que indudablemente contribuye a mejorar la calidad de sus servicios en beneficio de los usuarios.

Precisamente para solventar las cuestiones enunciadas, en el ámbito de la UE se ha procedido a emitir la Directiva sobre Firma Electrónica (DFE),⁵¹ sobre cuyo contenido y estudio ahondaremos en mayor profundidad a lo largo de la presente investigación.

En definitiva, debemos tomar debida atención al hecho que el comercio electrónico se configura como un recurso básico de Internet y constituye el soporte primordial de la prestación de servicios en la SI.

1.4. Firmas y certificados electrónicos.-

Resulta oportuno aclarar de inicio que la denominación “*firma electrónica*” hace alusión al género, comprende un amplio abanico de todos los medios tecnológicos que permiten firmar electrónicamente (desde los de existencia actual u otros de mayor avance tecnológico que surjan en el futuro), posibilitando la identificación del signatario o firmante.

Ya sea mediante: escaneo o digitalización de una firma manuscrita; firmas basadas en tecnologías de criptografía simétrica o clave única (v.gr. números PIN o Passwords); firmas basadas en tecnologías de criptografía asimétrica o doble clave, una privada y otra pública (v.gr. firmas digitales)⁵²; firmas basadas en tecnologías biométricas⁵³ (v.gr. individualización a través del reconocimiento de la retina del ojo o huellas digitales); firmas que no se basan en una tecnología específica, pero que como mínimo deben garantizar autenticación, integridad,

⁵¹ 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. Un análisis comparado de la Directiva es efectuado por Francisco Javier García Más, “La firma electrónica: Directiva 1999/93/CE, de 13 de diciembre de 1999 y Real Decreto-Ley 14/1999 de 17 de septiembre”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000; pp. 95-138 // Javier Plaza Penadés, “La firma electrónica y su regulación en la Directiva 1999/93 de la Unión Europea”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003; pp. 489-529.

⁵² Fernández asevera al respecto lo siguiente: “Se ha dicho con acierto que la criptografía simétrica goza de una seguridad probable, mientras que la criptografía asimétrica, tiene una seguridad matemáticamente demostrable.” (H. Fernández, 2000: 256).

⁵³ Las tecnologías biométricas, se basan en el reconocimiento e identificación de un sujeto, a través del dimensionamiento de ciertas características y/o proporciones corporales, las cuales son únicas e irrepetibles en cada ser humano (H. Fernández, 2000: 261) // Conforme apunta Giannantonio, el principio esencial de los estudios biométricos en materia de seguridad de datos, es que algunas características personales del individuo no son reproducibles y, por tanto, no son falsificables; por consiguiente, éstas pueden ser utilizadas por el computador como medio de control de la identidad física de la persona que accede a un sistema electrónico. Los datos biométricos más comúnmente usados son las huellas digitales, la retina del ojo, las huellas de los labios y de las manos, el reconocimiento tanto de la voz como de la grafía del individuo. Ettore Giannantonio, *Valor jurídico del documento electrónico; Informática y Derecho. Aportes de la Doctrina Internacional*, t. I, Buenos Aires, Depalma, 1987, p. 116.

no rechazo y confidencialidad (v.gr. firmas electrónicas avanzadas, que cuando emplean tecnologías de criptografía asimétrica coinciden con la denominación de firmas digitales).

A ésta última, de conformidad con la legislación española se suma además la firma electrónica reconocida, que no es otra cosa que una firma electrónica avanzada basada en un certificado electrónico reconocido⁵⁴ y generada mediante un dispositivo seguro de creación de firma.

Asimismo resulta conveniente precisar que la noción de “*certificado electrónico*”, hace alusión igualmente al género, constituye un documento electrónico que refleja determinada información de su titular y otros aspectos (v.gr. límites cuantitativos y/o cualitativos de empleo) que se encuentra firmado electrónicamente por una entidad de certificación que goza de la confianza de una determinada colectividad de usuarios de certificados. Al interior de este concepto general, Martínez subraya que tienen cabida distintos tipos de certificados cuyas finalidades también pueden ser diversas. Entre los certificados de mayor relevancia se encuentra el certificado digital o de clave pública, mediante el cual la clave pública de la firma digital se asocia de manera segura a una persona o entidad determinada.⁵⁵

En ese entendido, un certificado digital⁵⁶ es aquel que se encuentra refrendado con la firma digital de una tercera parte de confianza, nos referimos a la entidad de certificación,⁵⁷ la

⁵⁴ De conformidad con el art. 11.1. (LFE) son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

⁵⁵ (A. Martínez, 2001: 145-147). Sobre las distintas clases de certificados electrónicos, consultar el trabajo de José Cuervo y Mario Antonio Lobato de Paiva, “A Firma digital e entidades de certificação”, en *REDI: Revista Electrónica de Derecho Informático*, No.46, Brasil, Alfa-Redi, mayo/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1509> // En idéntico sentido las investigaciones de Antonio José Vilches Trassierra, *Aproximación a la Sociedad de la Información: firma, comercio y banca electrónica*, Mancha Real, Fundación Beneficentia et Peritia Iuris, 2002, pp.30-31 // Montserrat Tintó Gimbernat, “La criptografía asimétrica o de clave pública: la firma digital y el cifrado. Los certificados digitales y las autoridades de certificación. Aspectos Técnicos y Jurídicos”, en María del Carmen Bernal López, comp., *Jornadas sobre Actos de comunicación: Nuevas Tecnologías*, Madrid, 2001; en Estudios Jurídicos. Secretarios Judiciales, VI-2001, Madrid, S.A. de Fotocomposición, 2001, pp. 765-786

⁵⁶ Para Fernández, el certificado digital es el documento electrónico firmado digitalmente por un tercero (entidad certificadora) que vincula una llave pública con una persona determinada, confirmando su identidad, validando en su caso el contenido de los mensajes de datos generados por éstos. Su misión fundamental es permitir la comprobación de que la clave pública de un usuario corresponde realmente a ese usuario (H. Fernández, 2000: 259).

⁵⁷ Para asegurar la autenticidad del certificado con respecto tanto a su contenido como a su fuente, el PSC, a su vez, lo rubrica con su firma digital, la cual se puede verificar utilizando la clave pública de este último que está recogida en otro certificado de otra entidad certificadora (que puede ser de un nivel jerárquico superior aunque no tiene que serlo necesariamente). Entre otros métodos posibles para verificar la

cual ha procedido con carácter previo a la emisión del certificado a la confirmación de la identidad (u otros atributos) del titular de la respectiva clave privada, por ello, conforme hace notar Martínez, se denominan también “*certificados identificativos*”, toda vez que relacionan a una persona con determinada clave pública.⁵⁸

En el contexto de la criptografía asimétrica, de clave pública o también denominada de doble clave, aparece la necesidad de distribuir la clave pública del titular de la firma digital entre todos los posibles usuarios del sistema criptográfico.⁵⁹ Los instrumentos utilizados como base para efectuar la referida distribución son precisamente los certificados digitales, que consisten en una estructura de datos que relaciona una clave pública con la entidad a la que pertenece durante un intervalo de tiempo.⁶⁰ Es un archivo que incorpora la clave pública de un sujeto y la relaciona con su clave privada.⁶¹ Los certificados digitales verifican la firma de documentos o mensajes y encriptan mensajes, que posteriormente se descifrarán con la clave privada que el certificado relaciona.⁶²

La validez de un certificado digital se basa en que una entidad de certificación de reconocido prestigio, actúe como tercera parte de confianza verificando la identidad del

firma digital del PSC, esa firma se puede registrar en un certificado emitido por ese mismo PSC, que se denomina en ocasiones “certificado raíz”.

⁵⁸ Por ello Martínez hace hincapié, al afirmar que el acto de la entidad de certificación destinado a comprobar que la identidad del titular del par de claves vincula el nombre de esa persona directamente a una clave pública, e indirectamente a una clave privada y, en último término, a una firma digital, no es un acto trivial, sino especialmente delicado, que requiere ciertas garantías (A. Martínez, 2001: 147).

⁵⁹ En ese entendido, Pérez sustenta que la función básica del certificado digital, de la que deriva su aptitud para depositar la confianza en la entidad de certificación, será la de vincular de forma fiable un elemento de verificación de la firma (ligado inescindiblemente al de creación de ésta que se confiere al signatario) con una persona o entidad determinada. Julio Pérez Gil “Documento informático y firma electrónica: aspectos probatorios”, en Joseba A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001, p. 254.

⁶⁰ Martínez nos explica al respecto, que la criptografía de clave pública y las firmas digitales son elementos esenciales del comercio electrónico seguro; y los certificados de clave pública emitidos por las autoridades de certificación, constituyen un elemento esencial para la aplicación de esas tecnologías de forma segura y a gran escala (A. Martínez, 2001: 145).

⁶¹ Fernández aclara que el certificado digital, que se envía juntamente con el documento encriptado y firmado digitalmente, debe contener el código identificativo del certificado, los datos que identifiquen al suscriptor, los datos que identifiquen a la entidad de certificación, la clave pública, la metodología para verificar la firma digital del suscriptor impuesta a un mensaje de datos, el número de serie del certificado y la vigencia del certificado que generalmente es de un año. Apunta el referido autor asimismo, que juega acá también un papel importante la confidencialidad de la información por parte de la entidad certificadora, quien debe mantener la misma bajo la reserva correspondiente, pudiendo solamente levantarla por orden judicial (H. Fernández, 2000: 259).

⁶² Aunque se han definido varios formatos de certificados digitales, el X.509, aceptado por la International Telecommunication Union-Telecommunication Standardization Sector (ITU-T) y por ISO/International Electrotechnical Comisión (IEC), es el de mayor aceptación actualmente. La primera versión (v1) apareció en 1.988. Fue revisada en 1.993, apareciendo la versión 2 (v2), a la que se añadieron 2 campos opcionales de identificación única. Debido al uso del X.509 junto a Internet Privacy Enhanced Mail (PEM) apareció la necesidad de mayor flexibilidad en el formato del certificado. Así, en junio de 1996 apareció la versión 3 (v3), que incluye la posibilidad de tener campos de extensión y que es la que se usa actualmente en todos los sistemas. Una aplicación preparada para trabajar con certificados de la versión 3 puede trabajar con certificados de las versiones anteriores. El X.509 fue diseñado como un marco general para el uso de certificados. Este carácter abierto provoca que haya múltiples posibilidades de uso para algunos de sus campos. Otros formatos definidos son los siguientes: SPKI (Simple Public Key Infrastructure); PGP (Pretty Good Privacy); Certificados de atributos. Sin embargo ninguno de estos formatos tiene la aceptación ni ofrece las posibilidades que ofrecen los certificados X.509.

Para mayor información consultar Eduardo Fdez Parreño, *Extensiones de la V3 del certificado x.509. Seguridad en Redes telemáticas*, en <http://asignaturas.diatel.upm.es/seguridad/trabajos/trabajos/curso%2001%2002/v3x509.pdf>

emisor de un mensaje de datos y dé certeza al destinatario de dicho mensaje sobre tal información.⁶³

Conforme se tiene adelantado, debido a las inseguridades que se presentan en las transacciones efectuadas en redes electrónicas - especialmente en entornos abiertos de comunicación - se requiere la satisfacción de algunas necesidades legales, las cuales que se obtienen en base a una serie de soluciones técnicas, que configuran servicios de seguridad, siendo precisamente la firma electrónica la llamada a solventar los requerimientos legales. Hoy en día el intercambio cotidiano de información tiene como elemento esencial a la firma electrónica, instrumento creado con un triple propósito:

- a) La firma electrónica acredita la identidad de la persona o entidad que está al otro lado de la transacción (autenticación);
- b) Asegura que no ha existido ninguna manipulación posterior de la información o los datos que conforman el negocio (integridad);
- c) Protege los datos de revelaciones o accesos a la información por parte de personas no autorizadas (confidencialidad).
- d) Además, utilizando el sistema criptográfico de clave pública o asimétrica, el documento digital es firmado por el titular imprimiendo su clave privada secreta de la que solamente él tiene conocimiento y acceso. De esta manera, el autor queda vinculado a la firma digital que se verifica con la correspondiente clave pública, sin la posibilidad de negar su autoría (no repudio o irrevocabilidad).⁶⁴

⁶³ El certificado digital, señala Lorenzetti, tiene por función básica la de autorizar la comprobación de la identidad del firmante, pero además debe permitir que el titular lo reconozca indubitadamente y conozca su período de vigencia; determinar que no ha sido revocado; reconocer claramente la inclusión de información no verificada; especificar tal información; contemplar la información necesaria para la verificación de la firma e identificar claramente al emisor del certificado digital (R. Lorenzetti, 2001: 87).

⁶⁴ Cabe aclarar que el no repudio se refiere, en primera instancia, a la posibilidad de exigir al emisor el cumplimiento de la propuesta plasmada en el mensaje de datos; se refiere al hecho de que el deudor no pueda desconocer una obligación válidamente adquirida con un acreedor, lo que se denomina no repudio *en origen*. En segundo lugar, hace alusión al hecho que el destinatario de un mensaje de datos no puede negar la recepción del mismo, lo que se denomina como no repudio *en destino*. Ma. Isabel Huerta Viesca y Daniel Rodríguez Ruiz de Villa, *Los prestadores de servicios de certificación en la contratación electrónica*, Navarra, Aranzadi, 2001, pp. 63-64 // En otras palabras, permite proteger contra el hecho de que alguna de las partes de la transacción deniegue falsamente que ésta o alguna de sus actividades haya sucedido. Como se puede comprobar, los servicios de no repudio tienen un carácter de utilidad *a posteriori*, porque permiten proteger a las comunicaciones realizadas para celebrar los contratos, de posteriores disputas sobre el origen, envío, entrega, contenido o recepción de las comunicaciones. Dávila y Morant aclaran la temática en un interesante trabajo, al respecto consultar Jorge Dávila Muro y José Luís Morant

En consecuencia la firma electrónica es utilizada en infinidad de escenarios y circunstancias con diferentes propósitos y beneficios, dando lugar a una gran variedad de servicios accesorios.

Para el desarrollo de los SSI y particularmente el comercio electrónico, es imprescindible la creación de instrumentos que permitan a los consumidores y a las empresas intercambiar información, contratar y comerciar electrónicamente de una forma segura. En ese entendido, el estímulo de la prestación de servicios de certificación de firma electrónica en competencia a través de redes abiertas de comunicación (v.gr. Internet) resulta prioritario. Para que los medios de certificación electrónica sean verdaderamente efectivos y produzcan los efectos deseados sobre la seguridad del tráfico electrónico, es esencial que se les provea del reconocimiento adecuado por el ordenamiento jurídico.⁶⁵

Igualmente resulta conveniente la equiparación a todos los efectos legales y en la medida de lo posible de la firma manuscrita tradicional y la firma electrónica. Para ello habrán de implantarse mecanismos de firma electrónica avanzada que, relacionada con un certificado reconocido y creada mediante un dispositivo seguro de creación de firma puede considerarse jurídicamente equivalente a la firma manuscrita.

En este sentido, no debe perderse de vista el carácter transnacional de las relaciones a través de Internet: el desarrollo del comercio electrónico internacional necesita de convenios transfronterizos que involucren a terceros países; a fin de asegurar la interoperabilidad a nivel

Ramón, "Servicios básicos de seguridad en la contratación electrónica", en *Encuentros sobre Informática y Derecho. 1994-95*, Pamplona, Arazandi, 1995, pp.35 y ss..

⁶⁵ En base a toda la literatura revisada, considerando las opiniones de autorizados autores en la materia, verificando el estado actual de la cuestión y considerando el necesario rol normativo que le ocupa desempeñar a la Ciencia Jurídica en la SI, podemos concluir manifestando que el camino recorrido por el Derecho para brindar soluciones legislativas reguladoras del novedoso entorno virtual ha sido a todas luces importante, pero aun exíguo para los cambios y complejos desafíos que se vienen en esta era digital, puesto que la aparición de nuevas tecnologías acrecienta la necesidad de modificar las estructuras del Derecho, a objeto de adecuar sus preceptos a las necesidades que demanda la "Sociedad de la Información". La tendencia del ordenamiento jurídico, deberá ser en consecuencia, acopiar las normas que los propios actores de esta novedosa sociedad utilizan y darle el debido reconocimiento y validez jurídica, sin dejarse llevar por la tentación de disciplinar una tecnología en particular. Coincidimos con Andorno, cuando alega que "*La aparición de la nueva tecnología y su aplicación en la vida cotidiana implica del hombre de Derecho no sólo una apertura mental para aceptarla, sino también una elaboración intelectual para encauzar el tema en el espectro jurídico y solucionar los nuevos conflictos que van apareciendo*". Luis O. Andorno, *La informática y el Derecho a la Intimidad*, LL 1985-A.Sec. Doctrina, pp. 1110-1113. En definitiva, haciendo nuestras las palabras de Correa: "*La informática plantea al jurista el desafío de adecuar el cuerpo normativo y doctrinal a la evolución de la tecnología y de nuevas formas de producción y comercialización de bienes y servicios.*" (C. Correa, 1994: 8-9).

global deben celebrarse acuerdos con otros países sobre normas multilaterales en materia de reconocimiento recíproco de servicios de certificación de firma electrónica.

Dentro de este contexto, la heterogeneidad normativa en materia de reconocimiento legal de la firma electrónica y el funcionamiento de los PSC significan un serio obstáculo para el uso de las comunicaciones y comercio electrónico, lo que demanda esfuerzos de correulación técnica y jurídica entre los distintos estados involucrados.⁶⁶ Sin embargo, si bien las diferentes legislaciones del mundo establecen requisitos diferentes con respecto a la validez jurídica de las firmas electrónicas, existe consenso respecto a la utilización de certificados digitales que confirmen la identidad de la persona que firma.

Del análisis de todo lo anterior surgen algunos elementos que necesariamente deben ser considerados a tiempo de estudiar la firma digital. La estructura de la clave pública requiere, adicionalmente, de una compleja estructura de entidades que desempeñan funciones puntuales y normalmente jerárquicas y de fiscalización, en lo que se denomina como Infraestructura de Clave Pública (ICP). Estas entidades se relacionan entre sí vinculando la clave pública a la entidad registrada y se identifican unas a otras, avalándose entre sí para acreditar la autenticidad y origen de una comunicación.⁶⁷

Para relación de éstas se han creado otras Entidades de Registro (ER), quienes tienen como tarea la vinculación o relación de entes registrados en base a protocolos de conducta altamente técnicos. Finalmente, se han creado entidades de verificación del momento de perfeccionamiento de un acto que se denominan Entidades de Fechado Digital (EFD), las

⁶⁶ Así también lo pone de manifiesto la Guía para la incorporación al derecho interno de la LMFE, al señalar: “El riesgo de que distintos países adopten criterios legislativos diferentes en relación con las firmas electrónicas exige disposiciones legislativas uniformes que establezcan las normas básicas de lo que constituye en esencia un fenómeno internacional, en el que es fundamental la armonía jurídica y la interoperabilidad técnica.” Organización de Naciones Unidas, *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno*, Nueva York, CNUDMI, 2002, p.10.

⁶⁷ “51. Una ICP se suele basar en diversos niveles jerárquicos de autoridad. Por ejemplo, los modelos considerados en ciertos países para el establecimiento de una posible ICP entrañan referencias a los siguientes niveles: a) una “entidad principal” única que certificaría la tecnología y las prácticas a todas las partes autorizadas a emitir certificados o pares de claves criptográficas en relación con el empleo de dichos pares de claves, y llevaría un registro de las entidades de certificación subordinadas; b) diversas entidades de certificación, situadas bajo la autoridad “principal” que certificarían que la clave pública de un usuario corresponde en realidad a la clave privada del mismo usuario (es decir que no ha sido alterada); y c) diversas entidades locales de registro, situadas bajo las autoridades de certificación, que reciban de los usuarios peticiones de pares de claves criptográficas o de certificados relativos al empleo de esos pares de claves, y que exijan pruebas de identidad a los posibles usuarios y las verifiquen.” (ONU, 2002: 30-31).

cuales vinculan un documento a un momento en el tiempo avalando con su firma la existencia del documento en el momento referido con múltiples respaldos de orden técnico.

Con los elementos descritos es posible simplificar y precisar más aún el concepto de *Firma Digital*, afirmando que ésta no es más que información digitalizada que ha sido objeto de autenticación y certificación sobre su identidad e integridad, estableciendo de manera indubitable el origen y la vinculación del autor a dicha firma, así como su localización en un momento del tiempo.

Como mecanismo de comprobación de la clave pública del firmante se ha creado el *Certificado Digital*, el cual desde un punto de vista técnico es un fichero digital intransferible e inmodificable emitido por un PSC, que asocia a una persona con una clave pública. El conocimiento de la clave pública es imprescindible para autenticar la firma electrónica y su relación con una determinada persona. Generalmente al enviar un documento firmado digitalmente, éste siempre viene acompañado de un certificado del signatario con el fin de que el destinatario pueda verificar la firma electrónica adjunta.

Con las características anotadas esencialmente concentradas en la seguridad, muchos partidarios y autores de las regulaciones de la firma digital, afirman que ésta otorga actualmente mucha más seguridad que los medios físicos ofrecidos por los conocidos DNI (Documentos Nacionales de Identificación), los pasaportes o las mismas firmas manuscritas.⁶⁸

Conforme hacen notar Ellison y Schneier, los mayores obstáculos a los que se han enfrentado las empresas pioneras en la implantación de soluciones de ICP para sus

⁶⁸ Francisco Hernández Cruz, Juan José López Cebada y Armando Ortega Salamanca, "Breves Consideraciones sobre las Posibilidades Subyacentes en el uso de la Firma Electrónica Avanzada", en *REDI: Revista Electrónica de Derecho Informático*, No. 18, España, Alfa-Redi, enero/2000, disponible en <http://www.alfa-redi.com/rdi-articulo.shtml?x=399> // Fernando Ramos Suárez, "La Firma Digital", en *REDI: Revista Electrónica de Derecho Informático*, No. 10, España, Alfa-Redi, abril/1999, disponible en: <http://publicaciones.derecho.org/redi/No.%2009%20-%20Abril%20de%201999/1ramos> // Fernando Núñez Fernández, "La Firma Electrónica ya Tiene Respaldo y Regulación Legal en España", en *REDI: Revista Electrónica de Derecho Informático*, No. 17, España, Alfa-Redi, diciembre/1999, disponible en: http://publicaciones.derecho.org/redi/No_17_-_Diciembre_de_1999/8 // Ignacio Alamillo Domingo, "Confianza Digital Basada en Certificados", en *REDI: Revista Electrónica de Derecho Informático*, No. 13, España, Alfa-Redi, agosto/1999, disponible en: http://publicaciones.derecho.org/redi/No_13_-_Agosto_de_1999/confianza // Erick Ahón Iriarte, "Firma Digital y el Certificado Digital. El Proyecto Peruano", en *REDI: Revista Electrónica de Derecho Informático*, No. 14, Perú, Alfa-Redi, septiembre/1999, disponible en: http://publicaciones.derecho.org/redi/No_14_-_Septiembre_de_1999/9 // María Martín Reyes, "El Ocaso del Papel", en *REDI: Revista Electrónica de Derecho Informático*, No. 13, España, Alfa-Redi, agosto/1999, disponible en: http://publicaciones.derecho.org/redi/No_13_-_Agosto_de_1999/papel.

necesidades de negocio electrónico (e-Business) han sido tradicionalmente: la falta de interoperabilidad, los costos elevados y finalmente, la tecnología de ICP no se muestra totalmente transparente al usuario final, creando en éste un alto grado de desconfianza debido a su aparente complejidad.⁶⁹ Por lo tanto, ¿constituye la ICP una solución a todos los problemas de seguridad en las transacciones electrónicas? La respuesta depende de qué problema se afronte en cada caso. No existe una solución general única apta para todo tipo de negocio.

La ICP resulta ideal en una intranet, en la que se comparten documentos (trabajo en grupo), se accede a recursos de red (cálculo, servidores de archivos, bases de datos, etc.), se intercambia correo certificado entre los empleados, etc. La ICP resulta mucho más ágil que los sistemas tradicionales de control basados en nombre y contraseña y listas de control de acceso.

En el caso de extranets o de Internet, la ICP es de uso obligado. De hecho, es la única forma conocida actualmente de prestar confianza a los actores de las relaciones telemáticas que no se conocen entre ellos, tanto en el *business-to-business* (B2B) entre empresas, como en el *business-to-customer* (B2C) o comercio al por menor, entre vendedores y compradores particulares por Internet. La confianza en un grupo de PSC mundialmente reconocidas (como la norteamericana VeriSing) permite que las entidades involucradas puedan fiarse unas de otras, a pesar de no existir contacto físico ni vínculo previo entre las partes.

Los esfuerzos de las Administraciones Públicas para trasuntar sus procedimientos administrativos realizados en papel y sometidos a la burocracia estatal hacia procesos digitales interactivos,⁷⁰ lo que se conoce como “*Administración o Gobierno electrónico*” (en inglés: *e-administration; e-govtment*), hacen uso también de tecnología de ICP.⁷¹

⁶⁹ Carl Ellison y Bruce Schneier, *Diez riesgos de la ICP: lo que a usted no le contaron acerca de la Infraestructura de Clave Pública*, disponible en <http://www.counterpane.com>.

⁷⁰ En ese sentido precisamente se pronuncia la DFE entre sus considerándolos el señalar que: “La firma electrónica se utilizará en el sector público en el marco de las administraciones nacionales y comunitaria y en la comunicación entre dichas administraciones y entre éstas y los

II. Delimitación geográfica del ámbito de estudio.-

En el presente trabajo de investigación nos acomete la labor de estudiar un específico servicio de la Sociedad de la Información⁷²: la certificación reconocida de firma electrónica entre empresarios, el cual se instrumentaliza mediante un contrato celebrado entre el titular de firma electrónica (Firmante/Suscriptor) y el Prestador de Servicios de Certificación (PSC).

Advertiremos de inicio, que para abordar el estudio del régimen jurídico del contrato objeto de análisis es necesario aproximarnos a una región mundial y legislación en concreto, de modo que nuestro estudio se concentrará al ámbito del espacio geográfico europeo, y dentro de éste, a la legislación española que le resulta aplicable. Acudiremos además de forma complementaria a las Leyes Modelo de la Comisión de Naciones Unidas para el

ciudadanos y agentes económicos, por ejemplo en la contratación pública, la fiscalidad, la seguridad social, la atención sanitaria y el sistema judicial.”

⁷¹ Tan pronto como los avances tecnológicos, sobre todo en el ámbito de la informática, permitieron efectuar transacciones con fines comerciales por medios electrónicos, introduciendo los documentos y firmas electrónicas para llevar adelante dichos negocios, se observó que las soluciones tecnológicas aplicadas a los fines comerciales, podían perfectamente también ser adaptadas y aprovechadas en todo otro tipo de comunicaciones cuya finalidad no sea estrictamente mercantil. Así, las autoridades públicas, reconociendo estas oportunidades, cayeron en cuenta que era perfectamente posible llevar a cabo sus actividades administrativas por medios electrónicos, empleando documentos firmados electrónicamente, tanto para sus comunicaciones al interior de la administración, como para su relacionamiento con los ciudadanos y viceversa, con los consiguientes beneficios que ello acarrea, reducción de costos, celeridad en los trámites, mayor control social por parte de los administrados, etc. Lo propio ocurre en prácticamente todos los ámbitos, universidades, empresas, instituciones, centros de investigación, etc. han empezado a hacer uso de los medios electrónicos para su comunicación, tanto a nivel interno (entre sus funcionarios) como externo (con sus usuarios o clientes). // Sobre temas de gobierno en línea ver el trabajo de Rosa Laguna Quiroz, “Bolivia: El Gobierno Electrónico: Bases de la Administración Gubernamental en Línea”, en *REDI: Revista Electrónica de Derecho Informático*, No. 67, Bolivia, Alfa-Redi, febrero/2004, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1232> // Igualmente José Luís Barzallo, “El gobierno electrónico en el Ecuador”, en *REDI: Revista Electrónica de Derecho Informático*, No. 95, Quito, Alfa-Redi, junio/2006, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=6204> // Sobre temas de banca electrónica, ver la Tesis de Licenciatura en Derecho de Marcelo Harold Rollano Burgoa, “Fundamentos para un régimen jurídico especial para las transferencias electrónicas de fondos”, Cochabamba, Universidad Católica Boliviana, 2001 // También Alberto Vittone Davila, “Riesgos de la Contratación Bancaria Electrónica en el Derecho Comparado con la legislación colombiana”, en *REDI: Revista Electrónica de Derecho Informático*, No. 82, Colombia, Alfa-Redi, mayo/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=952>

⁷² La “Directiva sobre el comercio electrónico” (DCE), en el inc. a) del artículo 2, entiende por servicios de la sociedad de la información a aquellos “...servicios en el sentido del apartado 2 del artículo 1 de la Directiva 98/34/CE, modificada por la Directiva 98/48/CE;...”. El aludido apartado 2) del art. 1º de la Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998, más conocida como “Directiva de transparencia”, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas y de las reglas relativas a los servicios de la sociedad de la información, modificado a su vez por el apartado 2) del art. 1º de la Directiva 98/48/CE de 20 de julio de 1998, establece lo siguiente:

“Artículo 1º.- A efectos de la presente Directiva, se entenderá por:

2) «servicio»: todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios.

A efectos de la presente definición, se entenderá por:

- a distancia, un servicio prestado sin que las partes estén presentes simultáneamente;
- por vía electrónica, un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético;
- a petición individual de un destinatario de servicios, un servicio prestado mediante transmisión de datos a petición individual.....”

Asimismo en el ordenamiento positivo español, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), de modo homogéneo con la DCE contempla en su Anexo la siguiente definición: “a)...todo servicio prestado a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.”

Derecho Mercantil Internacional (CNUDMI)⁷³, nos referimos a la Ley Modelo sobre comercio electrónico (LMCE)⁷⁴ y la Ley Modelo sobre firmas electrónicas (LMFE)⁷⁵, debido a que dichos instrumentos han constituido indudablemente el modelo y referente normativo inmediato, tanto del legislador español como del comunitario europeo, a momento de encarar el diseño de sus respectivos ordenamientos en esta materia.

Ello sin óbice no obstante, de acercarnos mediante el estudio comparado a otras legislaciones provenientes de regiones no europeas o al análisis de documentos provenientes de organismos internacionales cuando así se ha juzgado conveniente.

2.1. Legislación española de firma electrónica.-

La legislación vigente que hace a la temática en España se encuentra fundamentalmente contenida en la Ley 59/2003, de 19 de diciembre, de firma electrónica (LFE).⁷⁶ De momento

⁷³ También reconocida por sus siglas en inglés como: UNCITRAL - *United Nations Commission on International Trade Law*.

⁷⁴ Organización de Naciones Unidas, *Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno*, Nueva York, CNUDMI, 1999. Al respecto resulta oportuno reseñar que la decisión de la CNUDMI de formular un régimen legal modelo para el comercio electrónico se debió a que el régimen aplicable en ciertos países a la comunicación y archivo de información era inadecuado o se había quedado anticuado, al no haberse previsto en ese régimen las modalidades propias del comercio electrónico. En algunos casos, la legislación vigente impone o supone restricciones al empleo de los medios de comunicación modernos, por ejemplo, al prescribir el empleo de documentos “escritos”, “firmados” u “originales”. Con respecto a los conceptos de documentos “escritos”, “firmados” u “originales”, la LMCE adoptó un enfoque basado en la equivalencia funcional. El “criterio de la equivalencia funcional” se basa en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico.

⁷⁵ Organización de Naciones Unidas, *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno*, Nueva York, CNUDMI, 2002. Cinco años después de haber publicado la LMCE, la CNUDMI conforme expresa en la Resolución aprobada por la Asamblea General de NN.UU. en su 85ª sesión plenaria, llevada a cabo el 12 de diciembre de 2001 “...Deseosa de desarrollar los principios fundamentales enunciados en el artículo 7 de la Ley Modelo sobre Comercio Electrónico con respecto al cumplimiento de la función de la firma en las operaciones de comercio electrónico, con miras a fomentar la confianza en las firmas electrónicas para que surtan efectos jurídicos cuando sean el equivalente funcional de las firmas manuales...” y “Convencida de que la armonización tecnológicamente neutral de ciertas normas relativas al reconocimiento jurídico de las firmas electrónicas y el establecimiento de un método para evaluar de un modo tecnológicamente neutral la fiabilidad práctica y la idoneidad comercial de las técnicas de firma electrónica darán una mayor certidumbre jurídica al comercio electrónico...” emitió en 2001, una nueva Ley Modelo, esta vez sobre las firmas electrónicas.

⁷⁶ Como antecedente cabe señalar que en España, el Gobierno procedió inicialmente a emitir el Real Decreto-Ley 14/1999, de 17 de septiembre sobre firma electrónica (RDL), constituyéndose en la primera disposición legal de aplicación general (y no únicamente sectorial), que norma en el ámbito del derecho español: la firma electrónica, los certificados y los prestadores de servicios de certificación. Dicho cuerpo normativo estaba formado por 28 artículos, reunidos en cinco Títulos, a saber: Título I (Disposiciones generales); Título II (La prestación de servicios de certificación); Título III (Los dispositivos de firma electrónica y la evaluación de su conformidad con la normativa aplicable); Título IV (Tasa por el reconocimiento de acreditaciones y certificaciones) y Título V (Infracciones y sanciones). Para mayores referencias sobre la primera legislación española en la materia, consultar Carlos Marín Calero, “Comentarios al Real Decreto-Ley 14/1999, de fecha 17 de septiembre, sobre firma electrónica, desde la perspectiva notarial. Breve examen de la Resolución de la Dirección General de los Registros y del Notariado, de 12 de noviembre de 1999”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000; pp. 275-307 // Posteriormente, a principios del año 2002 el Ministerio de Ciencia y Tecnología presentó un Borrador de Anteproyecto de Ley de firma electrónica, con el que se pretendía básicamente tres objetivos: a) su tramitación como Ley ordinaria (*lo cual finalmente no se concretó, debido a la expiración del mandato de las Cámaras en marzo de 2000*); b) enriquecer el texto original en base a la experiencia adquirida en esos casi tres años de vigencia del RDL; y c) eliminar las divergencias entre el RDL y la Directiva comunitaria de firma electrónica (*básicamente la referente a la prohibición de copia o almacenamiento de claves privadas por el prestador de servicios de certificación*). Luego se preparó un segundo borrador de Anteproyecto de Ley de firma electrónica, el cual se publicó el 26 de julio de 2002, siendo objeto de amplia difusión y enriquecimiento por diversas instituciones españolas. En 2003, luego de su aprobación por el Consejo de Ministros, se verificó su tramitación parlamentaria como Proyecto de Ley, que finalizó con su aprobación por el pleno del Congreso, en fecha 11 de diciembre del mismo año y su publicación como Ley 59/2003, de 19 de diciembre, de firma electrónica (LFE) en el Boletín Oficial del Estado de 20 de diciembre de 2003, n° 304. Posteriormente el art. 5 de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información (LMISI) introdujo modificaciones en la

focalizaremos nuestra atención en analizar dos aspectos de la referida normativa: su objeto así como efectuaremos un esbozo sintético de su estructura y ámbito de aplicación.

La lectura del art. 1º en su inc. 1ro., permite establecer que el objeto de la LFE es normar tres aspectos fundamentales:

- i) En primer lugar regula la firma electrónica como mecanismo de seguridad de las comunicaciones electrónicas, abordando su noción, estableciendo sus variantes y describiendo sus características;
- ii) Posteriormente se ocupa de establecer la eficacia jurídica que revisten las distintas clases de firmas electrónicas;
- iii) Finalmente se ocupa de regular la prestación de servicios de certificación de firma electrónica.⁷⁷

En cuanto a su estructura, la LFE consta de treinta y seis (36) artículos ordenados en seis títulos, once disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales. De la revisión del articulado de la norma en estudio, es posible inferir que sus disposiciones son de aplicación transversal, vale decir que sus preceptos rigen: i) en comunidades que han celebrado acuerdos previos para el empleo de firmas electrónicas y/o sin ellos; ii) en entornos cerrados y/o abiertos de comunicación; iii) para el caso del comercio electrónico en sentido amplio y/o el comercio electrónico en sentido estricto.⁷⁸

redacción de la LFE (concretamente se modificó la redacción de los apartados 5 y 8 del art. 3; apartados 2 y 3 del art. 13; apartado 4 del art. 31; y se añadió una disposición adicional Undécima). Para mayores referencias sobre la tramitación de las leyes de firma electrónica españolas, así como un estudio muy completo de la vigente normativa, consultar: Apol-Lònia Martínez Nadal, *Comentarios a la Ley 59/2003 de firma electrónica*, Madrid, Civitas, 2004, pp. 23 y ss..

⁷⁷ Estos servicios como venimos sosteniendo, poseen carácter de imprescindibles cuando se efectúan transacciones en redes abiertas de comunicación. La LFE regula por consiguiente los aspectos objetivos de este tipo de servicio (Certificados); como los elementos subjetivos (PSC y Firmante/Suscriptor).

⁷⁸ Conforme explica Huerta, antes de la aparición del RDL, en el Ordenamiento jurídico español se podía encontrar algunos precedentes de normas referidas a la contratación y a la firma por medios electrónicos, sobre todo en materia administrativa, tributaria y de seguridad social, pero conforme sostiene "...se trata de normas que, en todos los casos, hacían referencias puntuales y muy concretas; eran normas aisladas y dispersas en el océano del Ordenamiento jurídico. Y carecían de conexión entre sí, de una base sólida y común que admitiera, de forma genérica y positiva, la validez y la producción de efectos jurídicos de la firma electrónica o digital." Concluye afirmando que a diferencia de aquellas, a partir del RDL se pretende establecer "...una disciplina que permita utilizar, con carácter general, y con la adecuada seguridad jurídica, los nuevos medios tecnológicos." (M. Huerta y D. Rodríguez, 2001: 23-26).

2.2. Marco jurídico de las firmas y los certificados electrónicos.-

La legislación española en el art. 3 de la LFE regula tres categorías de firmas electrónicas, a saber:

- a) Firma electrónica simple o genérica.⁷⁹
- b) Firma electrónica avanzada.⁸⁰
- c) Firma electrónica reconocida.⁸¹

Por otra parte, el legislador español aprueba en el art. 6 LFE la coexistencia de dos tipos o categorías de certificados electrónicos⁸²:

- a) Certificados electrónicos ordinarios (simples o en general).
- b) Certificados reconocidos.⁸³

2.3. Marco jurídico de los servicios de certificación.-

La prestación de servicios de certificación se modulan en la LFE a lo largo de varios artículos fragmentarios centrados fundamentalmente en el PSC, que configuran una serie de deberes y obligaciones generales aplicables a todos los PSC, es decir emitan certificados reconocidos o no, y dedica un conjunto de obligaciones específicas para los PSC que emitan certificados reconocidos.

Su contenido deviene básicamente de las siguientes disposiciones:

Art. 9.- Determina los supuestos en los que el PSC se encuentra obligado a suspender la vigencia de los certificados electrónicos.

⁷⁹ Entendida en el art. 3.1. LFE como 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.

⁸⁰ Definida en el art. 3.2. LFE como aquella firma electrónica que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control, permitiendo su identificación y la detección de cualquier cambio ulterior de los datos firmados, encontrándose vinculada al firmante de manera única y a los datos a que se refiere.

⁸¹ De conformidad con el art. 3.3. LFE constituye una firma electrónica avanzada generada mediante un dispositivo seguro de creación de firma y se halla respaldada por un certificado reconocido. Por disposición del art. 3.4. LFE, a la firma electrónica reconocida se le otorga respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel.

⁸² El art. 6.1. LFE define al certificado electrónico como aquel documento que vincula unos datos de verificación de firma a un firmante y confirma su identidad, debiendo encontrarse necesariamente firmado por medios electrónicos por un PSC.

⁸³ Esta categoría de certificados para ser considerados como reconocidos, deben previamente cumplir una serie de requisitos adicionales de los que se exigen para la emisión de un certificado electrónico ordinario (contenidos en los arts. 17, 18 y 19 LFE). Dichas exigencias consisten entre otras cosas en: ser expedidos por un PSC que cumpla los requisitos establecidos en la LFE, en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes, como en cuanto a la fiabilidad y las garantías de los servicios de certificación que presten (art.11.1.) Los mencionados requisitos se hallan normados fundamentalmente en los arts. 11, 12, 13 y 20 de la LFE.

Art. 10.- Explicita una serie de obligaciones comunes que el PSC debe observar en los casos de extinción y suspensión de la vigencia de certificados electrónicos.

Art. 12.- Configura las obligaciones que el PSC debe observar con carácter previo a la expedición de certificados reconocidos.

Art. 17.- Obliga a que el tratamiento de los datos personales que precisen los PSC para el desarrollo de su actividad se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LPDCCP) y en sus normas de desarrollo.

Art. 18.- Establece las obligaciones generales y comunes a todos los PSC que expidan certificados electrónicos, ya sean certificados reconocidos o no.

Art. 19.- Dispone que todos los PSC deben formular una declaración de prácticas de certificación en la que detallarán las obligaciones que se comprometen a cumplir en relación con la gestión de las firmas y certificados electrónicos que emitan.

Art. 20.- Formula las obligaciones específicas de los PSC que expidan certificados reconocidos.

Art. 21.- Obliga al PSC que vaya a cesar en su actividad a comunicar dicha situación a los firmantes que utilicen los certificados electrónicos que haya expedido, así como a los solicitantes de certificados expedidos a favor de personas jurídicas.

Arts.22 y 23.- Estructuran el régimen de responsabilidad del PSC y se fijan los límites de su responsabilidad.

Al mismo tiempo, resulta oportuno señalar que la LFE no se ocupa de regular las obligaciones del Firmante/Suscriptor así como tampoco las del Usuario del certificado, a diferencia de lo que ocurre con el PSC, para quien como se ha visto dedica de forma más o menos meticulosa varios artículos que señalan sus obligaciones y específicamente dos

artículos para abordar la temática de la responsabilidad (art.22 LFE) y los límites a la responsabilidad (art.23 LFE) - sin agotar no obstante la materia - articulado del cual se pueden inferir ciertas obligaciones que recaen sobre el Firmante/Suscriptor y el Usuario del certificado. No obstante y en todo caso, habrá que recurrir a una interpretación integral del texto normativo para que a partir de ello, coliguemos en qué consisten dichas obligaciones, pues conforme afirma Martínez:

“...la Ley 59/2003, igual que el Real Decreto-ley 14/1999 y que la directiva en que se basa, no regula, a diferencia de otras legislaciones (véase, p. ej., la Ley de Utah, o la Ley Modelo de UNCITRAL), de forma completa y sistemática, los derechos y obligaciones de las partes que intervienen en el sistema de certificados, sino que ha optado por un enfoque basado en la regulación de la responsabilidad, del que, indirectamente, pueden deducirse una serie de derechos y, sobre todo, de obligaciones y deberes de las partes...”⁸⁴

III. Circunscripción del objeto de estudio.-

Es necesario advertir al lector que para el desarrollo de la presente investigación se ha juzgado conveniente efectuar las siguientes demarcaciones:

En primer lugar, de todos los hipotéticos casos que pueden dar lugar a una contratación de certificación de firma electrónica, a fines de la presente investigación delimitaremos el ámbito de estudio al contrato:

- i) En el que tanto el Firmante/Suscriptor como el PSC son ambos empresarios mercantiles;
- ii) En el que la intención del empresario Firmante/Suscriptor estriba en efectuar transacciones comerciales electrónicas seguras con sus clientes (comercio electrónico en sentido estricto) haciendo uso de su firma electrónica en sistemas

⁸⁴ (A. Martínez, 2004: 337).

que no se basan en acuerdos voluntarios de Derecho privado y se celebran entre un número indeterminado de participantes;

- iii) Donde los datos se transmiten por redes abiertas de comunicación, razón que motiva la adquisición de un certificado electrónico que respalde dicha firma a objeto de avalar la plena identidad del Firmante/Suscriptor ante sus clientes en la red, siendo su intencionalidad además, dotar a su firma y los documentos electrónicos suscritos con ella de la validez y eficacia jurídica que la ley reconoce a las firmas manuscritas y los documentos privados respectivamente;
- iv) Lo que da lugar a la emisión de un certificado reconocido.

En consecuencia, desde el punto de vista legal nos circunscribiremos a la emisión de certificados reconocidos y, por ende, a las firmas electrónicas reconocidas, toda vez que son esta específica clase de firmas las que de conformidad con la normativa española (art. 3.4. LFE) cumplen equivalencia a la firma manuscrita, siendo las que auténticamente aplican para efectuar de modo seguro negocios de comercio electrónico estricto en redes abiertas, concretamente Internet.

Desde el punto de vista técnico nos limitaremos el estudio a la Infraestructura de Clave Pública (ICP). Ello se justifica en razón de que si bien la legislación española⁸⁵ al igual que la DFE⁸⁶ acogen el principio de neutralidad tecnológica, es decir, no favorecen una tecnología determinada a momento de crear firmas electrónicas, no parece prudente sustraernos a la realidad del tráfico.⁸⁷

⁸⁵ La legislación española sobre firma electrónica no alude a tecnologías específicas, y por ello es neutra desde esta perspectiva. Determina la gestión con seguridad y certeza de documentos electrónicos firmados y autenticados, mediante: i) unos datos de creación y verificación de firma; ii) a través de dispositivos seguros de creación y verificación de firma, pero no se detiene a precisar tal o cual modalidad tecnológica que deberá considerarse para implementar las opciones de firma. Por lo demás, resultaba innecesario, porque el propio mercado ha estandarizado mundialmente dichos elementos técnicos. Al respecto, el art. 3 de la LMFE establece: “Igualdad de tratamiento de las tecnologías para la firma.- Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable”.

⁸⁶ La DFE señala en su parte considerativa expresamente: “Los rápidos avances tecnológicos y la dimensión mundial de Internet hacen necesario un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos.” (las negrillas son nuestras).

⁸⁷ La neutralidad tecnológica también es explícitamente reconocida en el art. 3 de la LMFE, señalando que: “Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1) del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.”

Lo cierto y evidente es que tanto el legislador comunitario como español, tienen presente que la tecnología más difundida hoy en día para la generación de firmas electrónicas seguras está representada por el cifrado asimétrico o de clave pública.⁸⁸ Ésta además resulta ser en la práctica la tecnología de mayor aplicación en el mercado, por la cual, además de confidencialidad de los mensajes se consigue realizar firmas digitales (*que encuadran según la terminología española y comunitaria, dentro del concepto legal de firmas electrónicas avanzadas*), mismas que pueden ser avaladas por un certificado digital o de clave pública (*que cuando cumple específicas condiciones legales adicionales señaladas para los certificados digitales, se denominan jurídicamente certificados reconocidos*). Adicionalmente, cuando dichas firmas digitales (*avanzadas jurídicamente*) han sido generadas a través de un dispositivo seguro de creación de firma y se respaldan en un certificado reconocido, se enmarcan legalmente en España dentro del concepto de “firmas electrónicas reconocidas”.

De ese modo se excluye la consideración de analizar a los PSC de naturaleza pública. Únicamente nos concentraremos, valga la reiteración, en los prestadores de naturaleza privada y su relación contractual con otra persona también de derecho privado, cuyo interés es obtener un certificado reconocido para efectuar negocios de comercio electrónico en sentido estricto a través de una red abierta como lo es Internet, con las debidas condiciones y garantías de seguridad.

Por tanto se excluyen también del estudio, los contratos celebrados con el certificador para operar en sistemas *con acuerdos previos*, a los cuales, de conformidad con los principios contenidos en la DFE⁸⁹, se respetará conforme las reglas que hayan pactado en el respectivo contrato de servicios de certificación (*nos referimos a las firmas electrónicas utilizadas*

⁸⁸ Varios autores expresan uniformemente este criterio, entre ellos: (M. Tintó, 2001: 785) // (M. Huerta y D. Rodríguez, 2001: 36-40).

⁸⁹ Considerando (16) de la DFE.

exclusivamente dentro de sistemas basados en acuerdos voluntarios de Derecho privado, celebrados entre un número determinado de participantes).

La manera característica en que se materializa el supuesto previamente esbozado, consiste en que el interesado suscriba el correspondiente *Contrato de Prestación de Servicios de Certificación Reconocida de Firma Electrónica* con un PSC debidamente establecido. A lo largo de la presente investigación el reto precisamente consiste en desentrañar el régimen jurídico que hace al referido contrato, considerando que, no obstante que la LFE explicita algunas obligaciones del PSC, regula su responsabilidad fijando los límites a la misma y de esta última se infieren ciertas obligaciones del Firmante-Suscriptor y el Usuario del certificado, podemos afirmar que no existe un tratamiento legal acabado del negocio objeto de estudio.

Inicialmente nos abocaremos a establecer la función económica de este negocio jurídico y luego describiremos a grosso modo la manera en que se desarrolla en la práctica comercial. Posteriormente fijaremos el concepto del contrato objeto de estudio, identificaremos las características principales y deduciremos su naturaleza jurídica, describiremos los elementos personales, objetivos y formales que intervienen así como analizaremos las etapas de formación, perfeccionamiento y el contenido contractual, para finalmente determinar las garantías y responsabilidades que surgen del contrato, de conformidad con la normativa española y comunitaria europea que hacen a la materia.

IV. Función económica.-

A objeto de establecer la función económica que el contrato objeto de estudio denota, nos parece apropiado primeramente contextualizar los hechos que darán origen a este particular y *sui generis* negocio.

Desde una perspectiva puramente económica y subjetiva, el empresario que opta por la modalidad electrónica para llevar adelante sus negocios, está delineando una verdadera

estrategia empresarial y un mecanismo de competencia para llegar de modo más eficiente a su mercado, pues incorpora una valiosa herramienta que genera una serie de beneficios para la empresa, entre los que podemos señalar:

- Acceso a una especie de vitrina mundial para ofertar sus bienes y/o servicios.
- La posibilidad de efectuar una amplia gama de negocios seguros de comercio electrónico en sentido estricto, cuyo objeto contractual consistirá en bienes de naturaleza tangible o intangible. Los primeros se articulan a través de contratos de compraventa o suministro (*comercio electrónico indirecto*); en tanto que los segundos, mediante contratos de cesión de derechos y/o contratos de prestación de servicios (*comercio electrónico directo*), mismos que reditúan para el empresario ingresos y ganancias económicas.⁹⁰
- Incremento de la velocidad de la transferencia de información así como en la distribución y toma de datos.
- Como consecuencia de lo anterior, se facilita la utilización de la técnica *just in time* y de producción flexible, que permiten la elaboración de los productos con escaso margen de anticipación al momento de su requerimiento por parte de los clientes.
- Ello acarrea como consecuencia la reducción al mínimo de las mercancías guardadas en stock, con el consiguiente ahorro que esto representa, ya que disminuyen los costes de almacenamiento y se reducen los gastos de transporte.
- Por otra parte se produce un ahorro de costo en mano de obra, pues muchas de las tareas son efectuadas automáticamente así como un ahorro de material y gastos de gestión, toda vez que los documentos son procesados y archivados en soportes electrónicos, lo que determina un ahorro por costos de papelería y liberación de

⁹⁰ Al respecto, consultar el trabajo de Juan Francisco Ortega Díaz, "Firma digital y tráfico económico. La Importancia del contrato de certificación digital", en M. Jesús Moro Almaraz, comp., *Autores, consumidores y comercio electrónico*, Madrid, Colex, 2004, p. 402.

espacios físicos (necesarios en los documentos en formato papel) para la conservación de dicha documentación.

- Dicho ahorro a su vez determina el aumento de capital circulante, con las correspondientes ventajas empresariales que de ello se derivan.
- Acortamiento del ciclo de pago.
- Mayores facilidades para las pequeñas y medianas empresas (PYMES) a objeto de acceder al comercio internacional, con los beneficios económicos que ello puede reportarles.
- Mejora la atención y el servicio al cliente, que son factores determinantes para que una empresa sea competitiva en el mercado permitiendo incrementar la puntualidad a momento de efectuar entregas, responder más rápidamente a consultas o reclamos, la disminución de los plazos de transporte, etc.

Concluiremos señalando en consecuencia, que los negocios que puede llevar a cabo un empresario en redes abiertas de comunicación junto con las ventajas que de ello devienen, descritas a título enunciativo pero no limitativo, reditúan para el empresario ingresos y ganancias económicas o revisten un componente económico.

No obstante, para gozar de las posibilidades que ofrece el comercio electrónico a través de redes abiertas es necesario garantizar un entorno fiable; resulta prioritario generar la debida seguridad para que el comercio electrónico se desenvuelva. Nótese en consecuencia, que la identificación de los operadores económicos en el tráfico virtual es uno de los pilares imprescindibles para hacer del ciberespacio un entorno fehaciente.⁹¹

En ese sentido, la razón del desarrollo de la firma electrónica y las continuas políticas de implantación en los Estados, tienen un claro fundamento económico. La identificación - *en*

⁹¹ La Guía para la incorporación al derecho interno de la LMFE, alude a los conceptos de “identidad” e “identificación” en los siguientes términos: “117. El Grupo de Trabajo convino en que, a efectos de definición de la “firma electrónica” en la Ley Modelo, el concepto de “identificación” podría ser más que la mera identificación del firmante por su nombre. El concepto de identidad o identificación sirve para diferenciar al firmante de toda otra persona recurriendo a su nombre o a otros datos, que pueden ser otras características notables como la posición o la autoridad de esa persona, ya sea en combinación con un nombre o sin ninguna indicación de nombre.” (ONU, 2002: 58).

sentido amplio -⁹² es imprescindible para la generación de confianza en el tráfico económico. El ciberespacio como espacio virtual de intercambio de bienes y servicios precisa que los operadores económicos sean capaces de saber y también de comprobar que el resto de los operadores en el tráfico son quienes dicen ser. La firma electrónica a través de la combinación de un sistema criptográfico adecuado junto con la intervención de los PSC ha conseguido este objetivo.⁹³

En el contexto descrito debemos comprender que un empresario mercantil (sea individual o colectivo), que desea efectuar negocios seguros valiéndose de una red abierta (*Internet*), requiere contar de manera previa con dos elementos fundamentales, a saber: i) una firma electrónica (que en el caso del cifrado asimétrico se denomina *digital* técnicamente hablando) y ii) un certificado electrónico (denominado digital cuando respalda precisamente una firma digital).

De manera que firma y certificado se configuran en lo que podríamos denominar “*requisitos habilitantes*” para efectuar transacciones seguras de comercio electrónico en sentido estricto, lo cual es obvio, pues sin firma y certificado que la avale el empresario se verá imposibilitado de cerrar negocios en la red. En otras palabras, la *habilitación* a transacciones electrónicas en la red demanda que el empresario disponga con carácter previo, de una firma y un certificado electrónico.

Aun cuando pueda darse por sobreentendido, consideramos oportuno aclarar que la función que cumplirá la firma electrónica es precisamente validar los negocios y transacciones electrónicas que efectúe el empresario en la red (contratos electrónicos firmados electrónicamente); en tanto que el certificado electrónico cumplirá la misión de

⁹² Decimos identificación *en sentido amplio*, toda vez que en el mundo virtual la generación de confianza no se limita únicamente a conocer la identidad del emisor de un mensaje de datos (autenticación), sino que lleva concatenadas las restantes funciones de seguridad inherentes a la infraestructura de clave pública, vale decir: integridad, no repudio y en su caso confidencialidad. Asimismo, en el caso de certificados de atributos, la posibilidad de conocer más allá de la identidad del interlocutor, otra información relevante, como por ejemplo los límites cuantitativos y/o cualitativos de uso de un certificado electrónico, verificar los poderes de representación del solicitante en el caso de certificados cuyo titular es una persona jurídica, etc..

⁹³ Juan Francisco Ortega Díaz, *La Firma y el Contrato de Certificación Electrónicos*, Navarra, Aranzadi, 2008, p. 174.

avaluar dicha firma, confirmando la identidad del empresario frente a sus clientes, quienes por el carácter amplio de la red es casi seguro que no se conocen personalmente entre sí, ni tienen porque llegar a hacerlo.

Pero si además es intención del empresario dotar a su firma electrónica el mismo valor que la firma manuscrita, requiere contar con un tipo específico de firma electrónica, denominada *reconocida* (art. 3.4. LFE), la cual es respaldada a su vez por un certificado electrónico reconocido (art. 11.1.LFE).⁹⁴

Obsérvese en consecuencia, que la firma electrónica y el certificado reconocido que la respalda se configuran como “*requisitos legales*” para que el Firmante/Suscriptor dote a su firma electrónica del valor y la eficacia jurídica otorgados por la LFE.

Respecto a los documentos electrónicos (entre otros, contratos electrónicos) a que dieran lugar las transacciones que efectúe el Firmante/Suscriptor, deben ser considerados como documentos privados de conformidad con lo establecido por el art. 3.6.c. LFE, teniendo el valor y la eficacia jurídica que corresponde a su naturaleza y legislación aplicable (art. 3.7. LFE), por consiguiente podrán ser eventualmente aportados como prueba en juicio (art. 3.8. LFE) o en un arbitraje⁹⁵.

Conforme venimos argumentando, el impresionante desarrollo de la tecnología y la democratización de los medios han obligado a las comunicaciones a utilizar mecanismos cada vez más rigurosos en términos de seguridad y eficiencia. En el contexto de las actividades comerciales, las firmas y los certificados electrónicos - junto a los demás

⁹⁴ La exposición de motivos de la LFE es explícita en este sentido al aclarar que “A la firma electrónica reconocida le otorga la ley la equivalencia funcional con la firma manuscrita respecto de los datos consignados en forma electrónica....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.”

⁹⁵ El apartado seis del art. 5 de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, introduce una disposición adicional Undécima referente a resolución de conflictos señalando que “Los usuarios y prestadores de servicios de certificación podrán someter los conflictos que se susciten en sus relaciones al arbitraje”. Mayores referencias sobre la solución extrajudicial de conflictos y arbitraje en el comercio electrónico entre empresarios (B2B), son deliberadas en el trabajo de (J. Echebarría, 2001: 140-142) // Para referencias sobre el arbitraje comercial internacional, nos remitimos al trabajo de Alfonso Luís Calvo Caravaca y Javier Carrascosa González, “Problemas de extraterritorialidad en la contratación electrónica”, en A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001, pp. 167-169.

servicios conexos de autenticación de datos - se han convertido en un recurso imprescindible para las actuales contrataciones y transacciones mercantiles.

La validez de un certificado digital se basa en que una entidad de certificación de reconocido prestigio, actúe como tercera parte de confianza verificando la identidad de una de las partes y dé certeza a la segunda sobre tal información. De esta forma, conforme apunta Martínez,⁹⁶ el comercio electrónico efectuado por medio de canales abiertos de comunicación (v.gr. Internet) se articula en torno a un elemento objetivo (el certificado)⁹⁷, a cuyo alrededor, a su vez, se interrelacionan tres elementos subjetivos:

- a) la entidad de certificación = emisora del certificado;
- b) el firmante o titular de la firma electrónica = suscriptor del certificado; y
- c) el verificador de la firma electrónica = usuario del certificado.⁹⁸

De manera que en el contexto de los negocios comerciales electrónicos (*actos de comercio electrónico en sentido estricto*) la entidad de certificación reviste la calidad de tercera parte de confianza entre las otras dos partes - contratantes entre sí - en el ámbito del comercio electrónico (*el firmante y el usuario del certificado*).

Las operaciones descritas en su conjunto se estructuran jurídicamente a través de una relación contractual. Cabalmente para obtener la firma y el certificado electrónico el empresario debe acudir a un PSC, con quien suscribirá el denominado “*Contrato de Prestación de Servicios de Certificación Reconocida de firma electrónica*”, momento a partir del cual y en virtud de la ejecución del contrato, el empresario se hace titular de la firma electrónica y consiguientemente del certificado pasando a denominarse “*Firmante/Suscriptor*”.⁹⁹

⁹⁶ (A. Martínez, 2001: 145).

⁹⁷ Para un estudio sobre el rol de los certificados, examinar Ignacio Alamillo, “Confianza digital basada en certificados”, en *REDI: Revista Electrónica de Derecho Informático*, No. 13, España, Alfa-Redi, agosto/1999, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=315>

⁹⁸ En idéntico sentido se pronuncia (J. Pérez, 2001: 253-254).

⁹⁹ Si bien normalmente los PSC de acuerdo con sus Prácticas y Políticas de Certificación, son quienes generan la firma electrónica junto con el certificado que la avala, es posible no obstante, que ambos se generen por separado, de modo que el solicitante de un certificado a

Nótese por consiguiente que entre la entidad de certificación y el Firmante/Suscriptor existe un vínculo contractual, por el cual el primer sujeto se obliga precisamente a la *prestación de servicios de certificación de la firma electrónica* en favor del segundo; en tanto que el Usuario del certificado, no parece tener - en principio - un vínculo contractual con el certificador.¹⁰⁰

Las obligaciones fundamentales que emanan para el PSC consisten en:

- Generar el certificado reconocido y ponerlo a disposición del Firmante/Suscriptor.
- Publicar el certificado en un directorio de acceso público para su consulta así como proporcionar los servicios de validación o verificación de certificados.
- Junto con estas, el PSC asume una serie de otras obligaciones adicionales y complementarias, tendientes básicamente a garantizar los niveles de seguridad que la ICP demanda y la operatividad de otros servicios conexos.

Por su parte, la obligación principal del Firmante/Suscriptor consiste en:

- El pago del precio por concepto del servicio contratado.
- Además asume una serie de otras obligaciones adicionales, como por ejemplo: conservar diligentemente su clave privada, respetar los límites cuantitativos y cualitativos que figuran en el certificado, entre otras.

Llegados a este punto cabe indagar respecto de cuál es fin o propósito perseguido objetivamente por las partes contratantes, en base al conjunto de obligaciones estipuladas y funcionalmente encadenadas en el contrato. La utilidad, como ya nos enseñara Ihering, es el fundamento del derecho y es su razón de ser, no existiendo negocio jurídico que no deba su origen a un fin, esto es, a un motivo práctico.¹⁰¹

momento de tomar contacto con el PSC ya posea unos datos de creación y verificación de firma, con lo que al PSC únicamente le corresponderá emitir el certificado, si de acuerdo con sus Prácticas y Políticas de Certificación, esto sea factible por supuesto.

¹⁰⁰ (A. Martínez, 2001: 145). Al firmante le es entregado el certificado digital, y la clave pública es incluida en listados públicos de la entidad certificadora donde se mencionan las claves públicas de los firmantes y a donde los terceros usuarios pueden acceder para conocerlas. El firmante posee entonces un certificado digital, conociendo tanto su clave privada (es el único que la conoce), como su clave pública - que además figura en los listados de uso público - (H. Fernández, 2000: 257).

¹⁰¹ R. Ihering, *El fin en el derecho*, T. I, 3ª Ed., 1893, p.VIII.

Con las consideraciones preliminares anotadas, estamos en condiciones de afirmar que la función económica que este contrato reviste es la identificación - en sentido amplio - de los operadores económicos en el tráfico virtual, como requisito imprescindible para generar un entorno seguro, de manera que tanto los consumidores como las empresas puedan tener confianza en que sus transacciones no serán interceptadas, ni modificadas y se tenga la certeza que tanto el comprador y vendedor (emisor y receptor de un mensaje de datos) son efectivamente quienes dicen ser.

La identificación en sentido amplio, debe entenderse como funcionalidad omnicomprendensiva de las restantes características de seguridad que aporta un certificado reconocido, además de la identificación, vale decir: autenticación, integridad, no repudio y confidencialidad.

Una vez emitido el certificado reconocido, el PSC envía copia del certificado a su titular y publicará una copia en un directorio público de consulta donde constarán las circunstancias que afecten a su validez, figurando la pérdida o suspensión de sus efectos en el caso que se produjesen. De esta manera el receptor de un mensaje firmado digitalmente solo podrá tener la plena confianza en el certificado electrónico y su clave pública asociada, si tras una visita a este directorio comprueba que el certificado está vigente.

El deber del PSC a conceder el acceso a los terceros para que verifiquen el contenido del certificado es una obligación al servicio de la certificación. De nada sirven todas las obligaciones si ésta no se cumple, ya que la utilidad del servicio no se traslada al firmante del certificado, debido a que no se generará la confianza que hará posible la fiabilidad de la firma electrónica ante los ojos de los Usuarios del certificado.¹⁰²

¹⁰² (J. F. Ortega, 2008:257). Idéntico criterio sostiene Umaña, quien cuestiona qué es lo que ofrece en realidad una entidad de certificación ¿Productos o servicios? En respuesta a la interrogante planteada, el referido autor señala que los usuarios de certificados digitales acuden al certificador, porque éste les brinda confianza respecto de las personas con las que se están comunicando en una transacción electrónica, y esta confianza - asevera - no se logra sólo con la emisión del certificado (que individualmente considerado lo concibe como un producto) sino desplegando una serie de actividades tendientes a asegurar la identidad de sus suscriptores y el uso del certificado a través del sistema de certificación digital. En primer lugar - refiere - el certificador debe efectuar un procedimiento de verificación de la identidad y demás información relevante del suscriptor, luego procederá a emitir el certificado en el que se deja constancia de dicha identidad, debiendo facultar a los usuarios la consulta sobre el estado de los certificados, a fin que éstos comprueben si se encuentran vigentes o revocados, así,

A partir de ahí conforme argumenta Ortega, debemos cuestionarnos el alcance del propósito objetivo perseguido. En otras palabras, la firma electrónica proporciona una identificación de las partes en el tráfico económico, esta identificación, articulada como sabemos a través de un certificado vinculado a la clave pública del titular de firma, será de mayor o menor amplitud en función de la información contenida en el certificado digital. Es esta sin duda la función tradicional de la firma electrónica a la que podríamos denominar función identificativa, en sentido estricto, aunque la firma electrónica tiene en el tráfico económico virtual un alcance mucho mayor.¹⁰³

En el conjunto de la contratación electrónica en redes abiertas existen ocasiones en las que no sólo es necesaria la identificación de la otra parte sino también sus sitios web o incluso los productos ofertados. Por ello es habitual que las empresas que comercian en la red doten a sus *web-sites* de certificados digitales para garantizar a los usuarios que dicho sitio web pertenece efectivamente a su titular legítimo.

No obstante, no debemos olvidar que la función identificativa es tan solo una de las dos funciones que desde una perspectiva jurídica resulta relevante. Su función como instrumento para prestar el consentimiento en las relaciones contractuales de sus titulares, al igual que ocurre con la firma manuscrita en el ámbito tradicional, es su auténtica y definitiva finalidad, lo que se conoce como equivalente funcional.¹⁰⁴

el usuario podrá confiar en el certificado siempre que no se encuentre incluido en la lista de revocación de certificados publicada. En ese entendido, concluye afirmando que “...*el certificado, aislado del sistema de certificación digital, no genera verdadera confianza en los usuarios del sistema. Son las actividades que la entidad realiza (el procedimiento de verificación, la revocación de los certificados que se han visto comprometidos, etc.), lo que genera la confianza que permite realizar una determinada transacción. Las anteriores razones nos permiten concluir que se trata de una actividad que acarrea esencialmente la prestación de servicios.*” Andrés Felipe Umaña Chaux, “Entidades de certificación: una aproximación a su régimen de responsabilidad.”, en Universidad de los Andes, Grupo de Estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática, *Derecho de Internet y telecomunicaciones*, Bogotá, Legis, 2003, pp.440-443.

¹⁰³ (J. F. Ortega, 2008:174-175). Las legislaciones existentes que regulan la utilización de la firma digital, cumpliendo con el principio internacionalmente aceptado de la “*equivalencia funcional*” le otorgan a ésta la misma validez y eficacia jurídica, como si fuera una firma manuscrita, lo que permite la identificación plena de su titular (H. Fernández, 2000: 259).

¹⁰⁴ Así lo pone de manifiesto, entre otros, Ortega (J. F. Ortega, 2008:176). En ese entendido, merecen particular atención los requisitos de formación de los contratos, que en la generalidad de los países que se rigen por el derecho romano-germánico, se encuentran representados por: el consentimiento; el objeto; la causa y la forma. De entre todos ellos, es precisamente el consentimiento quien debe ser considerado con bastante detalle al hablar de la firma electrónica y de la calidad de ésta firma y la necesidad de que sea rodeada de todas las formalidades del caso. Veremos que en realidad éste es el único punto tratado con minuciosidad por las legislaciones de firma electrónica, al tener relevancia con el consentimiento. Véase sobre el particular Carlos Barriuso Ruiz, *La contratación electrónica*, Madrid, Dykinson, 1998, pp.33 y ss. // V. Carrascosa López y otros, *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, Granada, Comares, 1997, pp. 3 y ss. // Olivier Hance, *Leyes y negocios en Internet*, México, McGraw-Hill, 1996, pp. 46 y ss. // Javier Ribas Alejandro, *Aspectos jurídicos del comercio electrónico en Internet*, Pamplona, Arazandi, 1999, pp.17 y ss.

La generación de confianza, fin último del sistema de firma electrónica, depende de la actuación tanto del PSC como de los firmantes. Garantizando un comportamiento seguro y fiable de estos dos sujetos - ora *ex lege*, ora vía contractual - el Usuario confiara en los certificados emitidos por el PSC.

Lo que nos llevará finalmente a cuestionarnos sobre ¿qué posición ocupa este tercero Usuario del certificado?

Si bien el derecho de verificación del estado de los certificados (vigente, suspendido o extinguido) a favor del Usuario, al margen de ser una obligación contractual del PSC (en sede del contrato de certificación reconocida), reviste categoría de auténtica obligación legal (art. 18.d. LFE), es posible percatarse que la certificación reconocida genera un entramado jurídico triangular entre tres sujetos jurídicamente independientes entre sí, pero vinculados por la operación económica subyacente.

Razonamiento que nos llevará finalmente a indagar sobre un aspecto: ¿es viable que entre el PSC y el Usuario del certificado se configure otra relación contractual, a través de un contrato nuevo y formalmente independiente del contrato de certificación reconocida? En otras palabras ¿es factible que las obligaciones del Usuario del certificado se contractualicen con el PSC?

Dejamos de momento abierta la interrogante, sobre la que volveremos en el Capítulo Cuarto a objeto de efectuar un detenido análisis indagando esta posibilidad.

V. Práctica comercial.-

5.1. Aproximación al concepto y definición inicial.-

Con carácter previo a la descripción de la práctica habitual del contrato de certificación reconocida de firma electrónica entre empresarios, procuraremos ofrecer una definición aproximada del mismo. No obstante, es conveniente aclarar que no fijaremos en este lugar un concepto jurídico ni definitivo del contrato objeto de estudio; radicando de

momento nuestra intención en delimitar desde un inicio y como punto de partida, el supuesto contractual que queremos abordar en nuestra investigación.

De entrada, procuraremos esbozar el concepto que hace al genérico contrato de certificación, proponiendo la noción siguiente:

La certificación electrónica es el contrato por cuya consecuencia y efecto una de las partes (*PSC*) asume la prestación de generar a favor de la otra (*Firmante/Suscriptor*) un certificado electrónico, mediante el cual se acredita la identidad del Firmante/Suscriptor frente a terceros (*Usuarios del certificado*) en redes de comunicación electrónica, vinculando de modo seguro los datos de creación con los datos de verificación de firma electrónica del Firmante/Suscriptor; asumiendo además el PSC (*frente al Firmante/Suscriptor y los Usuarios del certificado*), la obligación de gestionar el ciclo vital¹⁰⁵ de los certificados electrónicos y colocar a disposición todos los componentes tecnológicos que hacen al funcionamiento propio de la certificación electrónica, garantizando con la debida diligencia y medios las funciones de seguridad y confianza del sistema. En tanto que la otra (*Firmante/Suscriptor*), asume la contraprestación de entregar al PSC una cantidad de dinero (*precio cierto y determinado*) por concepto de pago del servicio recibido.

Conforme analizaremos en el presente Capítulo, el contenido contractual que suele quedar fijado en la práctica se halla compuesto por un conjunto de prestaciones a cargo de ambas partes contratantes. Inicialmente expondremos de manera general en qué consisten dichas prestaciones además de fijar los demás aspectos referidos a la relación contractual. Es necesario acotar que esta descripción será eminentemente práctica, ya que atendida su

¹⁰⁵ La expresión “ciclo vital del certificado” debe entenderse de forma amplia como el período que va desde la solicitud del certificado o desde la creación del certificado hasta su extinción o revocación.

condición de contrato legalmente atípico, aunque no innominado, consideramos oportuno partir de la realidad económica - como aconsejaba el maestro Garrigues - y obtener las notas caracterizadoras del contrato, procediendo a su delimitación tipológica e identificando las prestaciones socialmente típicas que lo caracterizan.

Posteriormente, para la construcción del régimen jurídico-privado del contrato recurriremos además del denominado Derecho de los formularios, también al análisis de la jurisprudencia recaída, no tanto sobre el contrato en sí (por ser prácticamente inexistente, dada la inclusión en tales contratos de cláusulas arbitrales así como la acusada tendencia a resolver los conflictos entre las partes por medio de la transacción), como sobre sus principales elementos y sobre aquellos contratos con los que presenta una semejanza no solo genética sino también funcional, integrándola en el marco de una relación de certificación reconocida de firma electrónica.

De igual modo acudiremos al estudio de la doctrina tanto española como comparada, que al igual que en el caso anterior, existe en relación con los elementos que configuran el contrato, así como respecto de contratos afines. Finalmente recurriremos al auxilio que presta el Derecho comparado y a las cada vez más comunes aportaciones del denominado *soft law*.¹⁰⁶

5.2. Diferenciación de otros contratos de certificación.-

Conforme se tiene analizado, el contrato de certificación de firma electrónica que estudiamos consiste, esencialmente, en la generación y publicación por parte del PSC de un certificado reconocido en favor del *Firmante/Suscriptor*, mediante el cual se acredita la plena identidad de este último frente a sus clientes (*Usuarios del certificado*) a momento de

¹⁰⁶ En terminología anglosajona el *soft law* o como se lo denomina en castellano “derecho blando, flexible o pre-derecho”, hace alusión a los llamados órdenes jurídicos privados, que se configuran como instrumentos normativos diseñados para resolver problemáticas muy específicas en determinados sectores y son elaborados por instituciones supranacionales y/o grupos de estudiosos del Derecho. No constituyen en consecuencia textos con valor oficial, en contraposición con el llamado *hard law* o “derecho duro”, conformado por normas de derecho internacional que poseen carácter vinculante para los estados. Asimismo cabe señalar, que en la medida que el tráfico lo demanda y se hace evidente una sentida necesidad, los instrumentos del *soft law* pueden constituir herramientas para el desarrollo futuro del derecho internacional mediante la construcción de una *opinio juris*. Al respecto consultar: Mauricio Iván del Toro Huerta, “El fenómeno del *soft law* y las nuevas perspectivas del Derecho Internacional”, *Anuario Mexicano de Derecho Internacional*, vol. VI, México, UNAM, 2006, pp. 513 - 549.

efectuar transacciones comerciales electrónicas, asumiendo el PSC además la obligación de gestionar el ciclo vital de los certificados reconocidos.

Con carácter previo al análisis del contenido del contrato, se hace necesario diferenciarlo de otras figuras contractuales también pertenecientes al ámbito de la certificación electrónica con los que guarda próxima relación, nos referimos a los contratos de certificación especiales. Ello contribuirá a concretar el tipo contractual que estudiamos.

a) El contrato de certificación de sitios web.-

En primer lugar, se debe diferenciar el contrato de certificación reconocida de firma electrónica del denominado contrato de certificación de sitios web. Mientras que en el primero opera una prestación de servicios a objeto de identificar de manera indubitada a una persona física o jurídica, en el segundo lo que se busca es identificar la pertenencia de un establecimiento virtual a una persona en concreto.

Conforme explica Ortega *“Para los empresarios que comercian en Internet a través de plataformas web, sitios web o websites, junto a las prestaciones habituales que los identifican como empresa, es habitual que exista la necesidad de identificar, igualmente, dichas plataformas. En otras palabras, el certificador debe proyectar al tráfico virtual la seguridad que dicha plataforma pertenece a su legítimo propietario”*¹⁰⁷.

Si bien es cierto que en base a la autonomía de la voluntad nada impediría que en una misma relación contractual las partes negocien la prestación conjunta de ambos servicios, la realidad comercial demuestra que la tarea certificadora que recae sobre personas físicas o jurídicas se formaliza contractualmente de forma independiente de aquella otra que recae sobre establecimientos virtuales, constituyendo por consiguiente dos tipos de contratos diferenciados.

¹⁰⁷ (J. F. Ortega, 2008:182-183).

b) El contrato de firma de códigos.-

En este caso nos encontramos “...ante un contrato de certificación de firma destinado a la identificación del firmante que es creador de programas o aplicaciones informáticas, con el fin de que tal producto se comercialice y distribuya de forma segura, manteniendo los derechos morales de su creador”.¹⁰⁸ Obsérvese en consecuencia, que el contrato de firma de códigos se diferencia del contrato de certificación reconocida de firma electrónica, en cuanto éste no posee por finalidad la certificación de los mensajes de datos, sino que su funcionalidad consiste en impedir cualquier posible violación de los derechos de la propiedad intelectual de los códigos informáticos.

c) El contrato de visados electrónicos.-

El servicio de visado digital también llamado sellado electrónico, consiste en firmar electrónicamente un documento incluyendo el cuño de una determinada entidad, siendo particularmente útiles por ejemplo en la presentación o transmisión electrónica de planos, proyectos, etc. Así, en el caso de los ingenieros o arquitectos que requieren presentar un proyecto con el visado colegial, es factible la presentación electrónica del proyecto mediante la firma electrónica del profesional, junto con el cuño o visado del colegio profesional al que se encuentran adscritos.

Difiere del contrato de certificación reconocida de firma electrónica, en el entendido que mediante el visado electrónico el mensaje de datos se firma y se señala una única vez, con el objetivo de que terceros utilicen tales mensajes de datos de manera equivalente al soporte papel.¹⁰⁹

A modo de conclusión general en esta parte, podemos señalar que una vez identificados los aspectos más sobresalientes de los contratos de certificación especiales, resulta evidente que los mismos guardan una directa relación con el contrato de certificación

¹⁰⁸ María Pérez Pereira, *Firma electrónica: Contratos y Responsabilidad Civil*, Navarra, Aranzadi, 2009, pp. 191-192.

¹⁰⁹ (M. Pérez, 2009: 194-195).

de firma electrónica, toda vez que en algunas ocasiones resulta necesaria la certificación de firma para poder contratar otro tipo de certificaciones. No obstante, los contratos de certificación de sitios web, firma de códigos y visados electrónicos se presentan en el tráfico como figuras contractuales diferenciadas del contrato de certificación de firma electrónica.

5.3. Clasificación de la certificación electrónica.-

Resulta igualmente oportuno detenernos un momento para efectuar una clasificación de los distintos tipos de certificados electrónicos y los servicios de certificación que existen, así como las modalidades contractuales del mismo.

5.3.1. Por el destinatario de los servicios.-

Los servicios de certificación de firma electrónica se pueden clasificar en primera instancia, atendiendo al destinatario de los servicios, de la manera siguiente:

a) Contratos de certificación con consumidores.-

En este primer caso nos encontramos ante un consumidor que contrata los servicios de certificación con el PSC, normalmente con la intención de identificarse en las redes de comunicación a objeto de efectuar pagos en infraestructuras que permitan dicha aplicación, cuyos mecanismos de pago electrónico se encuentren basados en firma electrónica.

De manera que los consumidores usualmente requerirán incluir en el certificado a ser expedido datos bancarios sensibles, como por ejemplo numeración de tarjetas bancarias.¹¹⁰ En consecuencia, nótese que en este tipo de contratos habitualmente el PSC deberá desplegar un número menor de prestaciones adicionales a sus clientes.

Asimismo es conveniente resaltar, que a este tipo de contratos se le aplica la normativa de protección destinada a los consumidores y usuarios contenida en el 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 (TRLGDCU).

¹¹⁰ (J. F. Ortega, 2008:180-181).

b) Contratos de certificación con empresarios.-

La contratación de servicios de certificación por parte de empresarios es la que más habitualmente se presenta en el tráfico, lo cual es lógico, pues son éstos quienes se encuentran muy interesados en mejorar el relacionamiento con sus clientes, llegar a un mercado mucho más amplio y diversificado, incorporar herramientas tecnológicas que les permitan incrementar sus niveles de rendimiento y eficiencia, acortando el ciclo de pagos, etc.

En definitiva, la posibilidad de efectuar una amplia gama de negocios seguros de comercio electrónico en sentido estricto, determina que los empresarios hagan uso de los servicios de un PSC con cada vez mayor frecuencia.

A diferencia de lo que ocurre con los consumidores, los empresarios requieren una función identificativa mucho más amplia, vale decir, una labor que vaya más allá de identificar y dotar de seguridad a las comunicaciones de su organización comercial, dado que conjuntamente demandan además la identificación del instrumento por medio del cual hacen llegar sus ofertas en el espacio virtual, nos referimos al *website* de la empresa.¹¹¹

Por consiguiente el PSC requiere efectuar en estos casos un número más amplio de prestaciones adicionales, como por ejemplo servicios de acuse de recibo, sellado temporal, entre otros. Paralelamente le serán solicitados seguramente servicios de certificación de sitios web, firma de códigos y/o visados electrónicos, de los que nos ocupamos con anterioridad en este trabajo e identificamos con la denominación de contratos de certificación especiales, respecto los cuales establecimos que habitualmente se formalizan contractualmente, de forma independiente a los servicios de certificación de firma electrónica.

5.3.2. Por la categoría de firma electrónica que contiene el certificado.-

Por otra parte, los servicios de certificación de firma electrónica se pueden clasificar atendiendo a la categoría de firma electrónica que contiene el certificado, del modo expuesto a continuación:

¹¹¹ Al respecto consultar (J. F. Ortega, 2008:181-182).

a) Certificados de firmas electrónicas simples.-

Este tipo de certificados respaldan firmas electrónicas simples o sencillas, que no son otra cosa que un conjunto de datos en forma electrónica consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante (art. 3.1. LFE y art. 2.1. DFE), pero que no ofrecen ningún tipo adicional de garantía de seguridad.

b) Certificados de firmas electrónicas avanzadas.-

Esta categoría de certificados se basan en firmas electrónicas avanzadas, que son aquellas que permiten identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que están vinculadas al firmante de manera única y a los datos a que se refiere y que han sido creadas por medios que el firmante puede mantener bajo su exclusivo control (art. 3.2. LFE y art. 2.2. DFE).

Este tipo de firmas si bien permiten una identificación segura de su titular, evidentemente no reúnen los requisitos para dotar a la firma electrónica de efectos jurídicos completos y plenos. El nivel de seguridad proporcionado en este caso es intermedio, entre el certificado basado en una firma electrónica sencilla y una firma electrónica reconocida.

c) Certificados de firmas electrónicas reconocidas.-

La firma electrónica reconocida es aquella firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma (art. 3.3. LFE y art. 2.10. DFE). Esta categoría de firmas además de identificar de manera indubitable a su titular, dotan a la firma de plenos efectos jurídicos, lo que se conoce como equivalente funcional.

5.3.3. Por la naturaleza del PSC que emite el certificado.-

Asimismo, los servicios de certificación de firma electrónica se pueden clasificar atendiendo a la naturaleza del PSC que emite el certificado, de la manera siguiente:

a) Persona física o jurídica.-

De conformidad con el art. 2.2. LFE, se denomina prestador de servicios de certificación a la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Al respecto cabe hacer notar, que si bien la LFE concibe al PSC de un modo amplio, es decir como persona física o jurídica, la realidad del tráfico demuestra que prácticamente en todos los casos los PSC revisten la categoría de personas jurídicas. Entendemos que ello es así debido a las fuertes inversiones que representa montar una infraestructura para prestar el servicio, sumado a la complejidad técnica del mismo, por lo cual será poco probable encontrar en el mercado a una persona física que proporcione servicios de certificación.

b) Persona de derecho público o privado.-

Siguiendo la concepción amplia del art. 2.2. LFE, el PSC puede también revestir la categoría de persona de derecho público o privado. En el primer supuesto, serán las instituciones y organismos públicos quienes operen como PSC en el ámbito de su jurisdicción y competencia, para avalar las comunicaciones y transferencias electrónicas de información, ya sea aquellas que se verifiquen al interior de la administración, como aquellas que se llevan a cabo entre el ciudadano y la administración o viceversa.¹¹² En España se tiene por ejemplo a la Fábrica Nacional de la Moneda y Timbre-Real Casa de la Moneda (FNMT-RCM) y el Ministerio del Interior, concretamente la Dirección General de la Policía, esta última encargada de la emisión de certificados reconocidos de firma electrónica para que se incorporen al DNI electrónico (DNI-e).¹¹³

¹¹² En ese sentido se pronuncia la DFE cuando entre sus considerandos expresa: “*Los servicios de certificación pueden ser prestados...por entidades públicas... cuando así se establezca de acuerdo con el Derecho nacional.*”

¹¹³ Efectivamente, en España la Dirección General de Policía se ha constituido en PSC público mediante RD 1553/2005, de 23 de diciembre, por el que se regula la expedición del DNI-e y sus certificados de firma electrónica (BOE nº 307, de 24 de diciembre de 2005).

En el caso de personas de derecho privado, como se tiene previamente señalado, normalmente serán personas jurídicas las que operan como PSC, más concretamente empresas constituidas como sociedades mercantiles y otras como asociaciones.¹¹⁴

c) PSC certificado o no certificado técnicamente.-

De conformidad con el art. 26.1. LFE, la certificación de un PSC constituye un procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un PSC, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público.¹¹⁵

De esta forma, es posible diferenciar en el mercado PSC certificados o acreditados de aquellos que no cuentan con certificación alguna para prestar sus servicios. En todo caso, debe quedar claro que la certificación de un PSC no es necesaria para reconocer eficacia jurídica a una firma electrónica (art. 26.4. LFE), aunque es indudable que los clientes optaran en la mayoría de los casos por contratar los servicios de un PSC certificado, en el entendido que ofrece mayores garantías de fiabilidad y seguridad en la prestación de sus servicios.

¹¹⁴ La coexistencia de los certificadores de orden público y privado conlleva la preocupación de que éstos ingresen en una dinámica de abierta competición en el mercado. Por ejemplo, en el ámbito europeo en general y español en particular, rigen los principios de “no autorización previa” y “libre competencia” para la prestación de servicios de certificación de firma electrónica. No obstante en criterio de Martínez, dados los principios que inspiran el ordenamiento comunitario, y en los que se basa el derecho español, es dudoso que ello sea posible o factible (A. Martínez; 2004: 108) // Precisamente la implementación del DNI-e ha sido uno de los aspectos que mayores y sendos debates ha generado en España, puesto que si bien su mayor utilidad radica en la posibilidad de su empleo de manera general ante cualquier administración, con el consiguiente beneficio de que se sustrae al ciudadano de tener que obtener un certificado asociado a un par de claves para las distintas reparticiones de la administración con las que se relaciona electrónicamente, su mayor cuestionamiento viene de la mano de un posible uso generalizado, no solo a fines administrativos, sino a fines comerciales del DNI-e, lo que representaría un serio problema para las empresas privadas que se dedican a prestar servicios de certificación, con el riesgo de salir *de facto* del mercado, puesto que si el ciudadano puede acceder a certificados gratuitos contenidos en el DNI-e, igualmente seguros y fiables a los que obtendría de un PSC privado nos cuestionamos nosotros ¿a qué objeto acudiría a estos últimos, quienes además le cobran un precio por sus servicios?. En este sentido también opina Martínez (A. Martínez, 2004: 250-251) // A nuestro juicio, todo dependerá de la interpretación (amplia o restrictiva) que se haga del contenido plasmado en el art. 15 de la LFE, para lo cual, consideramos que se debe sopesar de un lado, los principios legales de orden comunitario que consagran la libre competencia en el mercado de los servicios de certificación y, por el otro, las normas y principios que hacen a la leal competencia en el mercado. Para ello se deberá tomar en cuenta fundamentalmente las siguientes normas: el art. 38 de la Constitución Española, que consagra expresamente el ejercicio de la libertad de empresa, siendo la competencia, como principio rector de toda economía de mercado, la forma más importante en que se manifiesta dicha libertad; por lo cual, habrán ser consideradas las disposiciones de la Ley 16/1989, de 17 de julio, de Defensa de la Competencia, mismas que prohíben una serie de prácticas por considerarlas contrarias a la libre competencia, entre ellas, se prohíbe el abuso de posición dominante, que podrá consistir, entre otras, en la aplicación en las relaciones comerciales o de servicios, de condiciones desiguales para prestaciones equivalentes, que coloquen a unos competidores en situación desventajosa frente a otros. En todo caso, desde nuestro punto de vista, se debe efectuar una interpretación restrictiva del art. 15 de la LFE, ya que en caso contrario, podría presentarse el hecho que la Administración constituya un monopolio *de facto* en el mercado de la certificación, situación por demás asintomática y paradójica, toda vez que se supone que son los poderes públicos los llamados a garantizar y proteger el ejercicio pleno de la libertad de empresa, y por ende, de la competencia sana en el mercado.

¹¹⁵ La LFE al respecto establece en su art. 26.2. lo siguiente: La certificación de un prestador de servicios de certificación podrá ser solicitada por éste y podrá llevarse a cabo, entre otras, por entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo. Más adelante, el art. 26.3. señala: En los procedimientos de certificación podrán utilizarse normas técnicas u otros criterios de certificación adecuados. En caso de utilizarse normas técnicas, se emplearán preferentemente aquellas que gocen de amplio reconocimiento aprobadas por organismos de normalización europeos y, en su defecto, otras normas internacionales o españolas.

5.3.4. Por el ámbito territorial en que se presta el servicio.-

Finalmente es posible clasificar los servicios de certificación de firma electrónica desde el punto de vista territorial en que se presta el servicio. Así, se diferencia entre prestación de servicios en el ámbito nacional español, a nivel intracomunitario e internacional o extracomunitario.

a) Nacional.-

La prestación de servicios de certificación a nivel nacional no debiera en principio plantear mayores dificultades, ya que desde la esfera del titular del certificado, la confianza que le ofrezca el PSC dependerá de si nos encontramos ante un PSC de naturaleza privada o pública y de si éste cuenta o no con una certificación (acreditación). En el primer supuesto, existen diversas modalidades para obtener información sobre el PSC según el tipo de persona de que se trate, en el caso de una sociedad de capital será muy sencillo obtener información acudiendo al Registro Mercantil. En el segundo caso, si el PSC tiene carácter jurídico-público, no se generan mayores problemas de confianza en la prestación del servicio, dada la condición pública del PSC.

b) Intracomunitario.-

Al interior de la Unión Europea son cada vez más frecuentes las transmisiones electrónicas de mensajes de datos en el territorio comunitario, razón por la que resulta fundamental la correcta aplicación de la cláusula de mercado interior en relación con la actividad que despliegan los PSC, aspecto que estudiaremos con mayor detenimiento en el Capítulo III de esta investigación. De hecho, el correcto funcionamiento de procedimientos de reconocimiento mutuo de certificados constituye la base fundamental del mercado interior de los servicios de certificación electrónica.

c) Internacional.-

Finalmente la prestación de servicios de certificación de firma electrónica a nivel internacional o extracomunitario resultan de mucha importancia, en el entendido que la globalización de los mercados representa el surgimiento de múltiples relaciones comerciales con terceros países, particularmente con el continente americano, por lo que resulta prioritario establecer y reforzar los mecanismos de reconocimiento internacional mutuo de certificados.

VI. Descripción general del contenido contractual.-

Llegados a este punto, nuestro interés se concentrará a continuación en efectuar una descripción global y general del contenido más habitual del contrato de certificación reconocida de firma electrónica, atendiendo al análisis de los contratos que se presentan en el tráfico, identificando a grosso modo de momento, las prestaciones principales, adicionales y accesorias de cada una de las partes contractuales, marco global a partir del cual se nos facilitará la tarea posterior de identificar los caracteres del contrato objeto de nuestro estudio así como el régimen jurídico que le resulta aplicable.

La descripción que efectuaremos será por tanto eminentemente práctica, es a partir de su observación que conformaremos la disciplina jurídica de este contrato; en todo caso, como quiera que existen una amplia variedad de contratos de certificación resulta imposible describir todas las prestaciones con las que podemos encontrarnos, razón por la que nos detendremos en el análisis de las prestaciones más habituales y que se repiten en todos los contratos de certificación reconocida.

6.1. Descripción de las prestaciones propias del PSC.-

6.1.1. Obligación preliminar.-

El PSC tiene la obligación con carácter preliminar a ofrecer sus servicios en el mercado, de elaborar unos documentos denominados Declaración de Prácticas y Políticas de

Certificación (DPC), debiendo ponerlos a disposición del público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

6.1.2. Obligaciones principales.-

El PSC posee dos prestaciones absolutamente necesarias o fundamentales, que se repiten en todos los contratos de certificación reconocida, a saber:

a) Sin duda alguna su primerísima prestación consiste en emitir y poner a disposición el certificado reconocido a favor de su cliente, el Firmante/Suscriptor.

b) La segunda prestación básica e indisolublemente ligada con la anterior, consiste en publicar los certificados manteniendo un directorio actualizado de consulta pública que refleje su estado (vigente, suspendido o extinguido), garantizando un servicio de verificación o validación de los mismos.

6.1.3. Obligaciones específicas para emitir certificados reconocidos.-

6.1.3.1. Previas a la emisión del certificado reconocido.-

a) Con carácter previo a la emisión del certificado reconocido, debe proceder a comprobar de manera indubitable la identidad del solicitante y futuro Firmante/Suscriptor, procediendo a su registro ya sea de manera directa, ya sea a través de la Entidad de Registro (ER) delegada por el propio PSC.

b) Debe igualmente asegurarse de la exactitud de la información que posee el certificado.

c) Cerciorarse de la efectiva posesión por parte del Firmante/Suscriptor del juego de claves: pública y privada.

d) Cuando el propio PSC genera el juego de claves, debe además garantizar su complementariedad.

6.1.3.2. A tiempo de emitir el certificado reconocido.-

a) A tiempo de emitir el certificado reconocido el PSC se encuentra obligado a constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros, a objeto de afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expiden.

b) Debe demostrar la fiabilidad necesaria para prestar servicios de certificación.

c) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.

d) Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.

e) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.

f) Tomar medidas contra la falsificación de certificados y, en el caso de que el PSC genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.

g) 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.

h) Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan

su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

6.1.4. Obligaciones adicionales.-

a) Una de las obligaciones adicionales del PSC consiste en administrar los servicios de extinción y suspensión de certificados.

b) Proporcionar cierta información con carácter previo a la emisión del certificado reconocido. En ese entendido debe informar mínimamente sobre los siguientes aspectos:

1) Las obligaciones del firmante; la forma en que han de custodiarse los datos de creación de firma; el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica, que sean compatibles con los datos de firma y con el certificado expedido; 2) Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo; 3) El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado; 4) Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial; 5) Las certificaciones que haya obtenido, en su caso, el PSC así como los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad; 6) Las demás informaciones contenidas en la DPC.

c) Asegurar la Protección de datos personales del Firmante/Suscriptor. En ese sentido el manejo de los datos recabados deben adecuarse a las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LPDPCP) y en sus normas de desarrollo.

d) No almacenar ni copiar los datos de creación de firma del Firmante/Suscriptor por motivos de seguridad, a objeto que se prevenga la utilización maliciosa por un tercero que disponga de una copia de la misma.

e) Cuando acontecen las circunstancias en que el PSC cesará en el ejercicio de sus actividades como certificador, ya sea por razones voluntarias (v.gr. disolución de la empresa por acuerdo de los socios) o incluso involuntarias (v.gr. quiebra de la empresa), tiene una doble obligación de comunicación del cese de actividad: por una parte, a los Firmante/Suscriptores (que prevista en el contrato constituye una obligación contractual) y, por otra, al Ministerio de Ciencia y Tecnología (la cual reviste la categoría de obligación legal) de forma respectiva.

6.1.5. Obligaciones accesorias.-

Dentro de las obligaciones accesorias del PSC, figuran otras prestaciones que eventualmente se pueden contratar. De hecho, el art. 2. LFE define al PSC como “*la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica*”¹¹⁶ (las negrillas son nuestras).

El PSC en consecuencia puede prestar diferentes servicios, aunque lógicamente su función básica es la emisión de certificados. La ley no obstante, deja abierta la posibilidad de que los PSC no expidan certificados al público sino que presten otros servicios en relación con la firma electrónica.

Para nuestro estudio nos concentraremos en los siguientes servicios accesorios: cuando el Firmante/Suscriptor lo ha solicitado, el PSC tiene la obligación de proporcionar el dispositivo criptográfico y el software correspondiente. Asimismo se encuentran los servicios de acuse de recibo y homologación de certificados.

¹¹⁶ La DFE lo define en el art. 2.11 “proveedor de servicios de certificación: la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica”. En tanto que la LMFE establece en su art. 2.e. “Por prestador de servicios de certificación se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas”.

6.2. Descripción de las obligaciones propias del Firmante/Suscriptor.-

6.2.1. Obligación principal.-

La obligación principal del Firmante/Suscriptor consiste en el pago de un precio a cambio del servicio de certificación reconocida contratado. En la mayoría de los casos el precio consistirá en la entrega de una suma de dinero, configurándose por tanto una obligación pecuniaria; el precio quedara fijado unilateralmente por el PSC, debiendo el cliente aceptarlo o rechazar la celebración del contrato.

6.2.2. Obligaciones adicionales.-

El Firmante/Suscriptor se encuentra sometido asimismo a una serie de obligaciones adicionales, entre ellas:

a) Proporcionar toda la información necesaria para realizar una correcta y plena identificación por parte del PSC, misma que debe ser veraz y entregada dentro de los términos fijados para ello.

b) Acudir de manera personal ante el PSC o la ER delegada a objeto de: acreditar y confirmar su identidad así como firmar la Solicitud del certificado reconocido, momento en el que habitualmente además se cumplimenta presencialmente el contrato de certificación reconocida.

c) Conservación diligente de su clave privada (datos de creación de firma), toda vez que junto con la generación y entrega de la misma empleando medios fiables (obligación del PSC), de la custodia segura de la clave privada depende completamente toda la certeza y confiabilidad de un sistema de certificados digitales.

d) Directamente relacionada con la anterior, comunicar al PSC los casos en los que su clave privada se ha puesto en peligro, ha sido extraviada o de cualquier otra manera se ve comprometida.

e) Observar la normativa contenida en la LFE y actuar dentro del marco general proporcionado por la Declaración de Prácticas de Certificación (DPC) constituyen deberes ineludibles del Firmante/Suscriptor, quien además se encuentra llamado a observar y respetar las Políticas de Certificación asociadas al certificado reconocido que solicita.

En ese sentido, la DPC vinculada al certificado acotan las reglas en base a las cuales el Firmante/Suscriptor debe emplear el certificado reconocido, debiendo respetarlas y no encontrándose facultado para dar al certificado un uso distinto del previsto en dichos documentos.

f) En las ocasiones que la información inicialmente proporcionada por el Solicitante para confeccionar el certificado reconocido sufra cambios posteriores, ésta debe ser inmediatamente comunicada al PSC; es decir, se debe notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

g) Cuando los hechos y las circunstancias lo demanden, solicitar al PSC que proceda a suspender o revocar oportunamente el certificado reconocido emitido. En otras palabras, debe informar al PSC a la mayor brevedad posible, de la existencia de algún motivo que comprometa el mantenimiento de la confidencialidad de la clave privada, si es de su conocimiento por supuesto.

h) Abstenerse en todo tipo de uso de su clave privada cuando haya expirado el período de validez del certificado o cuando el PSC le notifique la extinción o suspensión de su vigencia.

i) Los certificados sólo podrán ser empleados dentro de los límites y los usos para los que hayan sido emitidos en cada caso (descritos en las políticas de certificación correspondientes), por lo tanto, el Firmante/Suscriptor tiene la obligación de respetar los límites cuantitativos y cualitativos que figuran en el certificado, así como emplear el

certificado conforme a las condiciones establecidas en la DPC y comunicadas a éste oportunamente por el PSC.

VII. Sinopsis.-

Hasta el momento nos hemos ocupado de efectuar una somera descripción de los antecedentes y nociones generales que hacen a la presente investigación, habiendo efectuado una necesaria delimitación geográfica del ámbito de estudio (a la legislación española y comunitaria europea) así como una circunscripción del objeto de estudio (al contrato de certificación reconocida entre empresarios).

A continuación se ha establecido que la función económica que este contrato reviste es la identificación en - sentido amplio - de los operadores económicos en el tráfico virtual, como requisito imprescindible para generar un entorno seguro, de manera que tanto los consumidores como las empresas puedan tener confianza en que sus transacciones no serán interceptadas, ni modificadas y se tenga la certeza que tanto el comprador y vendedor (emisor y receptor de un mensaje de datos) son efectivamente quienes dicen ser.

Posteriormente se han destacado los elementos que hacen a la práctica comercial del contrato de certificación reconocida, proporcionando inicialmente una aproximación al concepto para luego efectuar su diferenciación de otros contratos de certificación especiales. Acto seguido se ha descrito que los servicios de certificación electrónica, se pueden clasificar atendiendo: ya sea a la categoría de firma electrónica que contiene el certificado; según la naturaleza del PSC que emite el certificado y por último según el ámbito territorial en que se presta el servicio.

Finalmente nos hemos ocupado de efectuar una enumeración descriptiva, global y general - al menos de momento - de las prestaciones habituales del contrato de certificación reconocida, estableciendo las obligaciones principales, específicas, adicionales y accesorias tanto del PSC como del Firmante/Suscriptor, reservando un estudio más pormenorizado de

estas cuestiones para el Capítulo IV de la presente investigación. Ello se justifica en función que el objeto de la tesis es la determinación del régimen jurídico de una práctica comercial que si bien está reconocida legalmente, no está regulada en su totalidad, por lo que hay que ir identificando las normas que se le aplican para la resolución de los problemas que se plantean.

En estas circunstancias conviene desde un primer momento describir esta práctica comercial, identificando las prestaciones más comunes y las que se acompañan en otros supuestos, diferenciando igualmente las que tienen carácter principal y las accesorias así como las que se puedan establecer al hilo del contrato, pero que no son imprescindibles para el mismo. Consideramos que de ese modo se facilitará el entendimiento de la tesis, pues al hacer alusión a las prestaciones estaremos en condiciones de establecer cuáles son las que normalmente se acuerdan y cuáles efectivamente se van a tomar en cuenta durante el desarrollo de nuestro trabajo.

El desafío en nuestro siguiente Capítulo reside en construir el concepto jurídico del contrato de certificación reconocida, establecer los caracteres propios, para finalmente identificar su naturaleza y el régimen jurídico que le resulta aplicable.

CAPÍTULO SEGUNDO

CONCEPTO, CARACTERES Y NATURALEZA JURÍDICA

I. Concepto.-

Luego de efectuar una sintética enunciación de los antecedentes y nociones generales, establecida la función económica y descrita la práctica habitual de la certificación reconocida de firma electrónica, corresponde fijar un concepto más aproximado del contrato objeto de nuestro estudio. En primer lugar, expondremos definiciones que se han dado por parte de algunos autores; posteriormente determinaremos la noción que, a nuestro juicio, resulta más pertinente en base a las obligaciones que surgen del contrato y el fin objetivo que buscan las partes con su celebración.

Con relación a las diversas definiciones que se han ofrecido de este contrato, comenzamos por María Pérez Pereira, quien, si bien omite proporcionar directamente un concepto, explica que:

“El objeto del contrato de certificación es, fundamentalmente, la emisión de certificados de firmas electrónicas...en el contrato de certificación se distinguen dos elementos: el primero, consistente en poner a disposición de la contraparte las herramientas técnicas para que éste pueda generar firmas electrónicas, y segundo, esencial, de certificar las firmas electrónicas generadas a través del certificado que haya emitido. La certificación de firmas se compone, a su vez, de dos pasos: el primero, la generación del certificado, y el segundo su emisión para la utilización por el titular del mismo.”¹¹⁷

En nuestra opinión, sin embargo, este concepto resulta muy amplio, pues con independencia de que en determinados casos se incluyan algunas de las prestaciones

¹¹⁷ (M. Pérez, 2009: 130).

enumeradas por la citada autora, concretamente la obligación del PSC de poner a disposición de la contraparte las herramientas tecnológicas para que éste pueda generar firmas electrónicas, lo cierto es que de conformidad con las disposiciones de la LFE la generación de firmas electrónicas se puede efectuar en un entorno ajeno al PSC.

Evidentemente, el interesado con carácter previo a la fase de presolicitud de un certificado, debe proveerse de la tarjeta criptográfica y del software de generación o importación de los datos de creación y de verificación de firma en la tarjeta. Para ello existen dos opciones: a) que obtenga dichos elementos de un proveedor ajeno al PSC, pero asegurándose que reúnan las características técnicas y de seguridad exigidas por el PSC seleccionado, b) que obtenga dichos elementos del propio PSC.

Debemos destacar también la definición establecida por Juan Francisco Ortega, quien concibe el contrato objeto de estudio del modo siguiente:

“Mediante el contrato de certificación electrónico, de carácter bilateral, oneroso, conmutativo y formalizado, comúnmente, mediante técnica de adhesión, una parte, el prestador de servicios de certificación, se obliga a realizar todas las conductas propias de su actividad, entre las que se encuentra fundamentalmente la expedición de un certificado, dirigidas a identificar, con niveles adecuados de seguridad a la otra parte, a cambio de un precio cierto y determinado”¹¹⁸.

Aunque esta definición resulta más acorde con el contenido propio del contrato de certificación de firma electrónica, como es posible observar se circunscribe - al igual que la noción precedente - a describir tan sólo una, de las dos obligaciones fundamentales del PSC.

En otras palabras, los autores citados resaltan en ambos casos uno de los contenidos principales del contrato de certificación de firma electrónica (generación y emisión del certificado), obviando referirse a la segunda prestación fundamental (habilitar los servicios de

¹¹⁸ (J. F. Ortega, 2008:178).

directorio y verificación del certificado) y otros aspectos del contrato que también resultan relevantes.

Por esta razón creemos conveniente fijar el concepto, que desde nuestro punto de vista, describe de un modo más completo el supuesto contractual ante el que nos encontramos.

Partiendo de la definición inicialmente desarrollada en el Capítulo Primero de esta investigación, adviértase que la misma sigue en su redacción una terminología neutral desde el punto de vista tecnológico, en el entendido que no vincula en sus descripciones a una técnica específica para generar firmas electrónicas, de modo que caben dentro de su concepto cualquier tipo de soluciones técnicas, presentes o futuras (*a condición que reúnan los requisitos establecidos por ley*). Asimismo, dicha definición es aplicable tanto a los servicios de certificación de firma electrónica que se desarrollan en redes cerradas (v.gr. EDI cerrado), como a los que se ejecutan en entornos abiertos de comunicación de datos (v.gr. Internet), independientemente de si existen acuerdos previos para la utilización de firmas electrónicas, o en ausencia de éstos. Por último, resulta aplicable indistintamente a las labores de certificación que respaldan actividades de comercio electrónico, ya sea en sentido amplio o en sentido estricto.

Como quiera a momento de establecer las delimitaciones al ámbito de estudio de este contrato, señalamos que nos circunscribiremos preferentemente al ámbito de los certificados reconocidos (*y por ende de las firmas electrónicas reconocidas*); que se basan en la tecnología asimétrica (*de clave pública*); desplegando sus funciones en redes abiertas (*Internet*); en comunidades que no han celebrado un acuerdo previo para el empleo de firmas electrónicas (*por ende, ofreciendo certificados al público*); y, a las transacciones propiamente de comercio electrónico en sentido estricto, nos parece apropiado afinar aún más el concepto genérico aportado inicialmente, del modo siguiente:

En términos generales podemos establecer que el contrato de certificación de firma electrónica reconocida, es aquel en el que una de las partes (*PSC*) asume la prestación de generar a favor de la otra (*Firmante/Suscriptor*) un certificado reconocido, mediante el cual se acredita la plena identidad del Firmante/Suscriptor a momento de efectuar transacciones comerciales frente a terceros (*sus clientes al mismo tiempo que Usuarios del certificado*) en redes abiertas de comunicación, vinculando de modo seguro la clave privada con la clave pública del Firmante/Suscriptor. Asumiendo el PSC además, las obligaciones de habilitar los servicios de directorio y verificación del certificado así como gestionar su ciclo vital, colocando a disposición todos los componentes tecnológicos que hacen al funcionamiento propio de la Infraestructura de Clave Pública, garantizando con la debida diligencia las funciones características del sistema (*autenticación, integridad, no repudio y confidencialidad*). En tanto que la otra (*Firmante/Suscriptor*), asume la contraprestación de entregar al PSC una cantidad de dinero (*precio cierto y determinado*) por concepto de pago del servicio recibido. Esto constituye el contenido esencial del contrato de certificación reconocida.

Debemos señalar que además de las prestaciones descritas, el PSC incluye habitualmente en el contenido contractual otros servicios accesorios de carácter informático que principalmente se ofrecen para complementar el servicio principal de certificación reconocida. Así, entre los más comunes se encuentran el servicio de datación electrónica o *time stamping*, el servicio de acuse de recibo, el servicio de homologación de certificados, la emisión de los denominados certificados transaccionales¹¹⁹ y los de atributos.¹²⁰ Además, es bastante frecuente que el PSC ofrezca un servicio de atención al cliente.

¹¹⁹ Los certificados transaccionales son definidos como aquellos destinados a una determinada transacción que incorporan por referencia una o más firmas digitales; de manera que es específico para una o más transacciones y las firmas digitales de tales transacciones, estando destinado por consiguiente a ser empleado únicamente para dichas firmas. Este tipo de certificado será útil, p. ej., para una entidad de certificación que ha pactado actuar para una sola transacción, o para un conjunto de transacciones, respecto de las que alguna de las partes o la entidad de certificación no desean aceptar el gran riesgo de un certificado aplicable a un número ilimitado de firmas digitales creadas

La definición apuntada no recoge, sin embargo, las obligaciones adicionales propias del tipo contractual que estudiamos. Éstas constituyen fundamentalmente una manifestación del deber de diligencia que se impone en virtud del contrato celebrado.

Respecto a las obligaciones adicionales del cliente o Firmante/Suscriptor, debemos destacar las siguientes. En primer lugar, debe proporcionar al PSC información fidedigna y veraz sobre su identidad personal. También se obligará a conservar diligentemente su clave privada; usar el certificado según lo establecido en la Declaración de Prácticas y Políticas de Certificación aplicables; comunicar la puesta en peligro o pérdida de su clave privada así como los cambios de la información reflejada en el certificado. Además, deberá solicitar la suspensión o revocación del certificado oportunamente, no debiendo utilizar la clave privada en caso de suspensión o extinción del certificado. Finalmente el Firmante/Suscriptor debe respetar los límites cuantitativos y cualitativos que figuran en el certificado así como las condiciones de su utilización establecidas en la DPC por el PSC.

Por su parte, el PSC se obliga con carácter preliminar a formular una Declaración de Prácticas y Políticas de Certificación. Igualmente está obligado de manera general a no almacenar ni copiar la clave privada (datos de creación de firma) del Firmante/Suscriptor.

Asimismo, el PSC con carácter previo a la emisión de un certificado reconocido debe proporcionar toda la información necesaria, por ejemplo respecto a las características y el precio de sus servicios; comprobar la identidad de los solicitantes; asegurarse de la exactitud de la información que posee el certificado; cerciorarse de la efectiva posesión por parte del Firmante/Suscriptor del par de claves; y, cuando es el propio PSC quien genera el juego de claves, debe garantizar su complementariedad.

durante su período de validez. El certificado transaccional sólo será válido para aquellas firmas digitales incorporadas a él por referencia (A. Martínez, 2001: 315).

¹²⁰ La existencia de los certificados de atributos esta prevista en diversas legislaciones de firma digital. El art. 5 de la Ley alemana de firma digital establece que, previa petición de un solicitante, el certificador registrará información relativa al poder de representación respecto de una tercera parte en el certificado de clave pública o en un certificado de atributos, siempre que el consentimiento de la tercera parte para que el poder de representación sea registrado sea demostrable de forma fiable. Por su parte, el art. 9 del Reglamento italiano establece como obligación del certificador la de especificar, a petición del solicitante, y con el consentimiento del tercero interesado, la existencia de poderes de representación (A. Martínez, 2001: 166). Además, tanto la DFE (Anexo I) como la LFE (art. 13.3.) prevén la inclusión de atributos en los certificados.

Conviene apuntar también que el contrato tendrá habitualmente carácter temporal, de tal forma que suele tener una duración determinada. Además, es frecuente prever su prórroga automática siempre que no se manifieste, por ninguna de las partes contractuales en el momento de vencimiento, su voluntad de no renovarlo.

Este es, fundamentalmente, el contenido que en la práctica presenta el contrato de certificación reconocida de firma electrónica. En este sentido, hemos aportado un concepto principalmente descriptivo del supuesto contractual. No obstante, podemos identificarlo desde un punto de vista jurídico resaltando las características esenciales que lo definen y determinar su naturaleza jurídica, labor en la que nos concentraremos en los próximos apartados.

II. Caracterización.-

Tomando en consideración la descripción que se ha efectuado del contrato de certificación reconocida de firma electrónica, es posible establecer sus características esenciales fijando las principales notas que distinguen al mismo y, de esta forma, encuadrarlo en las distintas categorías habituales de sistematización de los contratos. Dichas características sin duda determinarán la naturaleza y el régimen jurídico aplicable al supuesto contractual estudiado. Para el mencionado propósito, nos limitaremos exclusivamente a los criterios tradicionales de clasificación empleados comúnmente por la doctrina.

2.1. Consensual.-

Con carácter previo y general es pertinente señalar, que hoy en día subsiste en el ámbito académico y jurisprudencial español, un profundo debate respecto de la continuidad o no, y a pesar de la Codificación, de la categoría romana de los contratos reales¹²¹, conforme hace notar Prats Albentosa; quien enfatiza en sentido que una excepción a la regla general de

¹²¹ La categoría romana de contrato real es asignada a Gayo (*Inst.* 3.13.2 y D. 44.7.1). Lorenzo Prats Albentosa, *Préstamo de consumo, Crédito al consumo*, Valencia, Tirant Lo Blanch, 2001, p. 57. // Díez-Picazo explica que la clasificación de los contratos entre reales y consensuales, ha perdido en el derecho moderno gran parte de su valor. La regla general -sustenta el autor- es que los contratos se perfeccionan por el consentimiento, de acuerdo a las reglas contenidas en los arts. 1.254 y 1.258 del C.c., por lo cual, los contratos consensuales configuran la hipótesis normal. Luís Díez-Picazo, *Fundamentos del Derecho Civil Patrimonial*, vol. I, Madrid, Civitas, 1996, 5ª. ed., pp. 139-140.

perfección de los contratos *solo consensu*,¹²² precisa una norma que expresamente la establezca.¹²³

De manera que en el derecho español (*al igual que en el resto de los ordenamientos pertenecientes a la familia jurídica romano-germánica de derechos*) prima el principio del perfeccionamiento de todos los contratos por el mero consentimiento, contenido en el C.c. art. 1.254 “*El contrato existe desde que una o varias personas consienten en obligarse...*” y art. 1.258 “*Los contratos se perfeccionan por el mero consentimiento...*”. Por su parte el art. 51.- del C.com. señala que “*Serán válidos y producirán obligación y acción en juicio los contratos mercantiles, cualesquiera que sean la forma y el idioma en que se celebren, la clase a que correspondan y la cantidad que tengan por objeto, con tal que conste su existencia por alguno de los medios que el Derecho civil tenga establecidos*”.

Considerando que el principio general y codificado para el perfeccionamiento de los contratos es el consentimiento, reflexionamos que el contrato de certificación electrónica reconocida no escapa a dicha regla, máxime si tomamos en cuenta que no será posible encontrar ninguna norma en el C.c. ni en el C.com. que expresamente establezcan una excepción al principio general señalado.

De manera que a nuestro entender, el contrato de servicios de certificación electrónica reconocida tiene naturaleza consensual, la cual, de conformidad con el art. 1.262 C.c. se manifiesta en la coincidencia de voluntades (*concurso de la oferta y la aceptación*) entre el Firmante/Suscriptor y el PSC sobre el objeto y causa contractual, o más específicamente, con la adhesión del Firmante/Suscriptor al contenido contractual pre-redactado por el PSC.¹²⁴

¹²² Los contratos consensuales son aquellos que se perfeccionan por el mero consentimiento de las partes. Frente a éstos, se encuentran los denominados contratos formales, en los que se exige la observancia de una forma determinada de manifestación de las voluntades negociales para su validez. Por otro lado, se encuentra la categoría de los contratos reales en los que es necesario, para su perfección, la entrega de la cosa objeto del contrato. Existen, sin embargo casos, en los que sí se exige una forma determinada para la validez del contrato. Así, por ejemplo, en el Código Civil, el art. 633, para las donaciones de bienes inmuebles, el art. 1.628 para el censo enfiteútico o el art. 1.875 para el contrato constitutivo del derecho real de hipoteca. Véase sobre esta cuestión (L. Díez-Picazo, 1996: 139-140).

¹²³ (L. Prats, 2001: 57-59).

¹²⁴ En los instrumentos europeos de unificación del Derecho de contratos también se encuentra expresamente formulado. Así, en el art. 2.101(2) de los Principios del Derecho Europeo de Contratos (por sus siglas en inglés PECL) se establece expresamente que “el contrato no necesariamente se debe concluir ni hacer constar por escrito y no queda sujeto a ninguna otra exigencia de forma. Se puede probar su existencia por todos los medios posibles, incluida la prueba testifical”. Igualmente en los Principios UNIDROIT sobre Contratos

2.2. Mercantil.-

La determinación de la naturaleza de los contratos que se desarrollan en el ámbito jurídico enfrenta la problemática de la convivencia de una legislación civil con otra mercantil. En el caso de los contratos típicos, lo que ocurre normalmente es que la propia norma establece si el contrato se halla sometido a las reglas del derecho civil o por el contrario a las del derecho mercantil; mas tratándose de contratos atípicos, dilucidar sobre esta cuestión representa un desafío adicional toda vez que dependiendo del encajamiento del contrato en una u otra normativa, el régimen jurídico aplicable diferirá y, por consecuencia, determinará su naturaleza jurídica.¹²⁵

El art. 2 de la LFE establece que el PSC puede ser una persona física o jurídica, sobreentendiéndose en consecuencia por la amplitud de los términos, que dicha persona además, puede desenvolverse en el ámbito del derecho público o privado. Ahora bien, ya sea que se traten de personas físicas o jurídicas, de derecho público o privado, las normas jurídicas que regirán el contrato de certificación reconocida serán, o bien las comprendidas en el Código civil, o en su defecto, las dispuestas en el Código de comercio.

En principio es un contrato civil, por lo que le resultan aplicables todas las disposiciones generales que hacen al derecho de obligaciones y contratos (arts. 1.088-1.314 C.c.), asimismo, las disposiciones particulares y que le resulten aplicables del arrendamiento (arts. 1.542-1.545; 1.583-1.600 C.c.).

Pero debemos considerar que si en la ejecución del contrato de certificación reconocida participan empresarios, atendiendo a los criterios subjetivos como objetivos previstos en la normativa mercantil, entonces son de aplicación a este contrato las normas mercantiles. De manera que si tanto el PSC como el Firmante/Suscriptor revisten la categoría

Comerciales Internacionales (PUNIDROIT), en el art. 1.2: "Nada de lo expresado en estos Principios requiere que un contrato, declaración o acto alguno deba ser celebrado o probado conforme a una forma en particular. El contrato puede ser probado por cualquier medio, incluidos los testigos". Asimismo en la Convención de Viena sobre Compraventa Internacional de Mercaderías de 1980 (CVCIM), se dispone expresamente en su art. 11 que "El contrato de compraventa no tendrá que celebrarse ni probarse por escrito ni estará sujeto a ningún otro requisito de forma. Podrá probarse por cualquier medio, incluso por testigos".

¹²⁵ (J. Vega, 2002: 72).

de empresarios, la doctrina a tal respecto uniformemente viene calificando al contrato de certificación reconocida como un contrato mercantil, habida cuenta de que se trata de un contrato que, si bien resulta atípico legalmente, se lleva a cabo entre empresarios.¹²⁶

En este caso anticipábamos debe calificarse como contrato mercantil, tanto si consideramos los criterios subjetivos como si nos basamos, sobre todo, en criterios objetivos de clasificación. Partiendo de criterios subjetivos debemos analizar que los contratos de certificación reconocida, cuando participan empresarios en su ejecución, tienen su génesis y se despliegan en el medio empresarial, constituyendo por ende un contrato inter-profesional que ha surgido en auxilio de las actividades de los agentes económicos que intervienen en su perfeccionamiento y ejecución.

Desde ese punto de vista, resulta evidente que son los empresarios con sus prácticas quienes le confieren existencia, al mismo tiempo que emplean la certificación reconocida para el despliegue de sus actividades profesionales mercantiles. Con todo, hay que tener en cuenta que se asume la presunción de que los sujetos que participan en la celebración y ejecución de esta clase de contrato cuentan con un nivel medio de cualificación, aspecto que contribuye a reforzar aun más la tesis sobre la naturaleza profesional de este negocio jurídico.

De otra parte, bajo el prisma de análisis objetivo debemos convenir que el Derecho español no pertenece a un sistema objetivo puro, razón por la cual a momento de circunscribir la materia mercantil corresponde acudir a dos criterios complementarios: el criterio de la inclusión y el de la analogía.¹²⁷ En ese entendido, resultan siendo actos de comercio los contemplados en el Código de Comercio o en leyes especiales mercantiles, y cualesquiera otros de naturaleza análoga (art. 2.2 C.com.).¹²⁸

El criterio de la inclusión no resulta de mucha ayuda en este caso debido a la ausencia

¹²⁶ (M. Pérez, 2009: 269).

¹²⁷ (José A. Vega, 2002: 73).

¹²⁸ El art. 2 del C.com. establece: "Los actos de comercio, sean o no comerciantes los que los ejecuten, y estén o no especificados en este Código, se regirán por las disposiciones contenidas en él; en su defecto, por los usos del comercio observados generalmente en cada plaza; y a falta de ambas reglas, por las del Derecho común. Serán reputados actos de comercio los comprendidos en este Código y cualesquiera otros de naturaleza análoga".

de leyes especiales mercantiles sobre la materia, por lo que únicamente resta acudir al criterio de analogía, de donde se desprende que a dicho fin, el contrato de certificación reconocida celebrado entre empresarios, se encuentra imbuido de las particularidades que han valido para conceptuar como mercantiles a los contratos contenidos en la ley mercantil, o si se prefiere, para reputarlo como un acto propio de la organización instaurada y prolongadamente depurada por el empresario.

Concebida la certificación reconocida como un acto de comercio y debido a su ausencia de regulación, el empleo de la legislación mercantil a este contrato se materializa con asistencia del recurso de la cláusula de analogía, el cual se halla contenido en el artículo 2.2 del C.com.

Los efectos que devienen de esta calificación son de una parte, la sujeción del contrato de manera principal a las normas contenidas en los arts. 50 y ss. del C.com., debido a que en éstos se contienen las disposiciones generales que hacen al derecho de obligaciones y contratos comerciales, y de otra, la sujeción supletoria a las reglas del Derecho común, dentro las cuales caben las del Derecho civil.¹²⁹

2.3. Bilateral - sinalagmático.-

Conforme enseña la doctrina un contrato constituye siempre un negocio jurídico bilateral o plurilateral, debido a que para su perfeccionamiento han concurrido la declaración de dos o más voluntades respectivamente. En ese entendido, cuando se habla de la existencia de contratos unilaterales o bilaterales, no se alude en este caso al número de partes contractuales sino al número de obligaciones que el contrato crea, por consiguiente, resultan siendo unilaterales los contratos que crean obligaciones para una sola de las partes contratantes, como por ejemplo en el caso de mutuo.

En cambio constituyen contratos bilaterales o sinalagmáticos aquellos en que las

¹²⁹ Al respecto es necesario hacer notar que la doctrina contemporánea española viene cada vez con más fuerza propugnando la unificación del derecho privado, es decir, la fusión del derecho civil y comercial en un solo cuerpo normativo. Sobre el tema recomendamos consultar el trabajo de E. Beltran, quien efectúa un estudio muy analítico sobre la materia y termina justificando muy elocuentemente esta solución. Emilio Beltrán Sánchez, *La unificación del derecho privado*, Madrid, Consejo General del Notariado, 1995, p. 9 y ss..

obligaciones son recíprocas.¹³⁰ La bilateralidad consiste en que cada una de las partes contratantes es simultáneamente acreedora y deudora de la otra de distintas prestaciones, por lo que cada parte tiene derecho y acción para exigir de la contraparte la prestación que debe, especialmente si ha cumplido su obligación en tiempo y forma.¹³¹

Consideramos que la certificación reconocida se acomoda plenamente dentro de esta última modalidad, debido a que tanto el PSC como el Firmante/Suscriptor se reatan a efectuar las contraprestaciones convenidas en el instante determinado previamente.¹³² Lo que sucede es que concurre una causa recíproca o mejor dicho una interdependencia entre las prestaciones de las partes contractuales, de tal forma que cada una de estas prestaciones opera como contravalor de la otra.¹³³

Los efectos que devienen de la calificación como contrato sinalagmático residen primero, en el hecho que las prestaciones de una y otra parte deben realizarse simultáneamente, siempre que no se haya establecido pacto diverso.

Segundo, en caso que una de las partes tenga la expectativa de reclamar el cumplimiento del contrato sin que medie contraprestación, la contraparte se encuentra facultada para plantear la “*exceptio non adimpleti contractus*”¹³⁴ (cuya base legal reside en el apartado último del art. 1.100 Cc.), en el entendido de que en los contratos con obligaciones mutuas, ninguna de las partes incide en mora si la otra no cumple apropiadamente lo que le corresponde.¹³⁵

Tercero, debido a la simultaneidad pregonada, el incumplimiento de la prestación por

¹³⁰ Walter Kaune Arteaga, *Teoría general de los contratos*, 4ª ed., La Paz, Temis, 1996, pp. 44-45.

¹³¹ Conforme sostiene Josserand, el contrato bilateral se caracteriza por desempeñar cada una de las partes el doble papel de acreedor y deudor. Josserand, *Derecho Civil*, vol. I, Buenos Aires, 1950, pp. 21-22.

¹³² Los rasgos más peculiares de los contratos bilaterales se refieren a la manera de producirse la mora del obligado (arts. 63 C.com. y 1.100 C.c.), a la llamada resolución por incumplimiento (art. 1.124 C.c.) y a la excepción de contrato no cumplido (art. 1.100, párrafo último C.c.). José Puig Brutau, *Fundamentos de Derecho Civil*, vol. I, Barcelona, Bosch, 1978, p. 444.

¹³³ (L. Díez-Picazo, 1996: 140-141).

¹³⁴ (W. Kaune, 1996: 45).

¹³⁵ El apartado último del art. 1.100 Cc. establece que “*En las obligaciones recíprocas ninguno de los obligados incurre en mora si el otro no cumple o no se allana a cumplir debidamente lo que le incumbe...*” Ello quiere decir, que cuando una de las partes contractuales demanda de la otra el cumplimiento de su obligación pero sin haber ejecutado primero la suya, el demandado puede enervar la acción del actor interponiendo la excepción procesal a la que hacemos referencia, denominada *exceptio non adimpleti contractus*, que en otras palabras significa: cumple tu primero para que yo cumpla después.

una de las partes acarreará como consecuencia la compensación de mora (art. 1.100 C.c.).¹³⁶

Finalmente, cabe señalar que en los contratos sinalagmáticos resulta de aplicación la resolución contractual (art. 1.124 Cc.) cuando se produce el incumplimiento de los términos pactados por alguna de las partes.¹³⁷ En todo caso, debido a que los contratos de certificación reconocida se presentan con un clausulado estandarizado - ya que el Firmante/Suscriptor se adhiere a contratos tipo - deberemos tomar en cuenta lo estipulado en el documento contractual.

2.4. Oneroso - conmutativo.-

El criterio de clasificación de los contratos que efectúa la doctrina de acuerdo al contenido de los mismos y en base al fin perseguido por las partes, determina que existan negocios jurídicos onerosos y gratuitos.¹³⁸ Se reputan como onerosos a los negocios en los que ambas partes se procuran un beneficio patrimonial, asumiendo por su parte un sacrificio también patrimonial. Frente a éstos se encuentran los negocios gratuitos, en los que una de las partes procura una ventaja patrimonial para la otra sin recibir nada a cambio.¹³⁹

Analizadas así las cosas, a nuestro entender la certificación reconocida resulta configurándose como un contrato oneroso, en el entendido que ambas partes realizan un sacrificio patrimonial a cambio de la ventaja que se procuran. De esta manera, el PSC realiza a favor del Firmante/Suscriptor el servicio consistente en certificar la firma electrónica del titular, publicando el certificado reconocido en un directorio de acceso público en la red y habilitando un servicio para su verificación, lo que conlleva sin duda alguna, la realización de sacrificios patrimoniales en orden a adquirir la tecnología necesaria y contratar al personal debidamente cualificado para llevar a cabo dicho servicio. Por su parte el cliente o

¹³⁶ El art. 1.100 Cc. dispone “*Incurrer en mora los obligados a entregar o a hacer alguna cosa desde que el acreedor les exija judicial o extrajudicialmente el cumplimiento de su obligación....Desde que uno de los obligados cumple su obligación, empieza la mora para el otro*”.

¹³⁷ El art. 1.124 Cc. señala “*...El perjudicado podrá escoger entre exigir el cumplimiento o la resolución de la obligación, con el resarcimiento de daños y abono de intereses en ambos casos. También podrá pedir la resolución, aun después de haber optado por el cumplimiento, cuando éste resultare imposible.*”

¹³⁸ (W. Kaune, 1996: 53-58).

¹³⁹ (L. Díez-Picazo, 1996: 81-84).

Firmante/Suscriptor, de igual modo efectúa un desplazamiento patrimonial a favor del PSC a través del pago de la suma de dinero acordada.

A su vez, los contratos onerosos se sub-clasifican en conmutativos y aleatorios, correspondiendo a la primera categoría *“todos aquellos en los que cada una de las partes tiene en cuenta la adquisición de un equivalente de su prestación, pecuniariamente apreciable, y bien determinado o determinable, en su caso, desde el momento mismo de la celebración del contrato”*.¹⁴⁰ En tanto que se reputan como contratos aleatorios aquellos en que *“...las partes no conocen de antemano las ventajas o pérdidas que obtendrán, porque las mismas no son apreciables en el momento de la formación del contrato, toda vez que dependen de un acontecimiento futuro e incierto...”*.¹⁴¹

Si bien es evidente que existe un cierto aspecto de aleatoriedad en el contrato de certificación reconocida, en la medida que una de las partes puede resultar perjudicada,¹⁴² consideramos que no por esta circunstancia se despoja de su carácter de conmutativo, a pesar que exista riesgo de pérdida para alguno de los contratantes, debido a que para concebirse como aleatorio, correspondería hacer alusión al *“aleas”* del negocio jurídico en su conjunto, más no únicamente a un factor de exigua incidencia respecto del total, y en estos contratos no se presenta el acontecimiento incierto contemplado por el art. 1.790 del C.c..¹⁴³

2.5. Relación obligatoria duradera de tracto continuo.-

La doctrina moderna distingue entre obligaciones instantáneas y obligaciones duraderas. Las obligaciones instantáneas son aquellas en las que la prestación se agota en un solo acto, mientras que en las obligaciones duraderas el deudor debe realizar un

¹⁴⁰ Román Sánchez, *Estudios de Derecho Civil*, IV, Madrid, p. 395. En el mismo sentido (W. Kaune, 1996: 57).

¹⁴¹ (W. Kaune, 1996: 57).

¹⁴² Por ejemplo en el caso del Firmante/Suscriptor, puede resultar perjudicado en ocasión del quebrantamiento de la seguridad del sistema tecnológico por parte de un tercero (v.gr. un hacker), quien a pesar de todas las medidas diligentes de seguridad adoptadas por el PSC, suplante al Firmante/Suscriptor y haciéndose pasar por éste celebre negocios electrónicos en perjuicio del titular de firma y del certificado.

¹⁴³ El principal interés de la distinción entre contratos conmutativos y aleatorios estriba en que, por regla general, los contratos aleatorios son refractarios a la rescisión por causa de lesión, ya que en caso de que pudiera plantearse alguna alteración de las contraprestaciones, encontraría la posibilidad, de resolución o rescisión en otra causa, v.gr.: error (Josserand, 1950: 29). No obstante debemos considerar que en la actualidad, teniendo en cuenta el principio de autonomía de la voluntad y la libertad contractual, la lesión económica en sí, no está admitida como causa de resolución o rescisión de los contratos.

comportamiento (o una abstención) permanente y prolongado en el tiempo. A su vez, dentro de las obligaciones duraderas se han distinguido las denominadas obligaciones continuadas y las de ejecución periódica. En las primeras, se exige la conducta o abstención de forma permanente, mientras que en las segundas, se requiere la realización de actos de idéntica naturaleza y de contenido homogéneo, pero separados por periodos de tiempo determinados.¹⁴⁴

Desde nuestro punto de vista la obligación principal del PSC se configura como una obligación duradera, pues obliga al mantenimiento de una situación durante toda la vigencia del contrato, esta es, la certificación de firma electrónica y publicación del estado del certificado reconocido en un directorio, junto a la habilitación de un servicio de verificación.

Teniendo en cuenta que la obligación del PSC es la que caracteriza y le da sentido al contrato de certificación reconocida, lo podemos calificar además como de tracto continuo. Esta calificación tiene una importante consecuencia práctica en orden a la resolución por incumplimiento del art. 1.124 C.c., toda vez que en los contratos de tracto continuo esta resolución no tiene efectos retroactivos sino que, con ella, se pone fin a la relación sin que las partes deban restituirse las prestaciones realizadas.¹⁴⁵

Efectivamente, el contrato de certificación reconocida normalmente no concluye con la ejecución de una sola de las obligaciones, por el contrario, comprende encadenadas prestaciones las cuales van plasmándose a lo largo del tiempo de vigencia del certificado reconocido y por consecuencia del contrato. En ese entendido no dan lugar a obligaciones instantáneas sino duraderas, las cuales como hemos referido se materializan en las distintas etapas de vigencia de un certificado (emisión, publicación en un directorio, suspensión, revocación, extinción).¹⁴⁶

¹⁴⁴ (Walter Kaune, 1996: 59).

¹⁴⁵ El art. 1.124 C.c. establece que “*La facultad de resolver las obligaciones se entiende implícita en las recíprocas, para el caso de que uno de los obligados no cumpliere lo que le incumbe...*”

¹⁴⁶ Sobre contratos de tracto único o sucesivo, puede consultarse (W. Kaune, 1996: 59).

Tampoco estamos en presencia de un contrato con duración indefinida, en el que cada prestación puede ser concebida en cierta medida como autónoma de las restantes. Por consiguiente debemos razonar que la certificación reconocida constituye un contrato único que comprende variadas prestaciones, todas ellas interdependientes entre sí, cuyo plazo de duración se encuentra previamente fijado en el mismo contrato, y en caso de ausencia de previsión pactada al respecto, su duración máxima está fijada por disposición de la norma, la cual estipula un plazo de validez de los certificados reconocidos de hasta cuatro (4) años (art. 8.2. LFE).

En base a un análisis estrictamente teórico, si se fijara un solo plazo de vencimiento para la ejecución de las distintas prestaciones, hablaríamos de la existencia de obligaciones instantáneas. En el caso que esta hipótesis sea factible, debemos convenir que en la ejecución de los contratos de certificación reconocida no es posible dar cabida a este supuesto, toda vez que quebrantaría con ello su principal propósito; por consiguiente, debemos concluir que, con carácter general, la certificación reconocida se configura como una relación obligatoria duradera y de tracto continuo, aspectos que denotan una característica distintiva del mismo.

2.6. Sujeto a condiciones generales, perfeccionado por adhesión.-

La doctrina enseña que las etapas en el *íter* de un contrato son básicamente dos: la fase de preparación o formación y la fase de ejecución. Asimismo se dice que la formación de un contrato es instantánea, cuando se efectúa en un solo acto por parte de los otorgantes sin que exista ningún otro acto previo; en tanto que el contrato es de formación sucesiva, cuando existe un período de tiempo durante la fase de preparación, en el cual las partes primeramente toman contacto, negocian algunos aspectos, redactan borradores de contrato, etc. por lo que el contrato se va formando *ex intervallo temporis*.¹⁴⁷

En este último supuesto, evidentemente la formación del contrato no es consecuencia de un acto único sino de varios actos interconectados, en los que inclusive es posible la

¹⁴⁷ (L. Díez-Picazo, 1996: 269 y ss.)

intervención no sólo de las partes sino de otras terceras personas que cooperan con los contratantes a objeto de concretar el negocio jurídico.¹⁴⁸

En general existen cinco procedimientos típicos en la formación de un contrato, a saber: i) a través de una fase previa de sondeos y deliberaciones; ii) por la concurrencia de una oferta y una aceptación; iii) mediante la celebración de un concurso o de una subasta; iv) previa celebración del contrato preliminar y, finalmente v) la formación del contrato mediante adhesión a las condiciones contractuales preestablecidas por el otro contratante.

De todas ellas, nos interesa analizar la que hace referencia a la formación de un contrato mediante adhesión a condiciones contractuales preestablecidas por uno de los contratantes, ello debido a que el tradicional contrato negociado, como consecuencia de la producción masiva o en serie de bienes y servicios aunado al acelerado tráfico económico, tuvo forzosamente que evolucionar para enfrentar a la nueva realidad social y económica.

Surgió así la necesidad que el Derecho de contratos cuente con un instrumento igual de ágil y eficiente, con la capacidad de viabilizar relaciones masivas de intercambio, emergiendo en respuesta el contrato masivo, estandarizado o predispuesto a través de formularios pre-redactados que permiten la contratación en serie, cuyos contenidos han sido fijados con anticipación a su celebración por una de las partes contractuales. La contratación masiva presenta precisamente las dos modalidades antedichas como son: los contratos por adhesión y las cláusulas o condiciones generales de la contratación, instrumentos que en la actualidad cuentan con amplia normativa en la legislación comparada.

A objeto de una mejor comprensión de la temática, esquematizaremos nuestra exposición desagregándola en cinco apartados subsiguientes.

2.6.1. Concepto de adhesión.-

Como uniformemente sostiene la doctrina, fue Saleilles quien a principios del s. XX

¹⁴⁸ Respecto de los contratos de adhesión sugerimos consultar: Xavier O'Callaghan, y otros, *Contratos de adhesión y derechos de los consumidores*, Madrid, Mateu Cromo S.A., 1993, p. 203 y ss. // Igualmente Francisca Llodrà Grimalt, *El contrato celebrado bajo condiciones generales*, Valencia, Tirant Lo Blanch, 2002, p. 29 y ss.

acuñó la expresión “*contrato de adhesión*”, para designar aquellos casos en los cuales una de las partes contratantes (normalmente un empresario mercantil) que efectúa contrataciones en masa, determina la redacción de contratos con un contenido prefijado y uniforme.¹⁴⁹ De manera tal que el interesado en contratar con el empresario no tiene otra opción que aceptar las cláusulas del contrato de adhesión conforme están redactadas unilateralmente, lo que algunos tratadistas denominan como el único contrato posible.¹⁵⁰

En la doctrina se ha suscitado una profunda discusión en procura de indagar respecto a si quien se adhiere a un proyecto de contrato, encontrándose por este motivo en una situación donde su voluntad se halla bastante contraída, otorga - o no - un auténtico consentimiento respecto de las cláusulas o condiciones generales impuestas por la otra parte. Al respecto surgieron dos teorías, por un lado la denominada *Teoría de los contratos de adhesión*, la cual niega que estos contratos constituyan auténticos negocios contractuales comprendiendo que en la adhesión existen dos actos jurídicos unilaterales - y por consiguiente - independientes entre sí.¹⁵¹ Por otra parte surgió la *Tesis contractualista pura*,

¹⁴⁹ Saleilles acuñó el término “*contrats d’adhésion*” en 1902 al publicar su obra sobre la declaración de voluntad a propósito de su comentario de los arts. 116 a 144 del Código Civil alemán, específicamente cuando trataba el art. 133 que regulaba la interpretación de las declaraciones de voluntad, introduciendo así el concepto de “contratos de adhesión” en el ámbito jurídico. Se expresaba así respecto a este contrato: “*Hay unos pretendidos contratos que no tienen de contrato más que el nombre, y cuya construcción jurídica está por efectuarse; para los cuales, en cualquier caso, las reglas de interpretación individual deberían experimentar, ciertamente, importantes modificaciones; trátase de aquello que podría llamarse, a falta de algo mejor, los contratos de adhesión, en los cuales hay predominio exclusivo de una sola voluntad que actúa como voluntad unilateral, que dicta su ley no ya a un individuo, sino que a una colectividad indeterminada, obligándose por anticipado, unilateralmente, a la espera de la adhesión de los que querrán aceptar la ley del contrato, apoderándose de este compromiso ya creado sobre él mismo...*”, citado por Leslie Tomasello Hart, *La Contratación. Contratación Tipo, de Adhesión y Dirigida. Autocontratación y Subcontratación*, Edeval, Valparaíso-Chile, 1984, p. 31.

¹⁵⁰ (L. Díez-Picazo, 1996: 347 y ss.).

¹⁵¹ De conformidad con esta teoría, la peculiar forma de constitución de relaciones jurídicas como resultado de la formación del contrato por adhesión, ha conllevado a considerarlo como un “acto jurídico unilateral”. Así, Vallespinos indica que cuando hablamos del contrato por adhesión estamos frente a actos provenientes de una declaración de voluntad unilateral pues, independientemente de su aceptación, son determinados por la sola voluntad del oferente, reforzando esta idea al señalar que “*No se resta ni niega la intervención de una segunda voluntad (la del adherente), tan sólo se le quita eficacia por cuanto esta última carece de relevancia jurídica.*” Carlos Gustavo Vallespinos, *El Contrato por Adhesión a Cláusulas Generales*, Ed. Universidad, Buenos Aires-Argentina, 1984, p. 246 // Por otra parte, Zavala afirma que la teoría del acto unilateral considera a la adhesión como un acto de sometimiento y no como uno de consentimiento, consecuentemente, no puede llamarse contrato a lo que no es consentimiento, siendo éste, elemento para la celebración del contrato. Además sostiene que “*La adhesión como declaración unilateral no podrá ser alterada por el aceptante; así entonces, la adhesión resulta un verdadero sometimiento, a la voluntad de una sola de las partes.*” Luis Zavala Romero, *Derecho de los Contratos en el Código Civil Peruano de 1984*, Fecal, Lima, 2002, p. 215 // En la misma línea de pensamiento se pronuncia Díez-Picazo, para quien la aceptación de las cláusulas unilateralmente fijadas con carácter inmodificable, no representa un genuino consentimiento sino simplemente un “*acto de adhesión*” (L. Díez-Picazo, 1996: 130-131). En consecuencia, si la conclusión del contrato no es precedida de una negociación o discusión, se dice que no hay verdadero contrato, sino solamente la voluntad unilateral de una de las partes // Finalmente Tomasello a momento de comentar la tesis del acto unilateral, expone que los contratos por adhesión son claros supuestos de un acto unilateral emanado de una voluntad privada y cuyos efectos, una vez verificada al adhesión por el tercero, se determinan según la sola voluntad del oferente (L. Tomasello, 1984: 36).

la cual sostiene que el contrato de adhesión constituye un verdadero y auténtico contrato.¹⁵²

Al presente la doctrina predominante acepta la *Tesis contractualista pura*, pero la condición para que exista un auténtico contrato, estriba en el hecho que todas las cláusulas sean puestas a disposición de los interesados en el momento que manifiestan su aceptación y por consiguiente su adhesión. Ahora bien, toda vez que el contenido contractual está unilateralmente pre-redactado por una de las partes, obliga que al momento de su interpretación exista una mínima medida.

Es necesario distinguir dos supuestos: i) cuando todas las cláusulas han sido puestas en conocimiento del interesado adherente al momento de manifestar su aceptación, o ii) cuando las condiciones de ejecución de las obligaciones surgidas del contrato serán conocidas por el adherente de forma posterior. En criterio de Díez-Picazo, esta diferenciación permite identificar entre aquellos que pueden denominarse estrictamente contratos de adhesión de la figura de las condiciones generales de la contratación.¹⁵³

2.6.2. Concepto de Condiciones Generales de la Contratación.-

Con carácter previo a definir las condiciones generales de la contratación (en adelante CGC) es necesario establecer el concepto de cláusula, toda vez que su significado no es sinónimo a una condición general. Una cláusula reviste categoría de condición general

¹⁵² Para los seguidores de esta teoría, el elemento determinante que configura el carácter contractual del contrato por adhesión es la aceptación del adherente o destinatario; manifestación - libre o impuesta - que da lugar al nacimiento de una relación jurídica patrimonial vinculante para las partes. Con anterioridad a dicha declaración, la oferta propuesta aún no es contrato ya que por sí sola no es suficiente para configurarlo. De la Puente manifiesta que lo característico del contrato por adhesión no es que el destinatario se vea colocado en la alternativa de aceptar o rechazar íntegramente la oferta, sino que las estipulaciones que la conforman han sido fijadas previa y unilateralmente por el oferente y no surgen fruto de tratativas previas. Continúa diciendo: "*considero que si la formación del contrato se produce por razón de la aceptación de la oferta, que es el acto en virtud del cual el destinatario de la oferta hace suya la voluntad del oferente contenida en ella y lo declara así en su aceptación, con lo que se da lugar a la declaración conjunta de una voluntad común, esto ocurre tanto en el contrato paritario como en el contrato por adhesión.*" Manuel De la Puente y Lavalle, *El Contrato en General*, vol I, Palestra Editores, Lima, 2001, p. 667 // Por su parte Carbone refiere que "*El consentimiento de las dos partes es perfecto, pues la firma del adherente, al pie de las condiciones ofrecidas por la otra parte, demuestra que a lo sumo pudo faltar discusión "tête a tête" pero no la conformidad con respecto a dichas cláusulas.*" Carlos Carbone Oyarzun, *Contratos de adhesión*, Ed. Librería Jurídica, Buenos Aires, 1922, p. 13 // A su turno, Vallespinos resalta que aunque se observa una "alteración" en el acuerdo de voluntades, debido a la predisposición unilateral, ni esta circunstancia ni ninguno de los caracteres típicos del contrato por adhesión impiden su nacimiento ni lo alejan del ámbito contractual (C. Vallespinos, 1984: 245) // Zavala considera que el contrato por adhesión es un verdadero contrato, donde se manifiesta la oferta y la aceptación de las partes como resultado de la libre determinación, ya que "*En nada cambia que los términos del contrato estén redactados a plenitud por una sola de las partes, cuando, finalmente ambos llegan a coincidir. El vínculo jurídico que relaciona a los contratantes es directa consecuencia de la voluntad expresada por cada uno de ellos.*" (L. Zavala, 1984: 215) // Por último, Díez-Picazo comentando la "*tesis contractualista pura*" expresa que en los contratos por adhesión existe una verdadera prestación del consentimiento y como tal, se perfecciona un auténtico contrato, "*el vínculo contractual se genera voluntariamente y libremente.*" (L. Díez-Picazo, 1996: 348-349).

¹⁵³ (L. Díez-Picazo, 1996: 349).

cuando ha sido predispuesta de manera unilateral por una de las partes que interviene en la contratación, de tal manera que ha sido pre-redactada e incluida a una pluralidad de contratos, sin que ello signifique necesariamente que se trate de una cláusula abusiva.¹⁵⁴

Únicamente revestirá el carácter de abusiva, aquella cláusula que se incluya en contra de la buena fe que debe regir la contratación y a la que todo empresario o profesional está sujeto en virtud del art. 57 del C.com..¹⁵⁵ Se debe atender al perjuicio que pudiera causar una cláusula al consumidor que contrata con un empresario o profesional que se vale de la misma, a fin de establecer si la cláusula es en definitiva o no abusiva, para lo cual debe causar un desequilibrio notorio y sin justificativo real en las obligaciones de esta parte - la cual nótese - no necesariamente tiene por qué ser una condición general, toda vez que es posible que se la haya incluido en contratos particulares.

Conforme señalamos previamente el origen de las CGC se encuentra en la economía moderna, en la cual los empresarios desarrollan sus actividades negociales en base a condiciones uniformes y mediante contratos establecidos por ellos mismos de manera previa - *lo que se ha venido a denominar contratación en masa* - donde no existe la posibilidad por parte de los clientes de negociar o modificar las cláusulas previamente elaboradas.¹⁵⁶ Nótese

¹⁵⁴ Miguel Ángel Davara Rodríguez, *Comercio Electrónico*, Navarra, Aranzadi, 2004, pp. 538 y ss.

¹⁵⁵ El art. 57 del C.Com. dispone con carácter general que los contratos de comercio se ejecutarán y cumplirán de buena fe, por lo que resulta de aplicación en especial a la contratación efectuada por empresarios con los consumidores.

¹⁵⁶ Para el autor De Castro y Bravo las condiciones generales de los contratos se entienden como "*los conjuntos de reglas que un particular (empresario, grupo o rama de industriales o comerciantes) ha establecido para fijar el contenido (derechos y obligaciones) de los contratos que sobre un determinado tipo de prestaciones se propone celebrar. Mediante tales condiciones, se elimina "a priori" los tratos previos entre las partes; una de éstas (el empresario) se ha atribuido el papel de predisponer o dictar, conforme a su interés y a su gusto, la regulación de los contratos; se independiza el establecimiento de las condiciones de la celebración del contrato concreto; las condiciones se imponen de tal modo inexorable que pueden calificarse de apéndice de la prestación; se redactan en forma abstracta y articulada que se acostumbra en las leyes.*" Federico De Castro y Bravo, *Las Condiciones Generales de los Contratos y la Eficacia de las Leyes*, Reimpresión de la 2da. Ed., Civitas, Madrid, 1987, pp. 12-13 // Por otra parte Rezzónico señala que "*Condición negocial general o condiciones negociales generales es la estipulación, cláusula o conjunto de ellas, reguladoras de materia contractual, pre formuladas, y establecidas por el estipulante sin negociación particular, concebidas con caracteres de generalidad, abstracción, uniformidad y tipicidad, determinando una pluralidad de relaciones, con independencia de su extensión y características formales de estructura o ubicación.*" Juan Carlos Rezzónico, *Contratos con Cláusulas Predispuestas. Condiciones Negociales Generales*, Astrea, Buenos Aires, 1991, p. 109 // Otros autores sostienen que las cláusulas generales de contratación no son sino una suerte de figura que cohesiona parte del contrato por adhesión, inflexible en su contenido, y parte del contrato por negociación. Así por ejemplo lo señala De la Puente, quien anota que al advertirse que la masa de personas tenían necesidades similares pero no iguales "*...se hizo necesario plasmar tal diferenciación en el ámbito contractual, de allí que las cláusulas generales de contratación constituyan una feliz combinación de los contratos por adhesión y los contratos paritarios.*" Manuel De la Puente y Lavalle; "Las cláusulas generales de contratación y la protección al consumidor", en Carlos Alberto Soto Coaguila y Roxana Jiménez Vargas-Machuca, comp., *Contratación Privada*, Lima, Jurista, 2002, p. 294 // Así también lo destaca Silva para quien las condiciones generales efectivamente predeterminan unilateralmente el contenido de los futuros contratos de adhesión ya que "*...éstos tan sólo concretan las condiciones generales en las relaciones singulares entabladas entre la empresa y los adherentes...*" Pedro F. Silva Ruiz, "Contratos de adhesión, condiciones contractuales generales (condiciones generales de los contratos o de la contratación) y las cláusulas abusivas", en Atilio Aníbal Alterini, José Luis De los Mozos y Carlos Alberto Soto Coaguila, comp., *Instituciones de Derecho Privado. Contratación contemporánea. Teoría General y Principios*, Bogotá, Themis, 2001, pp. 55-56.

en consecuencia que las condiciones generales cumplen una función económica favorable, ya que estandarizando el contenido contractual, se facilita la administración de los negocios comerciales posibilitando el ahorro y la eficiencia empresarial, entre otros.¹⁵⁷

Pero al mismo tiempo, no puede negarse que la contratación por medio de fórmulas predisuestas o cláusulas redactadas unilateralmente ubican al cliente o consumidor en un estado de inferioridad respecto de la parte contratante más fuerte, es decir el empresario, quien de alguna manera ve acrecentados sus derechos y relativizadas sus obligaciones, en tanto que para el cliente o usuario, ocurre el fenómeno contrario, puesto que muchos de sus derechos se ven limitados y sus obligaciones amplificadas.

Si bien desde el punto de vista económico no es aconsejable una prohibición total de este modo de contratación, desde el punto de vista jurídico es necesario implementar un régimen de previsión y control, a objeto de prevenir o en su caso impedir que esta forma de contratación lleve a situaciones de abuso de la parte económicamente más fuerte, respecto de la más débil en cualquier tipo de negocio.¹⁵⁸

Las características de las condiciones generales son fundamentalmente cuatro:¹⁵⁹

- i) la contractualidad, es decir que las CGC deben estar redactadas con la finalidad de ser incorporadas a una pluralidad de contratos.;
- ii) la predisposición unilateral, es decir que las condiciones son elaboradas por una de las partes contratantes;
- iii) la generalidad de las condiciones, o sea destinadas a ser aplicadas a todos los contratos;
- iv) la imposición o imposibilidad de negociación, llamada también inevitabilidad de la aplicación, en sentido que su aplicación no puede ser evitada por el consumidor o

¹⁵⁷ (L. Díez-Picazo, 1996: 367 y ss.)

¹⁵⁸ (L. Díez-Picazo, 1996: 368).

¹⁵⁹ Juan José Marín López, "El ámbito de aplicación de la ley sobre Condiciones Generales de la Contratación", en Ubaldo Nieto Caro, comp., *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000, pp. 127-140 // (L. Díez-Picazo, 1996: 370-371).

usuario si quiere recibir el bien o gozar del servicio. Esta última se complementa con dos reglas: i) por una parte, la negociación de una cláusula aislada no excluye la imposibilidad de negociación de las condiciones consideradas como conjunto; ii) la segunda regla, es que rige en esta materia una inversión de la carga de la prueba, de modo que no es el adherente el que debe probar la imposibilidad de negociación o la efectiva falta de negociación, sino que es el predisponente quién tiene la carga de la prueba de la existencia de una negociación individual.¹⁶⁰

Con los antecedentes expuestos, señalaremos que existen contratos sujetos a condiciones generales perfeccionados por adhesión en los que la problemática radica finalmente, no tanto en el debate académico y teórico sobre su carácter contractual o no contractual, sino en la implementación de un adecuado régimen normativo que reprima o evite los posibles abusos a que puede dar lugar la situación de poder de la parte más fuerte (normalmente el empresario), sobre todo en los contratos que se celebran con usuarios o consumidores.

Para ello existen fundamentalmente dos soluciones: a) la implementación de un régimen jurídico y sistemas de control sobre las condiciones generales y cláusulas abusivas; b) la implementación de un régimen especial de interpretación.

2.6.2.1. Régimen jurídico de las CGC en el Ordenamiento español.-

A efectos de normar las CGC en España,¹⁶¹ primeramente se sancionó el año 1980 la Ley 50/1980, de 8 de octubre, reguladora de los contratos de seguros privados, en la que se encuentra por primera vez una disposición legal de las condiciones generales de la contratación.¹⁶² Posteriormente, se dictó la Ley 26/1984, de 19 de julio, General para la

¹⁶⁰ Al respecto el art. 82.2 del TRLGDCU señala: “El hecho de que ciertos elementos de una cláusula o que una cláusula aislada se hayan negociado individualmente no excluirá la aplicación de las normas sobre cláusulas abusivas al resto del contrato. El empresario que afirme que una determinada cláusula ha sido negociada individualmente, asumirá la carga de la prueba”.

¹⁶¹ Un estudio muy completo respecto del régimen jurídico de las CGC en el Ordenamiento español puede ser consultado en: Ubaldo Nieto Carol, y otros, *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000, p. 29 y ss. // Igualmente recomendamos consultar: Aurelio Menéndez, Luís Díez-Picazo, y otros, *Comentarios a la Ley sobre Condiciones Generales de la Contratación*, Madrid, Civitas, 2002, p. 61 y ss. // Asimismo (F. Llodrà, 2002: 71 y ss.).

¹⁶² (L. Díez-Picazo, 1996: 369).

Defensa de los Consumidores y Usuarios (LGDCU).¹⁶³ Finalmente, y dada la sentida necesidad en el ámbito español, se aprobó la Ley 7/1998, de 13 de abril, sobre Condiciones Generales de la Contratación (en adelante LCGC).¹⁶⁴ Asimismo, en el ámbito europeo se emitió la Directiva 93/13/CEE del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores.

Resulta oportuno aclarar con carácter previo, que existen básicamente dos modelos de control del contenido de los contratos en el Derecho comparado: i) el primero, se circunscribe a regular aquellos contratos en las que una de las partes carece de libertad contractual *-leyes de condiciones generales-* seguido por ejemplo en Alemania, Portugal, Reino Unido; ii) el segundo, regula y controla las relaciones contractuales en las que intervienen contratantes mercedores de protección *-leyes de contratos con consumidores-* que es el sistema seguido en Francia y determinadas Directivas comunitarias.¹⁶⁵

El sistema seguido a nivel Comunitario en Europa por la Directiva 93/13/CEE del Consejo de 5 de abril de 1993 sobre las cláusulas abusivas en los contratos celebrados con consumidores,¹⁶⁶ y en España, inicialmente por la LGDCU, representa el segundo modelo antes descrito, pues únicamente se circunscribía al control de los contratos celebrados conforme a CGC en los que el adherente era un consumidor en el sentido de los arts. 1.2 y 3 de la propia Ley, por lo que resultaba ser una *ley de consumidores con regulación de las condiciones generales*.¹⁶⁷

Con esta delimitación por consiguiente, resultaban huérfanos de regulación los contratos sujetos a CGC pero en los que el adherente era un empresario. Se consideraba por ciertos sectores que éstos no requerían una protección toda vez que, a diferencia de los

¹⁶³ La cual estuvo vigente hasta el 1 de diciembre de 2007, entrando a partir de esa fecha en vigencia el 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.

¹⁶⁴ Un estudio sobre el ámbito de aplicación de esta ley puede ser consultado en: (J.J. Marín, 2000: 113 y ss.).

¹⁶⁵ Una explicación muy prolija sobre estos modelos puede ser consultada en: (U. Nieto, 2000: 29 y ss.).

¹⁶⁶ Respecto de la Directiva 93/13/CEE y su transposición al ordenamiento español consultar: Rodrigo Bercovitz Rodríguez-Cano, "La transposición de la Directiva Comunitaria al derecho español", en Ubaldo Nieto Caro, comp., *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000, p. 439 y ss.

¹⁶⁷ Lo afirmado se corrobora de la lectura del art. 10 de dicha Ley en su redacción original, que precisamente se modifica por la LCGC.

consumidores, poseen un nivel mayor de preparación e información. Pero sin negar que el consumidor reviste mayor necesidad de protección que el empresario, resulta claro que en ambos casos se encuentran en una situación de *inferioridad funcional* con relación a quien pre-redacta el clausulado general, lo que indudablemente puede conllevar a situaciones de abuso, por lo que se hace necesario una protección general y no únicamente respecto de los contratos en los que participan consumidores o usuarios.¹⁶⁸

Con estas aclaraciones, señalaremos que la LCGC define las condiciones generales de la contratación como “*las cláusulas predispuestas cuya incorporación al contrato sea impuesta por una de las partes*” (art. 1 LCGC), por lo que nos encontramos ante una definición objetiva de condición general, ya que la ley no atiende a la autoría material de las mismas, de su apariencia externa, de su extensión y de cualesquiera otras circunstancias, habiendo sido redactadas con la finalidad de ser incorporadas a una pluralidad de contratos.

Las condiciones generales conforme explica Davara, no son otra cosa que cláusulas homogéneas redactadas de manera unilateral por el empresario o profesional a objeto de efectuar un número ilimitado de contratos.¹⁶⁹ Éstas - advierte - se pueden presentar tanto en los contratos celebrados entre el empresario con consumidores, como también es factible que se encuentren en contratos donde ambas partes revisten categoría de empresarios o profesionales; en cualquiera de los casos, no obstante, resulta imprescindible que confluyan determinadas condiciones para que exista efectivamente una condición general de la contratación. Dichas condicionantes son las siguientes:

- i) que la condición general forme parte del contrato;
- ii) sean conocidas, o en casos de contratación no escrita exista posibilidad real de ser conocidas;
- iii) hayan sido redactadas de forma transparente, con claridad, concreción y sencillez;

¹⁶⁸ De hecho, las normas de Derecho comparado tienen un ámbito de aplicación general, sin perjuicio de que añadan normas específicas para el caso de que el adherente sea un consumidor (U. Nieto, 2000: 30).

¹⁶⁹ (M.A. Davara, 2004: 539).

iv) cuando se contrata con consumidores, que no sean abusivas.

a) Validez de las CGC.-

La validez de las CGC - en virtud de los requisitos de incorporación establecidos por el art. 5 LCGC - está supeditada a que las mismas reúnan básicamente las siguientes condiciones:¹⁷⁰

- i) firma del adherente,
- ii) que el contrato haga referencia a las CGC incorporadas,
- iii) transparencia, claridad, concreción y sencillez en su redacción.

Por otra parte, es necesario remarcar que de conformidad con lo dispuesto por el art. 7 LCGC, no se entenderán como incorporadas al contrato aquellas CGC que:

- i) el adherente no haya podido conocer antes de la firma de manera completa, o
- ii) no hayan sido firmadas cuando ello sea necesario,
- iii) sean ilegibles, ambiguas, oscuras e incomprensibles, salvo que hayan sido expresamente aceptadas por el adherente y se ajusten a la normativa específica que discipline la necesaria transparencia de las cláusulas.

b) Nulidad de las CGC.-

Respecto de la nulidad de las CGC, es necesario señalar que ésta opera básicamente en dos supuestos. Serán nulas (art.8 LCGC, art. 83.1. TRLGDCU) las CGC que:¹⁷¹

- i) sean contrarias a lo dispuesto en la ley en perjuicio del adherente o en cualquier otra norma imperativa,
- ii) aquellas que sean abusivas, cuando el contrato se haya celebrado con un consumidor.

En todo caso, en cualquiera de los supuestos descritos si existen dudas sobre la

¹⁷⁰ Respecto de los requisitos de inclusión de la CGC al contrato, consultar: Javier Pagador López, "Requisitos de incorporación de las Condiciones Generales y consecuencias negativas", en Ubaldo Nieto Caro, comp., *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000, p. 223 y ss. // Asimismo (O'Callaghan y otros, 1993: 9 y ss.) // (F. Llodrà, 2002: 259 y ss.)

¹⁷¹ Con relación a la nulidad de las CGC consultar: (F. Llodrà, 2002: 346 y ss.)

interpretación de las cláusulas, éstas deben resolverse siempre a favor del adherente (art. 6 LCGC, art. 80.2 TRLGDCU, art. 1.288 C.c.). La Directiva sobre cláusulas abusivas establece un Anexo en el que enumera una serie de supuestos, no tasados, que recogen dichas cláusulas abusivas.¹⁷²

c) Sujetos de la contratación con CGC.-

Desde el punto de vista subjetivo, se hace imprescindible identificar quiénes pueden ser considerados como sujetos de la contratación sujeta a CGC. Éstos pueden ser:

- Un Empresario o profesional

La LCGC al establecer su ámbito subjetivo de aplicación, se refiere al adherente como cualquier persona física o jurídica que procede a la contratación con un profesional predisponente a través de condiciones generales, incluyéndose expresamente entre los mismos a los profesionales, sin necesidad de que actúen en el marco de su actividad (arts. 2.1 y 2.3). Define la LCGC al profesional como “*toda persona física o jurídica que actúe dentro del marco de su actividad profesional o empresarial, ya sea pública o privada*” (art. 2.2.).

¹⁷² Cláusulas contempladas en el apartado 3ro. del art. 3 de la Directiva 93/13/CEE, que tengan por objeto o por efecto: a) excluir o limitar la responsabilidad legal del profesional en caso de muerte o daños físicos del consumidor debidos a una acción u omisión del mencionado profesional; b) excluir o limitar de forma inadecuada los derechos legales del consumidor con respecto al profesional o a otra parte en caso de incumplimiento total o parcial, o de cumplimiento defectuoso de una cualquiera de las obligaciones contractuales por el profesional, incluida la posibilidad de compensar sus deudas respecto del profesional mediante créditos que ostente en contra de este último; c) prever un compromiso en firme del consumidor mientras que la ejecución de las prestaciones del profesional está supeditada a una condición cuya realización depende únicamente de su voluntad; d) permitir que el profesional retenga las cantidades abonadas por el consumidor, si éste renuncia a la celebración o la ejecución del contrato, sin disponer que el consumidor tiene derecho a percibir del profesional una indemnización por una cantidad equivalente cuando sea éste el que renuncie; e) imponer al consumidor que no cumpla sus obligaciones una indemnización desproporcionadamente alta; f) autorizar al profesional a rescindir el contrato discrecionalmente, si al consumidor no se le reconoce la misma facultad, o permitir que el profesional se quede con las cantidades abonadas en concepto de prestaciones aún no efectuadas si es el propio profesional quien rescinde el contrato; g) autorizar al profesional a poner fin a un contrato de duración indefinida, sin notificación previa con antelación razonable, salvo por motivos graves; h) prorrogar automáticamente un contrato de duración determinada si el consumidor no se manifiesta en contra, cuando se ha fijado una fecha límite demasiado lejana para que el consumidor exprese su voluntad de no prorrogarlo; i) hacer constar de forma irrefragable la adhesión del consumidor a cláusulas de las cuales no ha tenido la oportunidad de tomar conocimiento real antes de la celebración del contrato; j) autorizar al profesional a modificar unilateralmente sin motivos válidos especificados en el contrato los términos del mismo; k) autorizar al profesional a modificar unilateralmente sin motivos válidos cualesquiera características del producto que ha de suministrar o del servicio por prestar; l) estipular que el precio de las mercancías se determine en el momento de su entrega, u otorgar al vendedor de mercancías o al proveedor de servicios el derecho a aumentar los precios, sin que en ambos casos el consumidor tenga el correspondiente derecho a rescindir el contrato si el precio final resultare muy superior al precio convenido al celebrar el contrato; m) conceder al profesional el derecho a determinar si la cosa entregada o el servicio prestado se ajusta a lo estipulado en el contrato, o conferirle el derecho exclusivo a interpretar una cualquiera de las cláusulas del contrato; n) restringir la obligación del profesional de respetar los compromisos asumidos por sus mandatarios o supeditar sus compromisos al cumplimiento de formalidades particulares; o) obligar al consumidor a cumplir con todas sus obligaciones aun cuando el profesional no hubiera cumplido con las suyas; p) prever la posibilidad de cesión del contrato por parte del profesional, si puede engendrar merma de las garantías para el consumidor sin el consentimiento de éste; q) suprimir u obstaculizar el ejercicio de acciones judiciales o de recursos por parte del consumidor, en particular obligándole a dirigirse exclusivamente a una jurisdicción de arbitraje no cubierta por las disposiciones jurídicas, limitándole indebidamente los medios de prueba a su disposición o imponiéndole una carga de la prueba que, conforme a la legislación aplicable, debería corresponder a otra parte contratante.

- Un Consumidor

El TRLGDCU define a los consumidores o usuarios como “*las personas físicas o jurídicas que actúan en un ámbito ajeno a una actividad empresarial o profesional*” (art. 3). Eso significa que la norma excluye de la consideración de consumidor o usuario, a todas las personas ya sean físicas o jurídicas que adquieran los bienes o servicios objeto de la contratación, pero que no se constituyan en efectivos destinatarios finales de los mismos y actúen con ánimo de lucro.

Por consiguiente, es necesario hacer notar que el beneficiario de la protección conferida por la LCGC no es únicamente el consumidor o destinatario final de los bienes y servicios objeto de contrato, sino que también goza de la referida protección legal cualquier otra persona, entre los que se incluyen los profesionales, que operan con un propósito foráneo a su actividad profesional.

SUJETOS DE LA CONTRATACIÓN¹⁷³

Directiva 93/13/CEE	LCGC
<ul style="list-style-type: none"> • Vendedor de bienes o prestador de servicios: <ul style="list-style-type: none"> - persona física o jurídica - pública o privada - que actúe dentro del marco de su actividad profesional • Comprador <ul style="list-style-type: none"> - persona física - que actúe con un propósito ajeno a su actividad profesional 	<ul style="list-style-type: none"> • Profesional <ul style="list-style-type: none"> - persona física o jurídica - pública o privada - que actúe dentro del marco de su actividad empresarial o profesional • Persona física o jurídica que sea destinatario final de los bienes y servicios, con inclusión de toda persona que actúe con un propósito ajeno a su actividad profesional, aunque no fue destinatario final de los bienes o servicios objeto del contrato. <ul style="list-style-type: none"> - persona física o jurídica - destinatario final o no de los bienes o servicios - que actúe con un propósito ajeno a su actividad profesional

d) Cláusulas abusivas.-

A objeto de comprender cuándo nos encontramos ante una cláusula de un contrato que reviste la categoría de abusiva, es necesario en primer lugar señalar que esta posibilidad

¹⁷³ Tomado de (M.A. Davara, 2004: 541).

únicamente puede presentarse en contratos celebrados con consumidores.¹⁷⁴

En segundo lugar, una cláusula contractual no negociada reviste la condición de abusiva, en aquellos casos en los que ocasiona - en perjuicio del consumidor - un desequilibrio notorio entre los derechos y obligaciones que devienen del contrato (art. 82 TRLGDCU). Asimismo, los arts. 85 a 90 TRLGDCU contienen un listado de cláusulas que, en todo caso, serán consideradas abusivas y, por tanto, se tendrán por no puestas en el contrato celebrado. En ese sentido, para catalogar a una cláusula contractual como abusiva es necesario acudir a la valoración de una serie de elementos, como por ejemplo: las circunstancias en que ha sido celebrado el contrato, la naturaleza de los bienes y servicios que constituyen el objeto del contrato, así como también se debe acudir a la valoración integral de las restantes cláusulas del contrato.

Así como la interpretación de las cláusulas oscuras o poco claras no pueden beneficiar a la parte que las dispuso, de conformidad con los principios que rigen en otros ámbitos generales del Derecho, en este caso acontece de la misma manera y en idéntica forma, puesto que la interpretación de la cláusula en caso de dudas siempre debe beneficiar al consumidor (art.80.2 TRLGDCU).

Al respecto, es posible reconocer dos clases de criterios generales de control sobre estas cláusulas: el primero constituye un criterio formal, para lo cual cabe remitirse al contenido del art. 80.1 del TRLGDCU, con relación a la exigencia en la claridad y sencillez de la exposición, así como los requisitos de comprensión de parte de la persona con la que se pretende contratar. El segundo criterio es sustantivo o de fondo y hace referencia al contenido de las cláusulas.¹⁷⁵ De forma que en términos generales, en las ocasiones en que se contrata con consumidores, resultan siendo nulas - por abusivas - aquellas cláusulas que se redactan

¹⁷⁴ Respecto de las cláusulas abusivas y la nulidad de las mismas consultar: Justino F. Duque Domínguez, “Las cláusulas abusivas en contratos de consumo”, en Ubaldo Nieto Caro, comp., *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000, p. 463 y ss.

¹⁷⁵ Al respecto (L. Díez-Picazo, 1996: 378 y ss.)

de modo contrario a la buena fe y al justo equilibrio entre las partes.¹⁷⁶

2.6.2.2. Régimen especial de interpretación de las CGC.-

El Código civil se ocupa de establecer las reglas de interpretación de los contratos en los arts. 1.281 a 1.289 C.c., pero dichas normas están pensadas para ser aplicadas a aquellos contratos que son obra común de la voluntad de las partes contratantes, por lo que resultan difícilmente aplicables a los contratos de adhesión. De esa manera es que, tanto la doctrina como la legislación, se han ocupado de desarrollar una serie de criterios específicos de interpretación para los casos en que los contratos contengan condiciones generales.

El art. 6 de la LCGC y el art. 80 del TRLGDCU contienen estas reglas de interpretación, las cuales han sido complementadas por la doctrina y podemos sintetizarlas en las siguientes cinco categorías:¹⁷⁷

- a) La regla de la interpretación “contra proferentem”.- Se refiere a que en el caso que existan dudas en la interpretación del contrato, se resolverán en contra de quien lo haya redactado, que es básicamente la regla contenida en el artículo 1.288 del C.c..
- b) La regla de la prevalencia.- Por la que en el caso de que exista una discrepancia entre el contenido de la condición general y el de una cláusula particular, habrá de estarse a lo que disponga esta última.
- c) La regla de la condición más beneficiosa.- Se refiere a que en caso de divergencia entre una condición general y una cláusula particular, se aplicará la que resulte más beneficiosa para el adherente; si ello no fuera posible prevalecerá la cláusula particular sobre la general.¹⁷⁸

¹⁷⁶ (L. Díez-Picazo, 1996: 382 y ss.) // En el mismo sentido Francisco Javier Orduña Moreno, “Derecho de la contratación y condiciones generales”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003; pp. 269-363 // Igualmente la obra de María Jesús Moro Almaraz, “La contratación en el comercio electrónico: luces y sombras”, en *REDI: Revista Electrónica de Derecho Informático*, No. 80, España, Alfa-Redi, marzo/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=968>

¹⁷⁷ Una sistematización bastante clara de estas reglas de interpretación puede ser consultada en (L. Díez-Picazo, 1996: 411-414).

¹⁷⁸ Al respecto, el art. 6 de la LCGC establece: “Reglas de interpretación. 1. Cuando exista contradicción entre las condiciones generales y las condiciones particulares específicamente previstas para ese contrato, prevalecerán éstas sobre aquéllas, salvo que las condiciones generales resulten más beneficiosas para el adherente que las condiciones particulares. 2. Las dudas en la interpretación de las condiciones generales oscuras se resolverán a favor del adherente. En los contratos con consumidores esta norma de interpretación sólo será aplicable cuando se ejerciten acciones individuales.”

- d) La regla de la condición más importante.- Planteada por la doctrina, se refiere a que en caso de controversia entre las condiciones generales, debe otorgarse importancia preferente a las cláusulas o condiciones de mayor trascendencia para el contrato.
- e) La regla de la interpretación restrictiva.- También de construcción doctrinal, señala que debe efectuarse una interpretación restrictiva de las condiciones generales.¹⁷⁹

2.6.3. Fundamento de la obligatoriedad de las CGC.-

En un primer momento, antes que el ordenamiento jurídico se ocupara de normar las CGC, se planteaba el problema de establecer el fundamento de su obligatoriedad, sobre todo cuando no existía una expresa aceptación por parte de los adherentes. Conforme explica Díez-Picazo, a quien seguiremos en esta parte, la doctrina del derecho mercantil consideraba que las CGC poseían un auténtico valor normativo, lo que suponía considerarlas como fuentes del derecho.¹⁸⁰ No obstante, ante la imposibilidad de su reconocimiento como fuente indirecta ante la ausencia de legislación positiva, es ampliamente conocido en la doctrina mercantil que Garrigues trató de resolver el problema calificando a las CGC como verdaderos *usos mercantiles*.¹⁸¹

Esta teoría que fue muy criticada en su momento toda vez que las reglas preestablecidas por las empresas no pueden considerarse fuente de derecho como usos mercantiles, de manera que únicamente pueden adquirir fuerza obligatoria como contenido estricto de cada contrato en particular.¹⁸²

¹⁷⁹ Respecto de las reglas de interpretación de las CGC, también recomendamos consultar: Juan Roca Guillamón, “Reglas de interpretación de las Condiciones Generales de los contratos”, en Ubaldo Nieto Caro, comp., *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000, p. 305 y ss.

¹⁸⁰ (L. Díez-Picazo, 1996: 373-375).

¹⁸¹ Conforme reseña Vallespinos, el fundador de la teoría por la cual se asimilan las cláusulas generales de contratación a verdaderos “*usos mercantiles*”, considerando que su inclusión más adecuada es dentro del Derecho consuetudinario, es el autor Garrigues, para quien las condiciones generales que forman el contenido de los contratos por adhesión tienen la fuerza de los usos de las costumbres, de los usos del tráfico negocial y, en consecuencia adquieren poder normativo constituyéndose en reglas objetivas con igual fuerza que las leyes (C. Vallespinos, 1984: 293).

¹⁸² Efectivamente, esta tesis fue sometida a las agudas críticas de la doctrina. Respecto a la consideración de las cláusulas generales de contratación como auténticas normas jurídicas, Vallespinos sostiene puntualmente que “*el Estado jamás puede dejar en manos de los particulares la misma fuerza jurídica que está reservada exclusivamente a sus organismos.*” (C. Vallespinos, 1984: 292) // Por su parte De Castro y Bravo hace conocer sus críticas indicando: “*Pues no puede desconocerse que el Estado de Derecho, en sus reglas constitucionales o fundamentales, es incompatible con la atribución a los empresarios de un privilegiado poder normativo. Tal poder legislativo, en favor de una clase, supone una previa subversión real de la organización político-jurídica, de máxima trascendencia, cuya existencia no se prueba y respecto a la que todo induce a creer que no se ha producido ni se producirá...*”, y continúa expresando, “*No hay un Derecho de la*

Por consiguiente en todos aquellos casos en que las condiciones no sean incorporadas en el contrato, quien pretenda su aplicación - el predisponente - tiene la carga de probar que el adherente las conoció y en todo caso las aceptó expresamente, de manera tal que las condiciones generales sólo vinculan a los adherentes en caso que se demuestre que tienen conocimiento de ellas y además que las aceptaron, aspecto que no puede ser presumido.

Ante esta realidad, Díez-Picazo refiere que surgió entonces la tesis de las condiciones generales de la contratación como fuente de integración del contrato por imperativo legal, de manera que la polémica antes señalada fue superada en la medida en que las condiciones que cumplen los requisitos legales, pasan a formar parte e integrar el contrato por decisión expresa de la ley, que constituye en definitiva el fundamento de la obligatoriedad de las condiciones generales.¹⁸³

2.6.4. La incorporación de las CGC al documento contractual.-

En algún momento se efectuaba la distinción entre condiciones generales de la contratación y condiciones generales del contrato, empleando esta última denominación para aquéllas que estaban incorporadas al texto contractual, reservando la primera denominación para aquéllas que se encuentran fuera del texto contractual.¹⁸⁴

Hoy en día para el derecho comparado resulta indiferente que las cláusulas o condiciones generales estén incluidas en el documento contractual o se ubiquen de forma externa y separada a él, asimismo no importa el tipo de documento en que las condiciones se encuentren contenidas, de manera tal que las condiciones generales integran un contrato aún prescindiendo de su incorporación documental. Además tampoco es necesario el completo

Economía, fuera del Estado, que las convierta misteriosamente en Derecho objetivo. No existe una autonomía originaria conquistada a favor de los empresarios. (F. De Castro, 1987: 24-25).

¹⁸³ (L. Díez-Picazo, 1996: 375).

¹⁸⁴ Sobre este punto (L. Díez-Picazo, 1996: 376) // Asimismo conforme refiere Vallespinos, fue precisamente Garrigues quien distinguía entre condiciones generales de los contratos y de la contratación. Explica que en criterio de Garrigues, las condiciones generales de los contratos son utilizadas por las empresas en la contratación con sus clientes y que éstos deben suscribir, tienen por consiguiente un auténtico carácter contractual, ya que vinculan por la aceptación implícita en la adhesión. En tanto que las condiciones generales de la contratación, son acordadas entre la asociación o grupos de empresas para que cada uno de sus miembros las utilice en los contratos con sus clientes, revistiendo un carácter semejante al de la ley por su obligatoriedad entre las partes, llegando a afirmar que si se respetan los límites de la buena fe contractual pueden calificarse como verdaderas fuentes del derecho mercantil (C. Vallespinos, 1984: 293-297). Debido a su repetición, consolidación y obligatoriedad para Garrigues son semejantes al uso legislativo, teoría que como analizamos en su momento fue duramente criticada por la doctrina.

conocimiento de las condiciones por parte del adherente, ya que para que éstas revistan carácter obligatorio es suficiente que el predisponente facilite el adherente los medios para que este pueda conocer su contenido, cualquiera sea en la práctica el modo por el que se produzca.¹⁸⁵

2.6.5. Las CGC en el contrato de certificación reconocida.-

El contrato de certificación reconocida usualmente consiste en un documento cuya extensión no supera de una a tres fojas, se encuentra pre-redactado de manera unilateral por el PSC y contiene una serie de condiciones generales de la contratación del servicio de certificación articuladas junto al clausulado de estilo. El contrato asimismo, deja constancia de la existencia de dos documentos complementarios al contrato principal: la Declaración de Prácticas de Certificación y las Políticas de Certificación vinculadas al certificado que se solicita, a las cuales el cliente debe acudir por remisión, toda vez que se deja claramente establecido que ambos instrumentos forman parte integral e indisoluble del contrato, siendo obligación del PSC ponerlos a disposición del público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita (art. 19 LFE).

De manera que quien se encuentre interesado en obtener un certificado reconocido (junto con aquél seguramente también una firma electrónica, en caso de no poseer una con carácter previo) y gozar de los servicios que hacen a la actividad de un PSC, no tiene más remedio que adherirse al contrato principal pre-formulado por el PSC y, por consiguiente, a las condiciones generales de prestación del servicio contenidas en las Prácticas y Políticas de Certificación, sin posibilidad de negociación individual, puesto que estos contratos revisten la característica de ser formularios aplicados en masa, con lo cual, la libre discusión entre las

¹⁸⁵ Rezzónico señala que el lazo de unión entre la manifestación del cliente y las condiciones negociales generales - que también puede advertir por comportamiento concluyente - se llama "*inclusión en el contrato*" o "*incorporación de los términos*", "*asunción*", "*aceptación*" (del adherente). Más adelante advierte que las condiciones negociales generales pasan por dos momentos: a) la etapa de elaboración que comprende la ideación y redacción para concluir en su pre-formulación abstracta y unilateral y, b) la etapa de efectivización de esa virtualidad eventual a través de la "*fijación*" o "*establecimiento*" en casos concretos. En la primera etapa, el protagonista es el estipulante, en tanto que en la segunda, el establecimiento o fijación pone en contacto al estipulante con el adherente (J. Rezzónico, 1991: 421-423) // Díez-Picazo puntualiza que no se exige un completo conocimiento de las condiciones generales por parte del adherente, "*es suficiente que el predisponente haya facilitado la posibilidad de conocerlas, cualquiera que sea la forma en que ello se haya conocido.*" (L. Díez-Picazo, 1996: 376).

partes resulta inexistente.

De todo lo expuesto, resulta evidente que la de certificación reconocida es un contrato sujeto a condiciones generales que se perfecciona por adhesión,¹⁸⁶ razón por la cual, le resultan de aplicación las normas contenidas en la LCGC, considerando que las partes intervinientes son ambos empresarios.

Asimismo, en los casos que el adherente (*que no es nuestro caso pero es oportuna la aclaración*) y Usuario del certificado revisten la condición de consumidor o usuario, le son además aplicables las normas del TRLGDCU.¹⁸⁷

Asimismo a efectos de interpretación del contrato, deberán observarse las reglas de los arts. 1.281 a 1.289 del C.c. en cuanto resulten aplicables y las contenidas en el art. 50 y ss. del C.com.

2.7. Contrato obligatorio.-

La doctrina moderna al referirse a la clasificación de los contratos, los divide entre contratos obligatorios y contratos reales. Conforme explica Díez-Picazo, los contratos reales, son aquellos que producen como efecto la constitución, transmisión, modificación o extinción de un derecho real, en tanto que los contratos obligatorios, son aquellos cuyo efecto se limita a constituir entre las partes una relación obligatoria y por consiguiente a atribuir derechos de crédito.¹⁸⁸

¹⁸⁶ Sin restarle importancia a la necesaria diferenciación entre contratos por adhesión y cláusulas o condiciones generales de la contratación, para algunos autores como Zavala estas diferencias no son más que teóricas, pues en la práctica comenta, las cláusulas generales se viabilizan a través de los contratos por adhesión; el proceso empieza con arreglo a cláusulas generales de contratación y termina como un auténtico contrato por adhesión, sin embargo, finaliza el autor, no todos los contratos por adhesión empiezan con cláusulas generales (L. Zavala, 2002: 226). Nosotros consideramos que las condiciones generales aluden al momento de la formulación previa del contenido del contrato, en tanto que con la expresión contrato de adhesión se hace referencia a la imposición del contenido de dicho contrato, se trata entonces, de dos aspectos de un mismo fenómeno, ambos conceptos hacen referencia a la misma realidad pero vista desde dos puntos de vista o, para ponerlo en otras palabras, constituyen dos caras de la misma moneda.

¹⁸⁷ Un estudio sobre la protección del consumidor en el mundo virtual, puede ser consultado en (R. Lorenzetti, 2001: 217-258) // Asimismo, conforme apunta Domínguez, las posibilidades del comercio electrónico no se limitan hoy en día a las relaciones entre empresas (B2B), sino que se amplían a la de éstas con los consumidores (B2C) y a la de los particulares entre sí (C2C), lo cual plantea el problema de la aplicación de la normativa existente sobre protección de consumidores y usuarios (A. Domínguez, 2001: 32-33) // La temática es ampliamente abordada por Mario E. Clemente Meoro, "La protección del consumidor en los contratos electrónicos", en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003; pp. 365-401 // Consultar asimismo Carlos Dionisio Aguirre, "El Desarrollo desde la perspectiva de la defensa del consumidor electrónico - el papel del conocimiento y la contratación", en *REDI: Revista Electrónica de Derecho Informático*, No. 87, Argentina, Alfa-Redi, octubre/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=3492>

¹⁸⁸ (L. Díez-Picazo, 1996: 140)

La certificación reconocida debemos ubicarla en consecuencia dentro de la categoría de contratos obligatorios, toda vez que su efecto no consiste en transmitir un derecho real (que indebidamente se podría identificar en el certificado reconocido), sino que genera entre el Firmante/Suscriptor y el PSC una relación obligatoria que origina derechos de crédito.

2.8. No es *intuitio personae*.

En la certificación reconocida, si bien es evidente que la persona que desee respaldar su firma electrónica mediante un certificado reconocido, buscará contratar a dicho fin los servicios de un PSC de su entera confianza, es decir, que su elección de entre todos los posibles certificadores que operan en el mercado, se basará finalmente en atención a las particulares características y distintivas cualidades de un PSC en concreto, contrariamente a lo que podría suponerse inicialmente, desde nuestro punto de vista no constituye un negocio jurídico *intuitio personae*.

Fundamentamos nuestra afirmación en atención a la disposición del art. 21 de la LFE, la cual establece que cuando el PSC vaya a cesar en su actividad, previa comunicación a los Firmante/Suscriptores que utilicen los certificados electrónicos que haya expedido así como a los solicitantes de certificados expedidos a favor de personas jurídicas, 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 PSC que los asuma.

De manera que la posibilidad prevista en la Ley de transferencia del contenido contractual de un PSC a otro, determina finalmente que este contrato no sea *intuitio personae*, como tenemos sostenido previamente.

2.9. Sinopsis.-

De todo lo reflexionado a través de la exposición que se ha efectuado sobre los caracteres esenciales de la certificación reconocida, nos parece que ha quedado suficientemente justificado que el contrato objeto de estudio constituye: un contrato

consensual, mercantil, bilateral o sinalagmático, oneroso conmutativo, con obligaciones duraderas y tracto continuado, sujeto a condiciones generales perfeccionado por adhesión, es un contrato obligatorio y no reviste carácter *intuitu personae*.

En definitiva, hasta acá se han expuesto las características fundamentales del contrato de certificación reconocida de firma electrónica, las cuales conforme venimos argumentando, serán determinantes para establecer la naturaleza y el marco jurídico aplicable al contrato.

III. Naturaleza jurídica.-

Con el concepto del contrato de certificación reconocida esbozado previamente y la identificación de sus caracteres esenciales, debemos ocuparnos a continuación de su calificación. A dicho efecto, debemos hacer notar que este negocio jurídico carece de un régimen jurídico acabado o completo, por ello y ante la insuficiencia del mismo, resulta pertinente proceder a estudiar en qué órbita o categoría de los contratos se ubica, al efecto de extraer reglas generales que le sean aplicables a objeto de determinar su naturaleza jurídica.

3.1.- Calificación del contrato.-

La calificación del contrato representa no pocas dificultades, sobre todo si consideramos la variedad de figuras contractuales cuyos elementos podrían confluir, yuxtaponerse o fusionarse al contrato objeto de estudio, por lo que cabría pensar que da lugar a una forma de contrato mixto, coligado o complejo.¹⁸⁹

Cabe advertir de inicio que la certificación electrónica en general y la reconocida en particular, es un contrato de servicios aún con escaso estudio en la doctrina y prácticamente inexistente jurisprudencia en la materia; en este último caso debido a que la mayor parte de estos contratos se someten a procesos de arbitraje o transacción, por lo que no llegan a los estrados judiciales. Por dicho motivo es que no hemos encontrado suficiente debate sobre su naturaleza jurídica, aunque podemos predecir que en la medida que surjan mayores estudios sobre esta figura negocial, este aspecto será objeto de no pacífica discusión en la doctrina.

¹⁸⁹ (L.Diez-Picazo, 1996: 388)

Como bien sabemos la calificación del contrato “*Es el acto por el cual se incluye al contrato, atendiendo a su contenido, en una de las categorías contractuales establecidas en la ley, la costumbre o la práctica o determinar su carácter atípico y los negocios con los que puede tener relación y normas que pueden ser aplicables*”.¹⁹⁰ A través de la calificación del contrato se establece en consecuencia, el tipo o clase a la que pertenece el contrato celebrado o, por el contrario, se determina su atipicidad en caso que éste no se pueda identificar con ninguno de los tipos regulados y reconocidos por el ordenamiento jurídico¹⁹¹.

La finalidad básica de la calificación de un contrato es la de establecer el régimen jurídico al que queda sometido el negocio jurídico que las partes han celebrado. Evidentemente, una vez establecido el tipo contractual ante el que nos encontramos podemos identificar las normas imperativas y dispositivas que configuran la regulación aplicable a las obligaciones de las partes.

Como es conocido la calificación del contrato es un acto sustraído de la autonomía de la voluntad de las partes. En efecto, en virtud del art. 1.255 C.c. las partes pueden libremente conformar el contenido contractual pero la determinación del régimen jurídico aplicable al contrato, consecuencia de su calificación, corresponde al legislador que es quien disciplina la relación contractual. En este sentido se ha establecido reiteradamente por parte de la doctrina y de la jurisprudencia que habrá que estar, en todo caso, a la esencia misma del negocio y al fin perseguido y no a la denominación que le hayan dado las partes.¹⁹²

Tradicional y doctrinalmente se establecido que hemos de atender a la causa del contrato para su calificación.¹⁹³ Conforme hace notar el autor José A. Vega, la naturaleza de

¹⁹⁰ J.L. Lacruz Berdejo, y otros, *Elementos de derecho Civil II. Derecho de obligaciones*, vol. I. (revisada y puesta al día por F. Rivero Hernández), Madrid, 2000, p. 510.

¹⁹¹ (J.L. Lacruz y otros, 2000: 510).

¹⁹² Así, entre otras, la STS 26 de abril de 2005 establece expresamente que “*la doctrina jurídica ha señalado que la naturaleza de un negocio jurídico depende de la intención de los contratantes y de las declaraciones de voluntad que la integran y no de la denominación que le hayan atribuido las partes, siendo el contenido real del contrato el que determina su calificación*”.

¹⁹³ Al respecto, Martín-Ballesteros establece que “*la causa es la tipicidad. Es el nomem iuris del contrato. Es la definición concreta y específica de lo que se opera en el tráfico jurídico, de aquello que tiene en la ley un concepto definido, y a lo que la ley por ello le hace seguir toda una serie de consecuencias previstas de antemano*”. L. Martín-Ballesteros, *De la causa en los negocios jurídicos contractuales*, RGLJ, 1956. p. 704.

un contrato se encuentra ligada con la causa eficiente o determinante del mismo.¹⁹⁴ De tal modo que hablaremos de la existencia de un contrato típico cuando su naturaleza jurídica se encuentra establecida en el marco normativo positivo. Ello independientemente de que el objeto del contrato sea plural (ya que no se debe confundir el objeto del contrato con la causa), toda vez que es perfectamente factible que el contrato responda a una unidad de causa, con lo que estaríamos en presencia de un contrato complejo con causa única. Asimismo diremos que de conformidad con el art. 1.277 C.c., en todo contrato se presume la licitud de la causa, por lo que ésta goza de la debida protección legal.

Pero en el caso de los contratos atípicos, mismos que de igual manera gozan de la presunción de licitud de la causa, a objeto de poseer un claro entendimiento de la función negocial resulta importante averiguar el fundamento de su causa.¹⁹⁵

En el ordenamiento jurídico español así como varios de los sistemas jurídicos *romano-germánicos*, una de las funciones que cumple la causa es la valoración de cada negocio, la cual dependerá en última instancia del resultado objetivo y concreto que las partes persiguen con la ejecución del negocio jurídico.¹⁹⁶ En ese entendido y conforme el criterio de Vega, para una calificación objetiva del contrato debe atenderse al criterio de la causa; de manera que si la causa es única - razona - el contrato será uno; pero si hay una pluralidad de causas, el contrato será plural.¹⁹⁷ Finalmente debemos caer en cuenta que nos encontraremos en presencia de un nuevo contrato cuando su causa sea distinta a la de los contratos conocidos.

Ahora bien, la causa unas veces se encontrará prevista por el ordenamiento legal, supuesto en el que existiría un negocio jurídico o contrato típico. Otras veces es factible que

¹⁹⁴ José Antonio Vega Vega, *El contrato de permuta financiera*, Navarra, Arazandi, 2002, p.55.

¹⁹⁵ En los contratos típicos - enseña Díez-Picazo - la causa se desprende del tipo negocial al que las partes acuden, de modo que la respuesta se halla implícita en el ordenamiento jurídico. En tanto que en los contratos atípicos, la respuesta se debe efectuar en base a la valoración de los tipos socialmente reconocidos (L. Díez-Picazo, 1996: 236).

¹⁹⁶ Federico De Castro y Bravo, *El negocio jurídico*, Madrid, INEJ, 1967, p. 191.

¹⁹⁷ (J. Vega, 2002: 55). Un mayor análisis de la relación entre el tipo con la causa, lo podemos encontrar en J.A. García-Cruces, *El contrato de factoring*, Madrid, Tecnos, 1990, p. 46 y ss. p. 111 y ss..

no se encuentre contemplada por la normativa jurídica, ocasión en la que existiría un negocio jurídico o contrato atípico. En base a las reflexiones previas se hace factible determinar el vínculo que existe entre la causa y la naturaleza jurídica de un contrato, al mismo tiempo que se dilucida la conexión que existe entre causa y tipicidad. En ese entendido, la causa - vista desde el criterio objetivo como subjetivo - permitirá efectuar la cabal diferenciación de un contrato con otro; por consiguiente, la causa establecerá la naturaleza del negocio jurídico que celebran las partes, del que devienen las implicaciones que las normas legales adjudican a su naturaleza.

Como es muy sabido, en los sistemas jurídicos pertenecientes a la familia romano-germánica (entre los que se encuentra el español) la teoría de de la causa es un asunto de poca claridad y bastante complejidad. El art. 1.274 del C.c. hace alusión a lo que se entiende por causa para cada parte negocial; por su parte el art. 1.261 del mismo cuerpo legal se refiere a “*la causa de la obligación que se establezca*” en el contrato.

La doctrina estudia la causa del contrato desde diferentes perspectivas, en procura de dar respuesta a las siguientes interrogantes: ¿Qué debe entenderse por causa?, ¿Cuáles son las funciones que cumple?, ¿Cuál es su ámbito de aplicación?, habiéndose manifestado de forma reiterada sobre estas cuestiones.¹⁹⁸ Precisamente a continuación procuraremos analizar de manera general en qué consisten las teorías formuladas al respecto, con la advertencia sin embargo, que los instrumentos europeos de unificación del Derecho de contratos no exigen, en ningún caso, la existencia de este requisito para la validez del contrato celebrado. Podemos afirmar, por tanto, que las funciones que en nuestro Derecho se han atribuido a la

¹⁹⁸ Díez-Picazo identifica dentro de la teoría de la causa, cuatro variedades: causa de la atribución, causa de la obligación, causa concreta y causa del negocio, a esta última, la denomina también como causa eficiente o determinante. Asimismo, respecto de las teorías objetivas, señala que éstas equiparan la causa con la función económico social del negocio, pero desde su punto de vista, esto no es causa del negocio, sino función del negocio (L. Díez-Picazo, 1996: 234).

causa se pueden llevar a cabo a través de otros expedientes, demostrándose que este elemento es, en cierto modo, prescindible.¹⁹⁹

Para algunos autores, entre ellos Gete-Alonso y Calera, la causa se exige en realidad de cada una de las obligaciones que surgen del contrato y, por consiguiente, no puede ser referido al contrato en su conjunto.²⁰⁰ De ese modo se ha razonado que la causa de la obligación responde a la pregunta ¿por qué se debe?, entendiéndose como la razón objetiva e inmediata aprobada por el Derecho, por la cual el deudor se ha obligado.²⁰¹ Adscribiéndonos a esta definición, la causa de la obligación es siempre la misma para cada obligación y resulta objetiva, de tal forma que en este concepto se no incluyen, en ningún caso, los móviles subjetivos de las partes contractuales.²⁰²

Confrontados con los autores que defienden que únicamente las obligaciones tienen una causa, otros, como De Castro, opinan que este elemento se exige del contrato en su conjunto.²⁰³ Dentro de los diferentes conceptos de causa del contrato destacamos en primer lugar, la teoría objetiva de la causa, según la cual ésta consiste en el fin objetivo y típico del negocio. En este sentido se manifiesta por ejemplo Jordano al exponer que “*la causa del contrato en sentido técnico consiste en el fin objetivo, reconocido como válido y digno de*

¹⁹⁹ Al respecto, Fajardo expone que la simulación del contrato regulada en el art. 6.103 PECL se plantea como falta de auténtico acuerdo entre las partes, produciéndose el mismo resultado, este es, la no validez del contrato. Por lo que se refiere a la resolución del contrato por incumplimiento, el principio de cumplimiento simultáneo de las obligaciones recíprocas o el reequilibrio de las prestaciones, pueden encontrar remedios independientes de la causa (Capítulo 9 PECL). Por otro lado, con respecto a la ilicitud de la causa, es “*perfectamente sustituible por una exigencia de legalidad y moralidad del contrato entendido en su conjunto*”. J. Fajardo Fernández, *Derecho privado Europeo*, S. Cámara Lapuente, comp., AAVV, Madrid, 2003, pp. 410 - 414.

²⁰⁰ Gete-Alonso y Calera sostiene que “*la causa recogida en el Código Civil es la causa de la obligación en cuanto que elemento sobrevenido al consentimiento que limita su eficacia nuda, cumpliendo la función de ser el fundamento jurídico de la obligación contractual*”. M^a. C., Gete-Alonso y Calera, *Estructura y función del tipo contractual*, Barcelona, 1979. p.543.

²⁰¹ Valpuesta la concibe en términos similares, como la razón jurídica que sirve para explicar la existencia y la permanencia de la obligación. Rosario Valpuesta Fernández, “Elementos esenciales del contrato”, en *Derecho Civil. Derecho de Obligaciones y contratos*”, A. López y López, V.L. Montés Penades, E. Roca I Trias (directores), AAVV, Valencia, 2001, p. 242.

²⁰² F. Sancho Rebullida, *Notas sobre la causa de la obligación en el Código Civil*, RGLJ, 1971, p. 671.

²⁰³ De Castro argumenta que “*la frase <causa de la obligación> del artículo 1.261 C.c., para que tenga sentido ha de entenderse no como <causa de la obligación que se establezca>, sino como diciendo <causa de la relación obligatoria que se establezca>, que es el significado con el que se utiliza otras veces también el término obligación (así, por ejemplo, en los artículos 1112 y 1303)*”. Asimismo señala que “*el artículo 1274, en su letra, es cierto que se refiere a cada parte, respecto de los contratos onerosos, pero considera en ellos unitariamente, como causa del todo el contrato, al servicio o beneficio, y la liberalidad de los remuneratorios y de beneficencia*”. Federico De Castro y Bravo, *El negocio jurídico*, Madrid, 1985, p. 186.

tutela por el ordenamiento jurídico por el cual cada parte se vincula a efectuar la prestación”.²⁰⁴

Frente a la noción objetiva de causa ha surgido un concepto subjetivo, que identifica la causa con los motivos o móviles internos que han llevado a las partes a contratar.²⁰⁵ Siguiendo este concepto, si dichos móviles resultan contrarios a la ley o a la moral, el contrato no producirá efecto alguno por aplicación del art. 1.275 C.c..²⁰⁶ Esta teoría sin embargo, se ha encontrado con el inconveniente de determinar en qué casos y con que alcance deben ser los móviles de las partes jurídicamente relevantes.²⁰⁷

Para concluir, debemos señalar que otro sector de la doctrina se ha esforzado por desarrollar una definición ecléctica de la causa, entre los que resalta Clavería, en cuyo criterio la causa del contrato corresponde a la *“función práctica social concreta querida por las partes al celebrar el negocio, es decir, aquello en lo que consienten comprendiéndose en esta función el motivo determinante común a ambas partes o al menos admitido por uno al ser pretendido por el otro”*.²⁰⁸ El referido autor expone que esta noción de la causa posee la ventaja de un carácter unitario, de manera que sirve de justificación no únicamente de los contratos sino también de las obligaciones y desplazamientos patrimoniales.²⁰⁹

A los fines de la presente investigación en nuestro criterio, la causa ha de referirse de modo exclusivo a las obligaciones nacidas del contrato, configurándose como un requisito necesario para establecer en qué casos la autonomía de la voluntad genera relaciones jurídicamente vinculantes²¹⁰. En este sentido se define en el art. 1.274 C.c., que identifica la causa en los contratos onerosos, a la prestación o promesa de prestación de la otra parte y en

²⁰⁴ J. Jordano Barea, *Los contratos atípicos*, RGLJ, 1953. p. 68. // Al respecto consultar también (L.Diez-Picazo, 1996: 228-229)

²⁰⁵ (L.Diez-Picazo, 1996: 229).

²⁰⁶ (L.Diez-Picazo, 1996: 240).

²⁰⁷ (R.Valpuesta, 2001: 244).

²⁰⁸ L.H. Clavería Gosálbez, *La causa del contrato*, Bolonia, 1998. p. 134.

²⁰⁹ (L.H.Clavería, 1998: 114)

²¹⁰ (L.Diez-Picazo, 1996: 232-236)

los gratuitos, al ánimo de liberalidad del bienhechor (*animus donandi*)²¹¹. Evidentemente, el art. 1.261 C.c. dispone expresamente que no existe contrato si no cuando concurre una *causa de la obligación* que se establezca, exigiéndose este requisito por tanto, de las obligaciones del contrato y no de éste en su conjunto.

Conforme hemos venido sosteniendo la calificación del contrato supone la búsqueda del derecho aplicable al mismo, tarea para la cual resulta necesario acudir al recurso de la analogía como operación medial que se utiliza con el fin de determinar, si el tipo previsto en la legislación resulta similar al contrato que se quiere calificar y, en caso afirmativo, el régimen jurídico legal previsto será aplicable al contrato que estudiamos.

Consideramos por tanto, que para fijar la naturaleza jurídica del contrato de certificación reconocida de firma electrónica, debemos atender al propio esquema del tipo y al propósito contractual concreto que se persigue con el mismo, esto es, al fin perseguido objetivamente por las estipulaciones propias del contrato de certificación reconocida y que se repite en todos ellos, sin que esto pueda denominarse, por carecer de base legal alguna, causa del contrato.²¹² Partiendo de ello debemos determinar si existe en el ordenamiento un esquema prefijado similar y si es posible, como venimos manifestando, la aplicación analógica del régimen previsto para aquél al contrato objeto de nuestro estudio.

Como es conocido la analogía es un procedimiento de creación de normas jurídicas para el caso concreto, partiendo de lo que se encuentra creado a fin de aplicarlo a lo abstracto, de manera que lo que nos proponemos en esta investigación es iniciar con las normas abstractas creadas para otros tipos contractuales, con el objetivo de obtener el precepto que se

²¹¹ (L.Díez-Picazo, 1996: 226)

²¹² Díez-Picazo señala que lo que define y delimita los tipos contractuales o los tipos negociales es la función que realizan, la finalidad que desempeñan dentro de la vida social, el resultado o resultados empíricos que con ellos tratan las partes de obtener, denominando el autor a este resultado *causa del negocio* (L.Díez-Picazo, 1996: 234-236).

encuentra en ellas y aplicarlo a nuestro contrato, configurándose por consiguiente en un proceso de creación del Derecho arrancando de las normas ya previstas.²¹³

Conforme hemos tenido la oportunidad de analizar previamente, el tipo del contrato de certificación reconocida se encuentra definido por la concatenación de un conjunto de prestaciones (alternativamente de dar, hacer y no hacer) de las partes contratantes, obligaciones que en el caso del PSC consisten fundamentalmente en la emisión y entrega de un certificado reconocido junto con la obligación de proporcionar los servicios de directorio y verificación del certificado, a cambio de un precio en dinero que debe satisfacer el cliente o Firmante/Suscriptor.

El propósito contractual que define al mismo es, por tanto, la identificación - en sentido amplio - de los operadores económicos en el tráfico virtual, como requisito imprescindible para generar un entorno seguro y confiable.²¹⁴ En tanto que el objeto del contrato se encuentra representado, esencialmente por el certificado reconocido y por el conjunto de actuaciones que despliega el PSC dirigidas a la identificación fiable y segura del Firmante/Suscriptor, a través de las aplicaciones tecnológicas de la Infraestructura de Clave Pública (ICP).²¹⁵

Tomando en consideración estas precisiones, el contrato de certificación electrónica podría ser identificado - al menos en principio - con los siguientes tipos contractuales: con el contrato de mandato y con los contratos de arrendamientos de obra y servicios. Pasemos a analizar cada una de estas posibilidades, para ello, acudiremos básicamente al análisis comparativo de la causa y el objeto del contrato que hacen a los negocios jurídicos previamente enunciados, respecto de la causa y el objeto del contrato que hacen a la certificación reconocida.

²¹³ Como pone de manifiesto Ángel M. López y López, “Conversaciones con difuntos. Luigi Caiani: analogía”, *Quaderni Fiorentini per la storia del pensiero giuridico moderno*, XXIX, 2000, p. 327, la analogía es un procedimiento de creación de normas jurídicas para el caso concreto, partiendo de lo ya creado para lo abstracto.

²¹⁴ La identificación del firmante electrónico es la causa contractual del contrato de certificación (J. F. Ortega, 2008:178).

²¹⁵ El auténtico objeto del contrato de certificación es una prestación de servicios dirigidos a la identificación en sentido amplio; prestación amplia que se manifiesta en cada una de las actuaciones concretas dirigidas a la consecución de dicho fin (J. F. Ortega, 2008:178).

3.1.1.- La certificación reconocida en la órbita del contrato de mandato.-

El art. 1.709 del C.c. español establece que “*Por el contrato de mandato se obliga una persona a prestar algún servicio o hacer alguna cosa, por cuenta o encargo de otra*”. Al respecto, el jurista Xavier O’Callaghan expresa que “*El contrato de mandato es definido en este artículo, con tal vaguedad que permite confundirlo con cualquier otro de cooperación por cuenta ajena, especialmente el de prestación de servicios*”.²¹⁶

Por esta razón considera que hay que buscar cuál es la esencia de este tipo contractual, pero alejándose de los criterios tradicionales, como el de gratuidad o el de representación y poniendo énfasis en el “*objeto del contrato*”.²¹⁷

Los caracteres del contrato de mandato, son: i) consensual, puesto que se perfecciona por el solo consentimiento de las partes intervinientes; ii) unilateral si es gratuito, bilateral si es retribuido; iii) *intuitu personae*, toda vez que se encuentra basado en la individualidad de la persona y en la confianza mutua; iv) el objeto del contrato lo constituyen actos jurídicos o la actividad jurídica; v) la causa del contrato es la ejecución de actos jurídicos por cuenta de otro; si es representativo, además se ejecutan los actos a nombre de otro.

Es necesario señalar que el mandato se subdivide en dos categorías: mandato con representación y mandato sin representación. Cuando el mandato se encuentra unido a la representación, el mandatario no sólo actúa por cuenta y en interés del mandante, sino que actúa al mismo tiempo en nombre de éste, distinguiéndose claramente la confluencia de dos negocios jurídicos, uno de carácter bilateral (el mandato) y el otro de naturaleza unilateral (la representación que se regula en el art. 1.259 C.c.), pero la característica esencial del mandato con representación es que los actos o negocios que lleva a cabo el mandatario, surten efectos en cabeza del mandante, es decir, a nombre del mandante.

En el caso del mandato sin representación, el mandatario procede a efectuar actos

²¹⁶ Xavier O’Callaghan, *Código Civil comentado y con jurisprudencia*, Madrid, 2ª ed., La Ley, 2001, pp.1781 y ss.

²¹⁷ A nuestro juicio el profesor O’Callaghan utiliza en esta parte el término “objeto” como sinónimo de objetivo y/o finalidad; y finalidad, entendida como función o propósito que se pretende conseguir, entra en el ámbito de la causa.

jurídicos por cuenta e interés del mandante, pero no en nombre de aquél sino a título personal y propio del mandatario por carecer de la representación, de modo que en este caso, el mandatario asume plena responsabilidad de los actos celebrados frente a terceros, en tanto que en el caso anterior, por los actos efectuados y encargados al mandatario, responde el mandante.

La delimitación entre el arrendamiento de obras o servicios y el contrato de mandato, ha suscitado no sólo en la doctrina y jurisprudencia española sino prácticamente en todos los ámbitos donde rige el sistema jurídico romano-germánico, profundos análisis y debate, acrecentada por la dificultosa frontera que existe entre el arrendamiento de servicios y el mandato, toda vez que ambos normalmente consisten en obligaciones de medios y no de resultado. A objeto de establecer las características distintivas entre estos contratos, se han formulado una serie de tesis que prácticamente han quedado superadas al presente, las cuales por su valor informativo nos limitaremos a enunciar, pues el contenido de éstas, se encuentra ampliamente difundido:

- i) En primer lugar, se pretendió encontrar en el carácter esencialmente gratuito del mandato la distinción con el arrendamiento de obras y servicios, que tienen carácter oneroso;
- ii) Otro criterio para encontrar la distinción radica en la representación que conlleva el mandato, por la cual en el mandato sea o no retribuido, se obra a nombre del mandante, en tanto que en el arrendamiento de obras o servicios se trabaja para el empleador o por cuenta independiente, pero no se le representa ni se obra a su nombre;
- iii) Otra teoría analiza la distinción de estos contratos, desde el punto de vista de la independencia de quien desarrolla la actividad frente a quien le encarga;
- iv) Algunos autores como Puig Brutau, pretendieron encontrar la nota distintiva

sosteniendo que en el arrendamiento de obras o servicios sólo se toma en cuenta la relación entre las partes que van a realizar las prestaciones convenidas (bilateralidad), en tanto que en el mandato, el mandatario gestiona los intereses de su principal frente a terceras personas (triangularidad).²¹⁸

La doctrina más recientemente desarrolló la *Tesis de la juridicidad de la actividad debida*, cuyo autor es Albaladejo.²¹⁹ O'Callaghan explica que de acuerdo con esta teoría, debemos prestar atención en el objeto del mandato, lo que constituye su real y consustancial esencia, que se identifica en la actividad jurídica, o más precisamente, en los actos jurídicos. El análisis de la regulación completa de este tipo contractual en el C.c., permite inferir que la función del mandatario consiste en ejercitar una actividad jurídica relevante, la cual incidirá en el ámbito jurídico del mandante, con la observación que no es necesario que tales actos se configuren en negocios jurídicos. De manera que constituyendo la esencia del mandato su objeto, el cual está conformado por la actividad jurídica, O'Callaghan define al mandato “como el contrato consensual por el que una persona, mandatario, se obliga hacia otra, mandante, a realizar algún acto jurídico, por cuenta de ésta”.²²⁰

Por otra parte, García Valdecasas formuló la *Teoría de la posibilidad de sustitución en ejecución de la actividad*, por la cual se sostiene que el dato que caracteriza al mandato es el de recaer tan sólo en los actos en que cabe la sustitución del mandante, que puede referirse a los actos jurídicos como los no jurídicos, incluyendo los puramente materiales. En tanto que forzosamente serán objeto del arrendamiento de obra o servicios, aquellos actos que por no pertenecer a la esfera de la propia actividad, de ningún modo realizaría el mandante, y por tanto, tampoco puede hacerse sustituir para el cumplimiento de los mismos.²²¹

Ahora bien, a efectos de nuestro estudio consideraremos de todas las teorías

²¹⁸ José Puig Brutau, *Fundamentos de Derecho Civil*, T.II, vol. II, *Contratos en particular*, Barcelona, 1982, pp. 395-396.

²¹⁹ Manuel Albaladejo García, *Derecho Civil*, T.II, *Derecho de obligaciones*, vol. II, *Los contratos en particular y las obligaciones no contractuales*, 9ª ed., Barcelona, 1994, pp.319-321.

²²⁰ (X. O'Callaghan, 2001: 1781 y ss.)

²²¹ Guillermo García Valdecasas, “La esencia del mandato”, en *Revista de Derecho Privado*, 1944, pp. 769-776.

anteriormente señaladas, las dos últimas, toda vez que vienen siendo las de mayor aceptación por la doctrina en la actualidad.

De entrada, señalaremos que vistos el objeto y la causa del contrato de prestación de servicios de certificación reconocida de firme electrónica, éstos no encajan dentro del contrato de mandato, ya que siguiendo el razonamiento de la *Tesis de la juridicidad de la actividad debida*, en el caso del mandato, sea con o sin representación, el objeto del contrato lo constituyen actos jurídicos y la causa del contrato estriba en la ejecución por parte del mandatario de dichos actos o negocios jurídicos por cuenta y en interés del mandante; en tanto que en la certificación reconocida, el objeto del contrato esta representado fundamentalmente por un servicio -y secundariamente por el certificado- que no pueden ser considerados técnicamente como un “*acto jurídico*”.

La causa del contrato consiste en la actividad profesional que despliega el PSC a objeto de identificar de manera indubitable al Firmante/Suscriptor, dotando con ello de seguridad y confianza a las transacciones de comercio electrónico, gestión que el PSC lleva a cabo no por cuenta y en interés únicamente del Firmante/Suscriptor, sino que es un servicio que lo despliega por cuenta propia y en interés del colectivo de personas que participan en el espacio virtual, en otras palabras, en función de un interés superior y social de seguridad jurídica y certeza, sin que ello quiera decir que el PSC actúa cumpliendo el rol que la ley a reservado a los notarios, pues el certificador no da fe pública, pero comprendemos que desempeña una labor que reviste un interés social.

Asimismo, si nos adscribimos a la *Teoría de la posibilidad de sustitución en ejecución de la actividad*, la cual postula como rasgo distintivo entre el mandato y el arrendamiento de obras o servicios la posibilidad de sustitución, resulta evidente que el Firmante/Suscriptor no puede hacerse sustituir por el PSC, toda vez que la actividad de certificación no pertenece a la esfera de la propia actividad del Firmante/Suscriptor, más todo lo contrario, constituye una

actividad alta y sensiblemente especializada que requiere no solo de particulares destrezas profesionales sino de una compleja organización, tanto a nivel técnico como de medios e infraestructura.

Pero por encima de ello hay que razonar sobre lo siguiente, en el caso del mandato, con o sin representación, el mandatario actúa a nombre o por cuenta - respectivamente - del mandante; en tanto que en la certificación reconocida lo que se busca es precisamente un tercero ajeno e independiente a la esfera del Firmante/Suscriptor, un sujeto que no actúe a nombre o por cuenta de otro, sino que actúe por cuenta propia y en función de un interés superior al del Firmante/Suscriptor, que de modo imparcial de cuenta sobre la identidad del Firmante/Suscriptor frente a terceros, asumiendo con su actividad evidentemente un riesgo y encontrándose sujeto a un régimen de responsabilidades muy estricto y concretamente delimitado, pero cumpliendo más allá de su relación comercial con el Firmante/Suscriptor, una verdadera función de interés social, razón por la que el ordenamiento jurídico tutela el ejercicio de este tipo de actividad.

Aún en el caso concreto del mandato sin representación, en el que por definición el mandatario actúa por cuenta propia e independientemente del mandante - lo que podría suscitar alguna duda sobre la tesis sostenida líneas previas - no puede dejar de verse que existe un cierto nivel de colusión y lealtad entre mandante y mandatario, que llegado el caso, y admitiendo que la certificación reconocida se asimile con el mandato, podría determinar una falta de imparcialidad o encubrimiento de irregularidades entre Firmante/Suscriptor y PSC, lo que restaría seguridad y confianza en los usuarios de certificados.

Por los argumentos expuestos, descartamos la posibilidad de que el contrato de certificación reconocida pueda enmarcarse como un contrato de mandato.

3.1.2.- La certificación reconocida en la órbita del contrato de obra.-

Por otra parte, cabe la posibilidad de asimilar la certificación reconocida con el arrendamiento de obra (arts.1.542, 1.544, 1.588-1.600 C.c.). Para analizar dicha probabilidad reflejaremos en primera instancia el contenido del art. 1.542 C.c., por el cual queda claro que para el ordenamiento jurídico formal español el arrendamiento puede ser “*de cosas, o de obras o servicios*”. De la lectura del art. 1.544 C.c., se establece que en “*el arrendamiento de obras una de las partes se obliga a ejecutar una obra a la otra por precio cierto*”. A su turno el art. 1588 C.c. especifica que “*puede contratarse la ejecución de una obra conviniendo en que el que la ejecute ponga solamente su trabajo o su industria, o que también suministre el material.*” De la lectura de las disposiciones citadas, queda claro que el objeto del contrato es una obra (una cosa) y que el contrato encuentra su causa precisamente en la ejecución de la obra convenida.

Los caracteres del contrato de obra son: i) consensual, puesto que se perfecciona por el solo consentimiento de las partes intervinientes; ii) sinalagmático, puesto que cada parte tiene derecho y acción para exigir de la contraparte la prestación que debe; iii) oneroso conmutativo, toda vez que existen contraprestaciones recíprocas y cada una de las partes tiene en cuenta la adquisición de un equivalente de su prestación, pecuniariamente apreciable desde el momento de la celebración del contrato; iv) no formal, pues no requiere de forma expresa; v) el objeto del contrato es crear una cosa material o inmaterial, o intervenir sobre una cosa de existencia previa, ampliando las funcionalidades del primero: la obra en sí; vi) la causa del contrato es sujetar la realización de la obra a las reglas del arte.

El estudio de los artículos subsiguientes (1589-1600 C.c.), revela que el empleo de las palabras: construcción, materiales y destrucción de la obra son predominantes, denotando con ello que el legislador tiene en mente fundamentalmente la ejecución de obras que repercuten sobre bienes inmuebles (v.gr. construir un edificio, pintar una casa, etc.) y, con menor

incidencia, la ejecución de obras que repercuten sobre bienes muebles (v.gr. desarrollar un artefacto que no existía previamente, o, a partir de un artefacto de existencia previa, desarrollar uno nuevo ampliando las funcionalidades del primero, etc.).²²²

Ello nos lleva a concluir ateniéndonos al espíritu codificado, que el legislador preponderantemente concibe al objeto del contrato, es decir la obra, ligado a un componente de materialidad “una cosa”. En otras palabras, la obra consiste en una cosa material, ya sea edificando algo que no existía previamente, ya sea efectuando reparaciones, adaptaciones, etc. sobre una cosa material de existencia anterior; en uno u otro caso, la nota sobresaliente es la sustanciación y objetivación material de la obra.

Por consecuencia, el objeto de la obligación es básica e inicialmente una prestación de hacer “ejecutar la obra (hacer una cosa)”, pero que tiene aparejada una prestación complementaria de dar “entregar la obra (dar la cosa)”. Lo que nos lleva a afirmar por consecuencia, que el arrendamiento de obra genera una obligación de resultado. Y ello es evidente, pues la única manera en que el deudor puede cumplir su obligación es haciendo y entregando un resultado concreto: la obra material. En ausencia material de la obra, el acreedor no satisface su interés y el deudor no se libra de la obligación.

Ahora bien, cabe hacer notar que como consecuencia del desarrollo doctrinal se ha dado paso a concebir “la cosa” en un sentido amplio, no solo como algo material sino también inmaterial. En otras palabras, las cosas no necesariamente están ligadas a un componente de materialidad, pues pueden perfectamente existir cosas de carácter inmaterial que igualmente constituyen bienes sobre los que recae un interés de las partes.²²³

Por ello es que a momento de hablar del objeto del contrato, la doctrina moderna (frente a la tradicional que veía como objeto del contrato a las cosas y los servicios) con

²²² Al respecto consultar Judith Sole Resina, *Arrendamiento de obras o servicios*, Valencia, Tirant Lo Blanch, 1997, pp. 83 y ss.

²²³ Sobre el tema la autora Trigo sostiene que los arts. 1.588 y ss. C.c., relativos al contrato de obra, parecen estar pensados para obras materiales, casi exclusivamente, pero explica que también se utiliza el término cuando se trata de una creación literaria, científica o artística; por tanto, con carácter general, obra implica actividad tendente a un fin y resultado de la actividad, consista éste en un nuevo objeto del Derecho o no, y sea su naturaleza material o inmaterial. Belén Trigo García, *Contrato de servicios. Perspectiva jurídica actual*, Granada, COMARES, 1999, pp. 175-176.

carácter más acertado prefiera referirse al objeto del contrato como los bienes susceptibles de una valoración económica que corresponde a un interés de las partes.²²⁴ Los bienes son de una naturaleza amplia y variada, unos gozan de materialidad y otros no.

Desde ese punto de vista, es perfectamente posible que el objeto del arrendamiento de obra revista de inmaterialidad, es decir, la obra pueda consistir en una cosa inmaterial y no únicamente en una cosa material. El ejemplo típico señalado por la doctrina en este caso son las obras intelectuales, literarias, científicas o artísticas. Pero nótese que en cualquiera de los dos casos, sea que la obra goce de materialidad o sea que consista en algo inmaterial, lo común es que se busca y persigue un resultado concreto: una obra. En ausencia de la obra no se consigue el resultado buscado por el acreedor.

Sintetizando ideas podemos señalar que el arrendamiento de obra (de conformidad al tipo codificado), pero más propiamente el contrato de obra (construcción doctrinal²²⁵ y jurisprudencial²²⁶ española, que concibe a la obra como un contrato autónomo e independiente del arrendamiento), tiene como objeto del contrato una obra - misma que puede gozar o no de materialidad - siendo la causa del contrato precisamente ejecutar la obra, por lo cual se genera inicialmente una prestación de hacer, pero que se complementa con una obligación de dar. Finalmente, sea que la obra consista en algo material o inmaterial la obligación del deudor es de resultado.

Llegado este punto es necesario hacer un par de matizaciones, a cuyo objeto y con carácter previo señalaremos que la clasificación en obligaciones de medios o de resultado, ha sido el criterio que tradicionalmente ha empleado la doctrina y la jurisprudencia para delimitar y diferenciar al contrato de obra del contrato de servicios, pues se dirá, que este

²²⁴ (L. Díez-Picazo, 1996: 202).

²²⁵ La configuración actual del contrato de servicios y de obra en el Derecho español se corresponde en principio con el modelo alemán de dos contratos, y no con el de un contrato (arrendamiento) con prestaciones diferentes. Sin embargo, se ha aceptado de modo mayoritario la dicotomía obligación de medios y obligación de resultado, tanto por la doctrina como por la jurisprudencia, utilizándola preferentemente para la delimitación entre contrato de servicios y contrato de obra (B. Trigo, 1999: 185 y ss.).

²²⁶ Sobre la construcción jurisprudencial del contrato de obra, consultar las Sentencias del Tribunal Supremo: 10 de junio de 1975 (RJA 1975, núm. 3265); 19 de junio de 1982 (RJA 1982, núm. 3433); 29 de septiembre y 3 de noviembre de 1983 (RJA 1983, núms. 4685 y 5953); 29 de junio de 1984 (RJA 1984, núm. 3441); entre otras.

último trae aparejadas - por definición - obligaciones de medios. Y ello - en principio - es evidente, pues quien presta un servicio, por ejemplo un profesional médico no puede asegurar la cura a su paciente, como tampoco un abogado puede asegurar que ganará el juicio a favor del litigante que patrocina. Con estas aclaraciones analicemos las dos observaciones enunciadas.²²⁷

La primera, va en sentido que si bien la doctrina ha dado por sentado durante bastante tiempo que en los contratos de obra y de servicios confluyen obligaciones de resultado y de medios respectivamente,²²⁸ no es menos evidente que las partes haciendo empleo de la libertad contractual bien podrían negociar alcances distintos respecto de estas obligaciones, así, nada obsta para que en un contrato de obra las partes de mutuo acuerdo convengan que el contratista habrá cumplido con su obligación, aún cuando no llegue efectivamente a entregar la obra, si demuestra que empleó todos los medios necesarios al alcance para su consecución.

Por contramano, nada limita a las partes para que de mutuo acuerdo negocien un contrato de servicios donde el deudor únicamente dará por cumplida su obligación, a momento de concretar un resultado buscado con el servicio. Por consiguiente, habrá que tomar muy en cuenta la voluntad de las partes a momento de interpretar el contrato.

La segunda, va en sentido que si bien se da por contado que en un contrato de servicios sobrevienen obligaciones de medios, no es menos evidente que existen fases a lo largo de la prestación del servicio que necesariamente involucran resultados. Por ejemplo, siguiendo el caso de los servicios ofrecidos por un profesional abogado que ha sido contratado para llevar adelante un juicio, como sosteníamos anteriormente, éste no puede

²²⁷ Detengámonos brevemente a analizar la consecuencia práctica de esta diferenciación. La división entre obligaciones de medios y resultado, apunta a contar con criterios que ayuden a establecer con claridad las responsabilidades que surgen para las partes contractuales. La responsabilidad puede ser objetiva o subjetiva; cuando la responsabilidad se enmarca en criterios subjetivos, se funda en la culpa como elemento de valoración e imputación del daño, únicamente quien actuó culposamente es responsable por el daño ocasionado y está en la obligación de repararlo. De esa manera, en las obligaciones de resultado, el acreedor no debe probar la culpa del deudor en el daño ocasionado sino que simplemente debe demostrar que no obtuvo el resultado esperado, se presupone la culpa del deudor. Recae en consecuencia en el deudor la carga de demostrar que el daño en todo caso no fue ocasionado por su culpa, sino que sobrevino un hecho fortuito o causa mayor. En tanto que en las obligaciones de medios, es el acreedor quien tiene la carga de probar la culpa del deudor en el daño ocasionado.

²²⁸ Como hace notar Trigo, no existen criterios de distinción entre obligaciones de medios y de resultado explicitados por la ley, sino que éstos constituyen aportaciones doctrinales y jurisprudenciales, en parte recogidas del art. 5 de los Principios de UNIDROIT (B. Trigo, 1999: 190).

asegurar a su cliente que ganará el juicio, no puede garantizar un resultado: una sentencia favorable al litigante que patrocina.

Pero sí está obligado a una serie de resultados concretos: reunirse con su cliente para tomar conocimiento del problema, elaborar un memorial fundamentado, presentar los recursos que correspondan en los plazos establecidos por ley, etc. En todos ellos no puede dejar de apreciarse que existen resultados a los que el profesional está obligado. Pero evidentemente no cabe duda que del conjunto e integración del contrato, de su objeto y su causa, la obligación última es una obligación de medios.

Lo anteriormente expuesto lleva a que en la práctica la distinción de obligaciones como de medios o resultado, resulte una frontera muchas veces con una delimitación poco clara y confusa. Por ello es que la doctrina y jurisprudencia contemporáneas han experimentado con el tiempo cierta moderación en el tema, y hoy en día, ya no se acepta con carácter absoluto como criterio distintivo entre el contrato de obra y servicios, la confluencia de obligaciones de medios o resultado por las razones expuestas.²²⁹

Al presente es necesario hacer notar que a la distinción entre obligaciones de medios y resultado le espera un nuevo horizonte, con el reconocimiento expreso o tácito en las llamadas normas del *soft law*²³⁰ y el Anteproyecto de Pávia de Código Europeo de Contratos (CEC).²³¹

En base a las consideraciones previamente estudiadas, corresponde volver nuestra atención al contrato objeto de estudio y hacer las comparaciones pertinentes con el contrato de obra, a efectos de determinar si la certificación reconocida encuadra, o no, dentro de la categoría típica de contrato de arrendamiento de obra.

²²⁹ Sobre las consideraciones anotadas recomendamos consultar el trabajo de Belén Trigo, quien desde nuestro punto de vista efectúa un análisis muy exquisito y completo respecto de las obligaciones de medios y resultado, el cual en gran medida contribuyó a las reflexiones y conclusiones por nosotros planteadas en esta parte (B. Trigo, 1999: 229 y ss.) // En idéntico sentido la obra de María Dolores Cervilla Garzón, *La Prestación de servicios profesionales*, Valencia, Tirant Lo Blanch, 2001, p. 98 y ss..

²³⁰ Las normas del *soft law* están integradas por: los Principios UNIDROIT sobre los contratos comerciales internacionales; los Principios del Derecho Europeo de los Contratos (Principles of European Contract Law - PECL), y los Principios de Derecho Europeo - Contratos de Servicios (Principles of European Law - Service Contracts PEL-SC)

²³¹ Publicado por la Academia de Iusprivatistas Europeos con sede en Pavía, cuya redacción definitiva estuvo a cargo del Prof. Giuseppe Gandolfi.

A dicho propósito señalemos que el PSC posee como primera obligación la emisión de un certificado reconocido (un hacer), el cual constituye un documento electrónico razón por la cual no reviste de materialidad, toda vez que su soporte es un medio digital. Como se tiene dicho el objeto del contrato de obra puede ser una cosa inmaterial, de manera que el certificado reconocido constituye ese bien susceptible de una valoración económica que corresponde a un interés de las partes. En consecuencia, en la certificación reconocida existe una obra representada por el certificado. Pero además de elaborar el certificado reconocido, el PSC debe entregar (un dar) una copia del mismo al Firmante/Suscriptor.

Hasta acá resulta evidente que surge para el PSC una obligación de resultado: i) primero, porque debe emitir un certificado que contenga todos los datos del Firmante/Suscriptor correctamente registrados, un error en la consignación de los datos del Firmante/Suscriptor no logra la identificación inequívoca; ii) segundo, porque además de emitir el certificado el PSC está en la obligación de entregar una copia al Firmante/Suscriptor. Nótese en consecuencia, que emisión correcta y entrega efectiva del certificado al Firmante/Suscriptor determinan que la obligación del PSC se configure como una obligación de resultado. En tanto que el PSC no emita un certificado veraz y lo ponga a disposición del Firmante/Suscriptor, éste no se libra de su obligación.

Pero el fin último buscado por el Firmante/Suscriptor al contratar con el PSC, que es su identificación cierta y segura en una red de comunicación abierta, no se logra únicamente con la emisión y entrega del certificado al Firmante/Suscriptor, sino que éste debe ser publicado por el PSC en un directorio de consulta por parte de terceros, a objeto que accedan a la clave pública asociada al certificado, con la cual llevaran a cabo la validación de la clave privada del Firmante/Suscriptor, lo cual únicamente se consigue con la prestación de un servicio ulterior de consulta y verificación de certificados.

Por tanto, descartamos las prestaciones de emitir el certificado (un hacer) y entregarlo al Firmante/Suscriptor (un dar) como únicos objetos de la obligación, pues la prestación del PSC no se limita simplemente a emitir y entregar el certificado sino a otra serie de obligaciones de hacer y de no hacer, como administrar el sistema tecnológico, que incluye la suspensión y revocación de certificados, la emisión de un listado de certificados para determinar su vigencia, no copiar los datos de creación de firma, etc..

Por los argumentos expuestos, descartamos la posibilidad de que el contrato de certificación reconocida pueda enmarcarse como un contrato típico de arrendamiento de obra, puesto que este tipo contractual no satisface integralmente el objeto y la causa de la certificación reconocida.

Sostenemos esta afirmación, porque pese a que el arrendamiento de obra satisface al menos uno de los objetos de la certificación reconocida: el certificado, no satisface los servicios ulteriores necesarios para lograr la efectiva identificación del Firmante/Suscriptor frente a terceros en una red abierta de comunicaciones.

Asimismo, el arrendamiento de obra no satisface la causa del contrato de certificación reconocida, toda vez que emitido el certificado reconocido pero sin su publicación en un directorio además de la ausencia de los servicios de consulta y autenticación-verificación de certificados correspondientes, ninguna identificación segura puede generarse, a lo sumo, satisface la *auto-identificación* del Firmante/Suscriptor, pero evidentemente sin ninguna utilidad práctica.

3.1.3.- La certificación reconocida en la órbita del contrato de servicios.-

Por último, existe la posibilidad que se pretenda encontrar cabida al contrato de certificación reconocida dentro de las disposiciones que hacen al arrendamiento de servicios (arts. 1542, 1544, 1583-1587 C.c.). Para analizar dicha probabilidad reflejaremos en primera instancia el contenido del art. 1544 C.c., por el cual queda claro que para el ordenamiento

jurídico español en “*el arrendamiento de servicios una de las partes se obliga a prestar un servicio a la otra por precio cierto*”. A su turno, el art. 1583 C.c. dispone: “*Pueden contratarse toda clase de servicios sin tiempo fijo, por cierto tiempo, o para una obra determinada. El arrendamiento hecho por toda la vida es nulo*”.

Finalmente los arts. 1584 a 1587 C.c. se ocupan de los servicios prestados por los criados, menestrales, artesanos y demás trabajadores asalariados. Nótese como bien resalta Belén Trigo, que el valor de los artículos referidos en su redacción actual es por demás pobre y escaso, por lo que es prácticamente imposible edificar el estudio del contrato de servicios basándose en su ordenación codificada. A tal punto ha devenido el anacronismo del C.c. en este contrato, que en criterio de la referida autora (y el de una pluralidad prácticamente uniforme de juristas españoles) puede afirmarse que el contrato de servicios es un contrato nominado pero atípico, pues pese a su mención en la Ley carece de regulación específica, ello sin perjuicio de que revista tipicidad social.²³²

Pero además esta Sección ha quedado virtualmente derogada por la legislación laboral, especialmente por el Estatuto de los Trabajadores, según T.R. aprobado por R.D.Leg. 1/1.995, del 24 de marzo (B.O.E. del 29 de marzo), el cual se complementa con varias otras normas legales y reglamentarias. Para los contratos de servicios profesionales la Jurisprudencia española suele además aplicar - adaptándolas - las normas reguladoras del contrato de mandato.²³³

Por las razones expuestas, no es posible estudiar de modo comparado al contrato de certificación reconocida ateniéndonos a la base de la regulación codificada del contrato de servicios, lo que nos lleva a acudir a la doctrina y la jurisprudencia española así como la legislación comparada, para estudiar y comprender este negocio jurídico.²³⁴

²³² (B. Trigo, 1999: 127-128).

²³³ (X. O'Callaghan, 2001: 1653).

²³⁴ En caso contrario, tendríamos que efectuar un estudio casuista de los diferentes supuestos en los que tenga lugar un contrato atípico de servicios, tarea evidentemente nada práctica.

La noción de servicio es muy extensa y su estudio admite muchos enfoques, tanto desde la perspectiva jurídica como económica. Al interior del propio C.c. español es posible encontrar al margen del contrato de arrendamiento de servicios codificado en los arts. 1.583-1.587, una diversidad de supuestos que dan origen a una prestación de servicios.

En términos generales, las características de todo contrato de servicios son las siguientes: i) consensual, puesto que se perfecciona por el solo consentimiento de las partes intervinientes; ii) sinalagmático, puesto que cada parte tiene derecho y acción para exigir de la contraparte la prestación que debe; iii) oneroso conmutativo, toda vez que existen contraprestaciones recíprocas y cada una de las partes tiene en cuenta la adquisición de un equivalente de su prestación, pecuniariamente apreciable desde el momento de la celebración del contrato; iv) no formal, pues no requiere de forma expresa; v) el objeto del contrato es el servicio en sí mismo considerado, que debe ser posible y lícito; vi) la causa del contrato es la realización o prestación de un servicio.

En esa línea de pensamiento toda prestación de servicios tiene por objeto del contrato al servicio en sí mismo, es decir, poner a disposición los medios para satisfacer un interés. Al tenor del espíritu codificado el servicio predominantemente reviste de inmaterialidad, toda vez que el C.c. no hace ninguna referencia a la especificación de materiales, ni a la construcción de un nuevo objeto del derecho, ni a la entrega o recepción de una cosa (obligación de dar), ni al supuesto del riesgo de pérdida de la cosa debida.

De modo que la actividad que constituye el servicio - en sentido estricto - es aquella que se agota con la propia prestación. Dicho de otra manera, el servicio es una actividad considerada en sí misma donde no se suma para el deudor del servicio una obligación de *dar* a la obligación de *hacer*, debido a que con este contrato no se obtiene un nuevo objeto de derecho.²³⁵

²³⁵ Al respecto consultar (J. Sole, 1997: 84).

Pero con todo hay que efectuar una precisión. Conforme el avance de la doctrina y la jurisprudencia se ha ido admitiendo la materialización del objeto de este contrato, así, se habla por ejemplo del caso de servicios hoteleros (que es un contrato atípico de servicios), donde el servicio se concreta materialmente en ciertos resultados, como la atención personalizada al huésped, diseño de juegos recreativos, organización de paseos guiados a lugares turísticos, etc. donde se detectan unos resultados concretos.

No obstante las excepciones lo frecuente es que el objeto de la obligación en este contrato constituya una prestación de hacer, que puede ir acompañada de obligaciones de no hacer, descartándose la obligación de dar como objeto de la prestación, y por consecuencia, devienen para el deudor obligaciones de medios.

El contrato de servicios ha sufrido una vigorosa e importante evolución desde su origen en la *Locatio conductio* del Derecho Romano, este último es concebido como un contrato único que admite contenidos diversos (*Locatio conductio rei* “locación de cosas”; *Locatio conductio operis* “locación de obras” y *Locatio conductio operarum* “locación de servicios”), pasando por construcciones jurisprudenciales y doctrinales que propugnan la distinción de tres tipos contractuales diferenciados (v.gr. España), hasta las codificaciones contemporáneas que distinguen expresamente los contratos de obra y servicios del arrendamiento o locación de cosas, constituyendo en consecuencia tres tipos de contratos independientes. Figuran entre éstas últimas: el derecho portugués (1867), pero sobre todo el derecho germánico (BGB de 1900) y los influenciados por éste, como el suizo (ZGB de 1912), el brasileño (1917) y el peruano (1984); además del derecho italiano (1942).

En el caso concreto del código civil español, el arrendamiento de obras o servicios se configura como un único tipo contractual, pero la doctrina más reciente propugna la tesis de la dualidad contractual, por la cual el arrendamiento de obra se configura como un contrato

independiente al arrendamiento de servicios, criterio que viene directamente influenciado del derecho alemán.

Como es sabido, el ordenamiento alemán aborda la regulación de los contratos de obras y servicios como dos tipos separados e independientes de contratos. La distinción entre uno y otro estriba en el objeto de la obligación de hacer, ya que en la obra ésta consiste en un resultado (la obra en sí misma) en tanto que en el servicio, la obligación de hacer consiste en una mera actividad (el servicio). En ese entendido, la generalidad de autores comprenden que el BGB establece que en el caso del contrato de servicios se contrata a la actividad misma (parágrafo 611), en tanto que en el caso del contrato de obra no constituye el servicio en sí lo que se contrata sino el resultado del trabajo, resultado que puede consistir en una cosa o cualquier otro resultado producido por el trabajo (parágrafo 631).²³⁶

La autora Sole explica que la distinción fundada en el objeto de la obligación de hacer (actividad o resultado), puede resumirse del modo siguiente: si se promete una actividad o *quantum* de trabajo, hay un contrato de servicios; en cambio - sostiene - sí se promete el resultado de una actividad o resultado de trabajo (entendido en sentido jurídico, es decir, como obra conclusa y completa y no como reflejo fáctico de todo hacer) hay un contrato de ejecución de obra.²³⁷

De manera que para la doctrina española, en el contrato de ejecución de obra el contratista se hace responsable por la obtención de un resultado, constituyendo precisamente este aspecto el elemento fundamental que lo distingue del contrato de servicios.²³⁸

²³⁶ §§ 611 y 631 BGB. El objeto de la obligación del contrato de servicios y del contrato de obra es, respectivamente, el trabajo o la prestación de servicios como tal o el resultado a obtener por los mismos, de modo que los servicios no son debidos como tales en el contrato de obra, sino sólo como medios para el resultado a obtener. K. Larenz, *Derecho de obligaciones*, vol. II, versión española y notas de J. Santos Briz, Madrid, 1959, pp. 281 y 305-306.

²³⁷ (J. Sole, 1997: 141)

²³⁸ En este sentido: Ramón García de Haro de Coytisolo, en Ludovico Barassi, *Instituciones de derecho civil*, vol. II, Traducción y notas de comparación al derecho español por Ramón García de Haro de Coytisolo con la colaboración de Mario Falcón Carreras, Barcelona, 1955, p. 255 // Cebollero Valera, "Algunos aspectos del contrato de arquitecto. Los honorarios", en *Revista de Derecho Privado*, 1985, p. 926 // J. Galvez Montes, "Colegios profesionales y tarifas de honorarios de ingenieros", en *Revista de Administración Pública*, 1983, pp. 937-938 // Encarna Roca Trias, "Naturaleza de la relación entre el arquitecto y los clientes. Responsabilidad extracontractual de los arquitectos", en *Revista de Derecho Privado*, 1976, p.787 // Manuel Alonso Olea y Marfa Emilia Casas Baamonde, *Derecho del trabajo*, 12ª ed., Madrid, 1991, pp.59-60 // Manuel Santos Briz, "El contrato de ejecución de obra y su problemática jurídica" en *Revista de Derecho Privado*, 1972, pp. 280-281 // Puig Peña, *Compendio de derecho civil español*, t. IV, vol. II, 3ª ed., Madrid, 1976, p.140 // J. Santamaría, *Comentarios al Código Civil*, Madrid, 1958, p. 586 // Fernández Costales, *El contrato del arquitecto en la edificación*, Madrid, 1977, p. 125 // Antonio

De este modo, en el ámbito español nacen por creación no sólo doctrinal sino también jurisprudencial los actuales contratos de ejecución de obra y de servicios, como dos contratos independientes o autónomos caracterizados, el primero, por originar una obligación de resultado para el contratista; y el segundo, por vincular al prestador del servicio con una obligación de medios.²³⁹

Como quiera que se trate de dos contratos nuevos en relación con los tipificados en la codificación civil española, vale la pena confrontar sus características y diferencias:²⁴⁰

Conforme el Código Civil.- El arrendamiento de obras tiene por objeto una actividad dirigida a la creación de una cosa material o un nuevo objeto de derecho, a cambio de un precio. En tanto que el arrendamiento de servicios tiene por objeto la realización de una actividad que se agota con la mera prestación, también a cambio de una contraprestación;

Conforme la construcción doctrinal y jurisprudencial.- El novedoso contrato de ejecución de obra tiene por objeto la actividad dirigida a la obtención de un resultado jurídico -que no material- que puede, o no, concretarse en una cosa nueva, a cambio de un precio. En tanto que el novedoso contrato de servicios tiene por objeto la prestación de una actividad considerada en sí misma, a cambio de una contraprestación.

Sin embargo como se tiene anticipado, la distinción entre obligación de medios y obligación de resultado en la práctica no se presenta de manera clara, ya que toda obligación

Gullón Ballesteros, *Curso de derecho civil. Contratos en especial. Responsabilidad extracontractual*, Madrid, 1972, p. 252 // Carlos Lasarte Álvarez, *Principios de Derecho Civil, vol. III, Contratos*, 3ª ed., Madrid, 1995, pp. 285-286 // Demetrio García Iglesias, *El contrato de obra: concepto y contenido. Los riesgos y la responsabilidad según la doctrina del Tribunal Supremo*, La Ley, 1993-4, p. 1.119; entre otros.

²³⁹ Conforme hace notar Sole, la jurisprudencia del Tribunal Supremo español ha convertido el objeto de la obligación de hacer en la nota definitiva en orden a la distinción entre el contrato de ejecución de obra y el de servicios (J. Sole, 1997: 143). En este sentido se pronuncian numerosas sentencias en las que se cuestiona directa o indirectamente la naturaleza jurídica del contrato celebrado entre las partes, que configura el objeto de la *litis*; para ejemplificar lo aseverado citaremos las siguientes:

La Sentencia de 4 de febrero de 1950 (RAJ 191), en la que se lee: “*aunque de ordinario se presenta la relación contractual entre el Letrado y su cliente como un contrato de servicios, también aparece otras veces como contrato de obra, supuesto que se da cuando mediante remuneración se obliga aquel a prestar no propiamente su actividad profesional sino el resultado producido por la misma, cual ocurre, entre otros casos, en el aceptar el Letrado el encargo de emitir un dictamen*”; y

La Sentencia de 10 de junio de 1975 (RAJ 3265), siendo la más representativa en la jurisprudencia española en relación al asunto que analizamos. Sostiene dicha sentencia que “*de los diferentes criterios ideados por la doctrina para distinguir el arrendamiento de servicios del de obra, el que goza de mayor predicamento y el aceptado por este Tribunal... radica en el objeto inmediato de la obligación del arrendador, de manera que si éste se obliga a la prestación de servicios o de trabajo o de una actividad en sí misma, no del resultado que aquella prestación produce, el arrendamiento es de servicios y, en cambio, si se obliga a la prestación de un resultado, sin consideración al trabajo que lo crea, el arrendamiento es de obra, sin que para suponer la existencia de un contrato de esta última especie sea suficiente que la actividad se prometa en dirección a un resultado determinado, cosa no frecuente dado que toda actividad humana va dirigida a un fin o resultado*”.

²⁴⁰ Al respecto (J. Sole, 1997: 144).

requiere del deudor una conducta diligente; asimismo y simultáneamente, todo acreedor busca la satisfacción de su interés a través de la obtención de un resultado. De manera que todo acto supone medios para alcanzarlo, al mismo tiempo que todo medio busca un fin.

No obstante, nótese que no siempre la diligencia debida garantiza la satisfacción del objetivo buscado por las partes, de manera que no cabe su identificación. De esa manera es que algunas veces el resultado constituye el objeto directo de la obligación, en tanto que en otras ocasiones, lo debido sea únicamente la actuación diligente. En estos casos, habrá que procurar determinar si el resultado, y cuál de los resultados posibles, ha sido incorporado al contrato, o no.

Conforme define Trigo “...*resultado es el efecto y consecuencia de un hecho, operación o deliberación; desde éste punto de vista, toda actuación produce un resultado: cualquier transformación o cambio en las cosas, la propia persona o los asuntos de alguien es en sí mismo un resultado*”.²⁴¹ Explica la referida autora, que a su vez el esfuerzo como tal - objeto del contrato de servicios - ha de exteriorizarse para que resulte perceptible aunque no implique materialización; por lo que infiere la posibilidad de que meras prestaciones de actividad se describan en el contrato aludiendo al resultado que normalmente se sigue de ellas. En consecuencia, concluye señalando que esta falta de claridad en la construcción de la prestación debida (ejecución de una actividad que se materializa como un resultado) ensombrece la distinción entre obligaciones de medios y de resultado.²⁴²

Precisamente en la vaguedad de la clasificación radica su principal crítica. Por ello, resulta necesario efectuar una interpretación de la relación contractual desde una perspectiva jurídica - no sólo material o lingüística - reparando particular atención a los usos del tráfico y a la buena fe.²⁴³

²⁴¹ (B. Trigo, 1999: 187).

²⁴² (B. Trigo, 1999: 187-188).

²⁴³ (B. Trigo, 1999: 188).

Por otra parte, es necesario reparar en el hecho que la norma positiva no contiene criterios de distinción sino que en realidad éstos constituyen aportaciones doctrinales y jurisprudenciales. Buena parte de estos aportes son tomados del art. 5 de los Principios UNIDROIT sobre Contratos Comerciales Internacionales (PUNIDROIT).²⁴⁴ Dichos principios fijan fundamentalmente tres criterios para diferenciar el carácter de la prestación, los cuales pasamos a explicar de modo sintético.²⁴⁵

- a) Autonomía de la voluntad.- De conformidad con este principio, ante la duda de si estamos ante una obligación de medio o de resultado, en primer lugar se debe atender a la intención de las partes. El problema radica en los casos en que dicha voluntad no resulte clara, pues su interpretación genera dificultades, pero en todo caso deben considerarse, entre otros: i) los términos en que la prestación ha sido descrita; ii) la interpretación de ciertas estipulaciones que sirvan de guía.²⁴⁶
- b) Aleatoriedad.- Hace alusión al nivel de riesgo normalmente involucrado en la obtención del resultado esperado a modo de medida para calificar la obligación, ya sea como de medios o de resultado. En ese sentido, si el cumplimiento de la obligación involucra un riesgo muy alto se debe presumir que no es pretensión del deudor garantizar un resultado y, por contramano, el acreedor no espera dicha garantía. Se arriba a la conclusión contraria - en principio - en las ocasiones en que el resultado esperado puede ser obtenido sin ningún inconveniente en particular, por ello es frecuente que en la doctrina se haga alusión a la aleatoriedad del resultado, con una intencionalidad similar.

²⁴⁴ Desarrollados por el *Instituto Internacional para la Unificación del Derecho Privado*, más conocido por sus siglas UNIDROIT.

²⁴⁵ Una explicación completa de estos principios puede ser encontrada en (B. Trigo, 1999: 194-229).

²⁴⁶ Respecto a la existencia de supuestos tipo, Trigo hace notar que existe moderada tendencia a identificar las actividades liberales, con el contrato de servicios, en consideración del ejercicio de las profesiones liberales como un arte, en contraste con los oficios técnicos. Así por ejemplo, en la regulación en el Derecho italiano del *contratto d'opera y appalto*, la obligación del prestador de obra manual (*contratto d'opera*) es siempre, como la del *appaltatore*, una obligación de resultado; consista en la ejecución de una obra o en la prestación de un servicio; en cambio, la obligación del prestador de obra intelectual es de medios. El art. 2236 *Codice Civile* establece inclusive, que si la prestación implica la solución de problemas técnicos de especial dificultad, el prestador *d'opera* no responde de los daños, sino en el caso de dolo o culpa grave. Al respecto (B. Trigo, 1999: 191).

- c) Influjo de las habilidades.- Finalmente, los PUNIDROIT se refieren al influjo de las habilidades de la otra parte en la ejecución de la obligación, como un referente que contribuya a diferenciar cuando nos encontramos frente a una obligación de medios, y cuando ante una obligación de resultado. En esta línea, Trigo sostiene que puede defenderse la existencia de una presunción favorable al contrato de servicios, si el resultado no está en la mano de quien realiza el trabajo.²⁴⁷

Con todo, podemos concluir señalando que la delimitación entre obligaciones de medios y de resultado no se establece con límites rígidos ni absolutos.²⁴⁸

Condensando ideas podemos señalar acorde a lo que se ha venido estudiando, que el contrato de servicios tiene como objeto del contrato al servicio en sí mismo considerado, a los medios para satisfacer un interés, que en principio y al tenor del espíritu codificado, reviste una inmaterialidad, pero que conforme el avance de la doctrina y la jurisprudencia se ha ido admitiendo su materialización en un hacer de resultado concreto. No obstante las excepciones, lo frecuente es que el objeto de la obligación en este contrato constituya una mera actividad, que se instrumentaliza en prestaciones de hacer, que puede ir acompañada de obligaciones de no hacer, descartándose la obligación de dar como objeto de la prestación, y por consecuencia, devienen para el deudor obligaciones de medios.

De conformidad a las consideraciones previamente estudiadas, corresponde volver nuestra atención al contrato objeto de estudio y hacer las comparaciones pertinentes con el arrendamiento de servicios, a efectos de determinar si la certificación reconocida encuadra, o no, dentro de la categoría típica al tenor de la regulación codificada.

A dicho propósito señalemos que en la certificación reconocida, el PSC tiene como obligación habilitar un directorio de consulta sobre vigencia de certificados al cual tengan acceso los usuarios del certificado, a objeto de comprobar la validez de un determinado

²⁴⁷ (B. Trigo, 1999: 228).

²⁴⁸ (B. Trigo, 1999: 229).

certificado, obteniendo la clave pública asociada al mismo para validar la firma electrónica del Firmante/Suscriptor y de ese modo autenticar su identidad con certeza.

Asimismo, el PSC debe administrar el ciclo vital de los certificados, procediendo a la suspensión o revocación de los mismos, etc. Estas obligaciones consisten evidentemente en una actividad (un hacer) que debe desplegar el PSC. Actividad que exige además un especial grado de diligencia, no la diligencia media que se exige a un *pater familias* sino un nivel elevado de diligencia profesional. Con todo el PSC no puede asegurar pese al empleo de todos los medios técnicos a su alcance así como el despliegue de todos los esfuerzos de seguridad y diligencia debida, la no vulneración del sistema por parte de un tercero *hacker*, que infiltrándose en la red, suplante al Firmante/Suscriptor y efectúe transacciones fraudulentas en nombre y perjuicio de éste o de otras personas. De igual modo, el PSC nunca podrá - siguiendo el criterio de J.F. Ortega - asegurar la convicción psicológica del tercero Usuario del certificado reconocido que le lleve a confiar en sus certificados.²⁴⁹

El fin último buscado por el Firmante/Suscriptor al contratar con el PSC - su identificación cierta y segura en una red de comunicación abierta - no se puede lograr sin la previa emisión correcta y entrega de una copia del certificado reconocido al Firmante/Suscriptor. En ausencia de certificado reconocido, no existe documento electrónico de identificación a ser publicado por el PSC en un directorio de consulta por parte de terceros, por consecuencia, no hay posibilidad que éstos accedan a la clave pública asociada a un certificado que no se ha emitido, y por ende, es inexistente la posibilidad de llevar a cabo la validación de la clave privada del Firmante/Suscriptor, lo cual únicamente se consigue con la elaboración y entrega con carácter previo de un certificado reconocido al Firmante/Suscriptor. Y ello, únicamente es posible a través de la ejecución de una obra con carácter anterior.

Por los argumentos expuestos, descartamos la posibilidad de que el contrato de

²⁴⁹ (J.F. Ortega, 2004: 415).

certificación reconocida pueda enmarcarse como un contrato típico (o incluso atípico) de arrendamiento de servicios, puesto que este tipo contractual no satisface integralmente el objeto y la causa de la certificación reconocida.

Sostenemos esta afirmación debido a que el arrendamiento de servicios individualmente considerado, no satisface ninguno de los objetos del contrato de certificación reconocida. Y ello es evidente, toda vez que en ausencia de un certificado reconocido que debiera ser previamente emitido (una obra), el PSC se ve impedido de desplegar las actividades ulteriores necesarias para lograr la efectiva identificación del Firmante/Suscriptor frente a terceros en una red abierta de comunicaciones; en otras palabras, el hecho de que el PSC carezca del certificado a ser publicado en un directorio, conlleva la imposibilidad fáctica de brindar los servicios de consulta y validación-verificación del certificado correspondientes.

Por lo expuesto, el arrendamiento de servicios tampoco satisface la causa del contrato de certificación reconocida, toda vez que sin la emisión y entrega previa al Firmante/Suscriptor de una copia del certificado reconocido, y por ende sin certificado que publicar en un directorio a objeto de validarlo o verificarlo, ninguna identificación segura ni certeza puede generarse.

Por todos los aspectos analizados precedentemente, finalmente podemos concluir señalando que el denominado contrato de servicios no se regula, en el ordenamiento español, como un tipo contractual particular, motivo por el cual somos del criterio que la calificación que hagamos del contrato de certificación reconocida no puede ir referida a este supuesto, en el entendido que dicha calificación conlleva simplemente la determinación de la obligación del prestador como un hacer, pero sin ningún tipo de concreción. Además, esta calificación no conlleva la aplicación de un régimen jurídico pormenorizado.²⁵⁰

²⁵⁰ Así lo pone de manifiesto la autora Vaquero al mencionar que: “*El Código Civil es muy parco en la regulación de este contrato. Debemos tener en cuenta que casi todas sus disposiciones no son ya de aplicación. Por tanto, una vez hecha la calificación jurídica de un*

3.1.4.- La certificación reconocida como contrato que comprende la ejecución de una obra previa y la prestación de un servicio ulterior.-

En base a todo lo que se ha venido analizando hasta el momento, hemos arribado preliminarmente a las siguientes conclusiones:

- primero, que la certificación reconocida no encaja dentro del típico contrato de mandato, toda vez que éste último no satisface el objeto y la causa del primero;
- segundo, que el contrato típico de arrendamiento de obra, si bien satisface uno de los objetos del contrato de certificación reconocida (el certificado), no satisface integralmente el objeto y la causa de la certificación reconocida;
- tercero, que el contrato típico de arrendamiento de servicios - e incluso la modalidad atípica de éste - no satisface ninguno de los objetos del contrato de certificación reconocida (en ausencia de certificado, ningún servicio de autenticación puede ser prestado) y por consiguiente tampoco su causa.

Se ha visto igualmente que cuando el objeto de un contrato es una prestación simple y homogénea, basta calificar la obligación del prestador de servicios cómo de medios o de resultado, para que se aplique el régimen del contrato de servicios o el de obra, respectivamente. Sin embargo en el caso de la certificación reconocida, lo que ocurre es que la prestación se descompone en una pluralidad de actos que, individualmente considerados, dan lugar a obligaciones de medios y a obligaciones de resultado encadenadas, dirigidas a la realización del fin contractual.

Ahora bien, debemos tomar en cuenta que tal fragmentación podría llevar a la disgregación del régimen normativo aplicable al contrato. Frente a esta realidad, consideramos que a los fines de estudio del contrato de certificación reconocida, no resulta

contrato como arrendamiento de servicios no se podrán aplicar las normas reguladores de este contrato del Código Civil". María José Vaquero Pinto, *El arrendamiento de servicios. Propuesta de modelo general para la contratación de servicios*, Granada, Comares, 2005, p.20 // Por su parte Trigo indica que "el valor de estos artículos en su redacción actual es muy escaso y resulta evidente que no puede construirse el estudio del contrato de servicios sobre la base de su regulación codificada" (B. Trigo, 1999: 127).

tan importante establecer la naturaleza de una obligación aislada, como determinar la naturaleza global e integral del contrato, que es en definitiva lo verdaderamente relevante.

En consecuencia, debemos formularnos la interrogante de si nos encontramos ante un contrato único - de servicios o de obra - o ante una superposición o combinación de contratos. De inicio, no es posible dar una respuesta absoluta toda vez que ambas opciones resultan viables. No obstante, en una situación como la expuesta, “*seccionar*” el contenido de la relación obligatoria carecería de todo sentido y el régimen jurídico aplicable es único en atención a la configuración global de la prestación debida; por lo tanto, debemos atender a la exigibilidad o no del suceso definitivo, sin que la existencia de obligaciones parciales de resultado impida la calificación del contrato como de servicios integralmente concebido.

La obligación de resultado aquí no es consustancial o implícita a la obligación de medios; puede entenderse, entonces, que se dan dos contratos: de obra y luego de servicios.

La otra opción, en vista del objetivo final perseguido, es entender que existe un único contrato de servicios que comprende la obra previa y el servicio subsiguiente. La unidad de la relación demanda la consideración de un único contrato, pero evidentemente que resulta un tanto forzado limitarlo únicamente al contrato de servicios, cuando la prestación de resultado (el certificado) se presenta diferenciada y sometida a sus propias reglas, sin perjuicio de su instrumentalidad respecto a la obligación de medios.²⁵¹ Por consecuencia, entendemos que lo más apropiado inicialmente es concebir la certificación reconocida como un contrato atípico de servicios.²⁵²

²⁵¹ Al respecto, Trigo advierte que en la medida que surge en la doctrina y la jurisprudencia una cierta tendencia objetivadora de la responsabilidad, se corre el riesgo de la eventual refundición del contrato de servicios y del contrato de obra en un único tipo contractual, sobre la base de la generalización, por obra del legislador. No obstante, postula que pese al avance del contrato de obra en determinadas hipótesis y la existencia de situaciones intermedias debido a la aproximación entre obligaciones de medios y resultado, puede seguir hablándose de contrato de servicios, como una categoría contractual independiente, introduciendo, en su caso, los matices oportunos (B. Trigo, 1999: 276-277).

²⁵² Díez-Picazo al referirse a los contratos coligados expone que: “*Algunos autores, partiendo de la idea de que cada uno de los contratos yuxtapuestos conserva su propia fisonomía...entienden que existe una pluralidad de contratos, cada uno de los cuales jugaría separado y sometido a su propio régimen. Sin embargo, lo cierto es que el fenómeno jurídico constituye una auténtica unidad económica, puesto que obedece a una unidad de interés y de función que exige que el fenómeno sea considerado como una unidad jurídica y que, por consiguiente, se entienda que existe un solo contrato.*” (L.Díez-Picazo, 1996: 389).

La solución propuesta - que podríamos calificar de *ecléctica* - posibilita superar las insuficiencias de concebir este contrato limitado únicamente a la ejecución de una obra²⁵³ o a la prestación de un servicio,²⁵⁴ conforme se viene planteando uniformemente al presente en la doctrina, toda vez que desde nuestro punto de vista, permite dar una respuesta más satisfactoria en los casos de incumplimiento que afecta a una de las obligaciones y no a la otra, o de quebrantamiento de la relación obligacional con carácter previo a la realización de la segunda fase de la prestación, bifurcándose ambas obligaciones. En esos casos, entendemos que deberá aplicarse estrictamente el régimen del contrato de obra o el de servicios, según corresponda.

3.1.5.- La certificación reconocida como contrato de actividad.-

En base a las reflexiones elaboradas precedentemente, consideramos que más que ante un tipo contractual determinado, podemos hablar de una categoría general de contratos que podemos denominar como contratos de actividad. Los diversos tipos contractuales que componen dicha categoría tienen como objeto una obligación de hacer o de un no hacer y, en todos, el cliente recibe el beneficio de la actividad que constituye el núcleo de dicha obligación²⁵⁵.

Existen contratos de esta categoría que cuentan con regulación expresa, tal es el caso del contrato de arrendamiento de obra (art. 1.588 a 1.600 C.c.), el contrato de transporte de

²⁵³ Entre los autores que sostienen que el contrato de certificación de firma electrónica constituye un contrato de obra, se encuentra D. Rodríguez, quien considera que la introducción de la noción “servicios” en la identificación del sujeto, no es correcta a estos efectos “*pues parece como si el prestador fuese parte de un contrato de arrendamiento de servicios*”, cuando a su entender, ello no es así, porque comprende que la expedición de certificados es una obra; por consiguiente, sostiene que sería mejor haber definido a este sujeto con un concepto que pusiese de manifiesto -para evitar cualquier duda- esta obligación del resultado que asume. Considera que hubiese sido más apropiado hablar de dos tipos de sujetos: los prestadores de certificados, a secas; y prestadores de certificados y de servicios relacionados con la firma electrónica. Al respecto consultar: (M. Huerta y D. Rodríguez, 2001: 88-92).

²⁵⁴ Entre los autores que consideran que el contrato de certificación de firma electrónica constituye un auténtico contrato de servicios se encuentran: Juan Francisco Ortega Díaz, “Firma digital y tráfico económico. La importancia del contrato de certificación digital”, en M. Jesús Moro Almaraz, comp., *Autores, consumidores y comercio electrónico*, Madrid, Colex, 2004, 1ª ed. p. 414-416 // María Pérez Pereira, “Régimen jurídico del prestador de servicios de certificación”, en Javier Cremares y otros, comp., *Régimen jurídico de Internet*, Madrid, La Ley, 2002, 1ª ed., pp. 931-968 // Carlos Vattier Fuenzalida, “Responsabilidad contractual y extra contractual en el comercio electrónico”, en Javier Cremares y otros, comp., *Régimen jurídico de Internet*, Madrid, La Ley, 2002, 1ª ed., pp. 1177-1201.

²⁵⁵ Villanueva establece que la categoría de los contratos de prestación de servicios “*pertenecen a un género que podría denominarse contratos de prestación de actividad en beneficio de otro*”. Carmen Villanueva Lupión, *Los contratos de servicios*, Madrid, La Ley, 2009, p.41.

personas y cosas (art. 1.601 a 1.603 C.c.), el contrato de mandato (art. 1.709 a 1.739 C.c.) o el contrato de depósito (art.1.758 a 1.784 C.c.).

En otras situaciones, por el contrario, carecen de una regulación específica, conformando un grupo variopinto de contratos atípicos, mixtos o complejos, en los que el objeto consiste en una actividad en beneficio de otro,²⁵⁶ siendo la doctrina y los tribunales los que han ido estableciendo su régimen jurídico.²⁵⁷

Analizada la situación de que no es posible identificar el contrato de certificación reconocida con ninguno de los tipos regulados en la legislación positiva, debemos proceder a establecer si es factible adscribirlo en la categoría general de los contratos de actividad, con la advertencia que en caso afirmativo, la consecuencia resulta en la aplicación al mismo de los principios generales que inspiran la regulación de los tipos contractuales que la conforman.

En el contrato objeto de estudio, evidentemente el PSC se obliga a realizar una actividad en procura de satisfacer el interés primario del acreedor, este es, la identificación en - sentido amplio - del Firmante/Suscriptor, como requisito imprescindible para generar un entorno seguro y confiable.

Esta actividad se concretará en contratar personal debidamente cualificado, adquirir los recursos tecnológicos adecuados para montar una Infraestructura de Clave Pública (ICP), mantener los mismos en unas condiciones adecuadas para que puedan servir para el uso al que se destina, efectuando tareas de mantenimiento, y garantizar un servicio de consulta de certificados a través de su publicación en el sitio web del PSC a objeto que los Usuarios del certificado puedan verificar el estado del mismo (vigente, suspendido o extinguido). Todo

²⁵⁶ (C. Villanueva, *Los contratos...*2009: 41- 45).

²⁵⁷ Así, los tribunales han ido resolviendo cuestiones concretas sobre los diversos tipos de contratos de servicios que se presentan en la práctica, basándose fundamentalmente en la voluntad de los contratantes, los usos y las costumbres, las reglas generales sobre obligaciones y contratos y, en su caso, las reglas específicas de carácter profesional o corporativo.

ello constituye el servicio del que se beneficia el Firmante/Suscriptor a cambio del precio fijado.

Por otro lado, debemos señalar que la actividad del PSC se encuentra caracterizada esencialmente por los elementos que componen la misma. La obligación principal del contrato se concreta, por un lado, en la emisión y entrega de un certificado reconocido, es decir, de un bien inmaterial, junto con la obligación de proporcionar los servicios de directorio y verificación del certificado y, por otro, en el resultado que se pretende obtener, que es la identificación en - sentido amplio - del Firmante/Suscriptor, como requisito imprescindible para generar un entorno seguro y confiable.

Por ello se puede argumentar que esta obligación se define, fundamentalmente, por la emisión, entrega y publicación del certificado reconocido y el resultado que con éste se pretende, más que por la propia actividad a desarrollar por el PSC.

No obstante ello no nos puede llevar a descartar su calificación como contrato de actividad. Efectivamente, existen casos en los que un determinado contrato de servicio aparece definido por el resultado que se pretende por el cliente más que por el conjunto de obligaciones de hacer que el prestador debe llevar a cabo para obtenerlo.²⁵⁸

En ese sentido podemos concluir señalando que el contrato de certificación reconocida se encuentra dentro de la amplia categoría de contratos de actividad, en el entendido que el PSC asume una obligación general de realizar una actividad. Y ello es evidente, debido a que la lógica interna del régimen jurídico que inspira esta categoría coincide con la propia del contrato de certificación reconocida pues, en ambos, la disciplina se basa en la obligación de una de las partes de realizar un servicio a favor de la otra que obtendrá, a través de dicha actividad, la satisfacción de su interés contractual.

²⁵⁸ Así, Trigo refiere el ejemplo del contrato por el cual el abogado se obliga a representar a su cliente haciendo todo lo que esté en su mano para que éste logre el éxito de su pretensión. En este caso, no suelen contemplarse de forma expresa las distintas actividades que llevará a cabo el letrado (estudio del caso, escrito de demanda, presentación de la misma, preparación de su representación en el juicio correspondiente, etc.). Las partes, por el contrario, llegarán en la mayoría de los casos a un acuerdo en el que simplemente se establezca la obligación del abogado de defender los intereses de su cliente, a cambio de un precio que deberá satisfacer el mismo (B. Trigo, 1999: 276-277).

Finalmente diremos que la certificación reconocida, por sus características tan particulares y únicas así como su carácter *sui generis*, goza respecto de cualquier otra clase de contratos de actividad, de una causa y objeto propio, razón por la que se configura como un contrato eminentemente autónomo respecto de otros contratos en los que se presta una actividad en beneficio de otro.

3.1.6.- Inserción de la certificación reconocida en la genérica categoría del

“contrato de servicios”.-

Finalmente para concluir con nuestro análisis en esta parte, nos parece necesario señalar que la doctrina española más reciente, ha venido trabajando en los últimos años de la mano de autoras como María José Vaquero Pinto, J. Solé Resina y Carmen Villanueva Lupión, en la elaboración de la genérica categoría del denominado “*contrato de servicios*”.²⁵⁹

Conforme se analizó previamente, lo evidente es que el contrato de servicios conforme se encuentra normado en la generalidad de los códigos civiles contemporáneos que pertenecen a la familia jurídica *romano-germánica* de derechos, presenta en la actualidad una deficitaria y anacrónica regulación positiva; con el agravante de que en muchos casos la regulación de la prestación de servicios ha salido del ordenamiento civil habiendo sido asimilada por otras disposiciones normativas, al punto de dejar prácticamente vacante y ausente el contenido del mismo en el Código Civil.

En consecuencia la realidad y el tráfico demandan una readecuación y enriquecimiento de este tipo contractual prácticamente huérfano de regulación, sobre todo considerando que vivimos en una economía terciaria, donde la prestación de servicios cobra mucha más importancia que la producción de bienes tangibles y fundamentalmente, tomando en cuenta el surgimiento de la denominada Sociedad de la Información, en la cual la

²⁵⁹ Para un estudio de la construcción doctrinal del genérico “contrato de servicios”, revisar las siguientes investigaciones: María José Vaquero Pinto, *El arrendamiento de servicios. Propuesta de modelo general para la contratación de servicios*, Granada, Comares, 2005 // J. Solé Resina, *Los contratos de servicios y de ejecución de obra. Delimitación jurisprudencial y conceptual de su objeto*, Madrid, 1997 // J. Solé Resina, *Arrendamiento de obras o servicios (Perfil evolutivo y jurisprudencial)*, Valencia, 1997 // Carmen Villanueva Lupión, *El servicio como objeto de tráfico jurídico*, Madrid, La Ley, 2009 // Carmen Villanueva Lupión, *Los contratos de servicios*, Madrid, La Ley, 2009.

prestación de servicios ocupa un espacio protagónico y central. En esta necesidad se hallan prácticamente todas las codificaciones civiles de los países Iberoamericanos, entre ellos, el español.

Varias codificaciones pertenecientes a la familia jurídica *romano-germánica* y prácticamente la mayor parte de la jurisprudencia y la doctrina, han superado de forma definitiva la inclusión del contrato de servicios dentro del arrendamiento. Visto de ese punto de vista, el contrato de arrendamiento ha quedado reservado exclusivamente para el caso de locación de bienes muebles e inmuebles, reconociéndose la independencia de éste, respecto del contrato de obra y del contrato de servicios. Asimismo, la separación del contrato de mandato respecto del contrato de servicios parece ser una realidad que ya nadie discute.

Resulta oportuno en consecuencia, establecer en primer lugar la naturaleza jurídica de los servicios para luego ofrecer un concepto jurídico del mismo. Con relación al primer aspecto, se ha fijado la naturaleza jurídica del servicio como “*actos humanos objeto de los derechos de crédito u obligación que consisten en un hacer cuyo ejercicio agota la prestación principal debida, generados mediante contratos bilaterales o unilaterales, que revisten actividades cualificadas o no, de carácter material, incorporal o intelectual, o combinación de ellas*”.²⁶⁰

Por otra parte, se conceptualiza jurídicamente al servicio como “*una prestación de hacer, generalmente de origen contractual, desplegada como actividad conforme a la diligencia debida por el deudor o prestador y en atención a las utilidades que debe procurar para satisfacer el interés del acreedor o destinatario*”.²⁶¹

Efectuadas estas precisiones, corresponde identificar en qué consiste exactamente la construcción resiente de la genérica categoría del “*contrato de servicios*”; para ello

²⁶⁰ (C. Villanueva, *El servicio...*,2009:168).

²⁶¹ (C. Villanueva, *El servicio...*,2009:169).

seguiremos la exposición de Villanueva Lupión, por considerar que constituye el estudio más depurado y reciente sobre la cuestión.²⁶²

La referida autora incluye a todos los contratos de actividad en beneficio de otro que presentan una regulación tipificada propia, en la significación amplia de “*los contratos de prestación de servicios*” como categoría de contratos de actividad. De manera que el tipo contractual concreto para las prestaciones de servicios sin regulación particular viene constituido por el “*contrato de servicios*”.

La relación entre el *contrato de servicios* y los distintos contratos tipificados o atípicos, innominados, mixtos o complejos de *prestación de servicios*, en criterio de la autora, es la de género a especie. No obstante - señala - la caracterización del *contrato de servicios* como figura huérfana de regulación o su atipicidad legal, plantea la posibilidad de integrar el género mediante referencia a alguno de los contratos de prestación de servicios tipificados.

Si bien - en criterio de Villanueva - no es válida una remisión genérica a ninguno de ellos, resulta preferible la integración del contrato a través de la teoría general de las obligaciones y de los contratos, teniendo en cuenta la voluntad de las partes y los usos del tráfico de la concreta actividad desarrollada y, en su caso, la analogía en determinados aspectos con los contratos tipificados.

3.1.6.1.- Los servicios según los “*Principios de Derecho Europeo - Contratos de Servicios*” en la elaboración del Marco Común de Referencia.-

Resulta necesario complementar nuestro análisis en esta parte, señalando que en el ámbito de la Unión Europea se viene trabajando desde varios años atrás precisamente en la integración del Derecho Europeo, desde los proyectos más ambiciosos, como el desarrollo de un Código Civil europeo, pretensión superada en la actualidad por las tareas a favor de establecer principios comunes de la contratación en el ámbito europeo y/o promover el desarrollo de un Código europeo de contratos.

²⁶² (C.Villanueva, *Los contratos*.,2009:44).

De ese modo, a partir de los trabajos de la Comisión Lando²⁶³ se avanza con la elaboración de los “Principios del Derecho Europeo de los Contratos” (más conocido simplemente por sus siglas en inglés como PELC, *Principles of European Contract Law*) y los “Principios de Derecho Europeo. Contratos de Servicios” (más conocido simplemente por sus siglas en inglés como PEL-SC, *Principles of European Law. Service Contracts*), que constituirán un Marco Común de Referencia (abreviadamente MCR, o en inglés CFR: *Common Frame of Reference*).²⁶⁴

En el borrador del Marco Común de Referencia, el Libro IV se encuentra dedicado a distintos contratos específicos y contempla en su apartado C el “*contrato de servicios*”. El texto presenta una parte general aplicable a todos los contratos en los que se presta un servicio y una parte especial en las que se contienen disposiciones específicas para cada una de las seis modalidades que se contemplan: construcción, actividades de mantenimiento y reparación de bienes, contrato de depósito y custodia, diseño y elaboración de proyectos, información y asesoramiento profesional, además los tratamientos médicos. Se excluyen expresamente el contrato de transporte, el de seguro, el de garantía y los contratos financieros, así como el contrato de trabajo.

Las disposiciones generales son de aplicación a los contratos en los que una parte es un “profesional” o “prestador del servicio” que efectúa un servicio para la otra parte, el “cliente”, a cambio de una remuneración. El servicio se desarrolla en el marco de una actividad profesional o empresarial, lo que requiere del prestador unos conocimientos y una organización de medios materiales y humanos. La contraparte es el cliente, que no se delimita como consumidor o usuario.²⁶⁵

²⁶³ Por su Presidente el Prof. Ole Lando, que viene trabajando desde 1980 en la elaboración de los Principios del Derecho Europeo de los Contratos.

²⁶⁴ Al respecto consultar: *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR)*, preparado por el “Study Group on a European Civil Code”, y el “Research Group on EC Private Law – Acquis Group, Munich, 2009.

²⁶⁵ Al respecto (C.Villanueva, *El servicio...*,2009:133-135).

El servicio objeto de este contrato de servicios es una categoría amplia, tanto como obligación de hacer o actividad sin producción, como también aquella que consiste en la creación de una cosa nueva, material o inmaterial.

El objeto de este genérico contrato de servicios contempla actividades profesionales de las que el cliente puede esperar la consecución de un resultado previsto o indicado por él mismo al momento de celebrar el contrato, siempre que sea un “resultado razonable” y el prestador no haya indicado que no se pueda alcanzar. Por consecuencia, el servicio en este marco general es una obligación de hacer que consiste en una actividad profesional desarrollada conforme a la diligencia debida o estándar de cuidado exigible, que podrá dar lugar o no a un concreto resultado.

Como es posible observar, dentro de los amplios contornos del genérico *contrato de servicios* encuentran acomodo muy diversas modalidades contractuales y, entre ellas, el contrato de certificación reconocida de firma electrónica objeto de nuestro estudio. De este modo se incardina en una categoría - si bien de carácter doctrinal más no tipificada legalmente - que facilita su tratamiento jurídico.

3.2.- El contrato de certificación reconocida como contrato atípico.-

En el entendido que ha quedado descartada la asimilación del contrato de certificación reconocida de firma electrónica dentro de cualquiera de los tipos legales con los que cabría alguna semejanza, nos encontramos en condiciones de proclamar su atipicidad, no obstante se encuadre dentro de los contratos de actividad o se adscriba más precisamente al genérico *contrato de servicios*, pues estas categorías constituyen una calificación eminentemente doctrinal más no legal.²⁶⁶

²⁶⁶ En este sentido, López establece expresamente que “la calificación del contrato, siendo como es la inserción de lo querido por los contratantes dentro de los tipos o esquemas negociales predispuestos por el ordenamiento, supone un juicio de adecuación del negocio concreto (o más rectamente dicho, a mi entender, del intento o propósito contractual concreto) a categorías establecidas a priori por las normas y ello, solo cabe hacerlo desde la óptica de las normas (lo que es formalmente idéntico para la calificación de atipicidad, en tanto ella supone no-tipicidad, y, en consecuencia, la exclusión de la aplicación de unas normas: o dicho más exactamente, porque no se encuentran normas directamente aplicables, el contrato se califica de atípico).” Ángel M. López y López, “*Comentarios al Código Civil y Compilaciones forales. Tomo XVII. Volumen 2º. Artículos 1281 a 1314*”, Madrid, Editoriales de Derecho Reunidas, 1981. p.6.

Es evidente que el contrato objeto de estudio no se encuentra reconocido ni regulado en el ordenamiento legislativo y, por consiguiente, conforme tenemos señalado se trata de un contrato atípico. Al respecto, es frecuente encontrar que la doctrina a momento de abordar la temática de la tipicidad de los contratos confunda los conceptos de nominación y tipicidad.

En ese sentido, varios autores recomiendan dejar de lado la vieja terminología de contrato nominado o innominado, para referirse únicamente a contrato típico o atípico;²⁶⁷ como hace notar Vega “...el “*nomen*” no basta por sí solo para establecer la tipicidad de un contrato...”.²⁶⁸ En el contrato que nos ocupa, podemos comprobar que la institución en estudio se nomina con bastante unanimidad: “Certificación reconocida”, “Certificación de firma electrónica reconocida”, o “Certificación digital”.

Por otra parte, la tipicidad se subdivide en tipicidad social y tipicidad legal. Partiendo de dicha división podemos señalar que la certificación reconocida cuenta con tipicidad social, toda vez que el contrato está conformado por un *tipo*, en la medida que se lo representa por medio de una serie de características distintivas y estructuradas del acto; se encuentra conformado por la práctica jurídica y es reconocido por sus destinatarios directos (los Firmante/Suscriptores).

Asimismo goza de una *causa* lícita, en el entendido que la función práctico social o socioeconómica que se le atribuye es digna de contar con la debida tutela legal. En base al análisis efectuado, podemos concluir señalando que la “tipicidad social” de la certificación reconocida se conforma en base al tipo referido a la estructura del contrato y su causa como interés social digno de tutela.

La problemática surge a momento de indagar respecto de su tipicidad legal. Sobre el particular debemos referir que la certificación reconocida es un contrato que - estableciéndose como una figura contractual de valor sustantivo - no está conceptualizado

²⁶⁷ (J.B. Jordano, 1953: 61). A su turno De Castro señala que “la vieja distinción romanista entre contratos nominados e innominados va siendo modernamente desplazada por la de negocios típicos y negocios atípicos.” (F. De Castro, 1967:202).

²⁶⁸ (J. Vega, 2002: 67).

como tampoco normado en la ley civil ni en la mercantil; meramente se encuentra esbozado fundamentalmente en la LFE (entre otras normas jurídicas), donde se establece el régimen general para la prestación de servicios de certificación de firma electrónica, y el régimen particular, cuando se trata de certificados reconocidos (arts. 11,12,13,14 y 20 LFE).

La duda que nace estriba en el hecho que, si al no poseer regulación sustantiva específica, pero al mismo tiempo encontrarse aludido en normativa legal que estructura un régimen jurídico aplicable a ciertos aspectos del mismo, el contrato de certificación reconocida ¿debe clasificarse como típico o atípico?. A objeto de dar respuesta a la interrogante planteada, resultará muy útil efectuar un análisis de los conceptos que la doctrina ha construido respecto de la tipicidad-atipicidad de las convenciones y contratos.

Se dice que un contrato es *típico* cuando el mismo posee una disciplina normativa contemplada expresa y directamente por el Ordenamiento jurídico. Restringiendo un poco más este concepto, se entiende por contrato típico aquel que la mención del contrato se hace por ley en tal lugar que se pueda inducir por vía de remisión la disciplina jurídica aplicable.²⁶⁹

Los argumentos expuestos nos llevan a pensar - en principio - que la certificación reconocida se configura como un verdadero contrato atípico, debido a que únicamente posee referencias legales y carece de regulación en cuanto al aspecto jurídico-privado. Ello sin perjuicio no obstante que, en su caso, puedan ser de aplicación preceptos de otro tipo de contratos.

No obstante, resulta conveniente examinar con mayor detenimiento la concepción que la doctrina posee respecto de la atipicidad de los contratos, a objeto de contar con mayores elementos de juicio a momento de adscribir la certificación reconocida a una de las

²⁶⁹ Jordano define el contrato atípico como aquel que, aun mencionado por la Ley, está desprovisto de una nominación específica, a menos que la mención del contrato se haga por la Ley en tal lugar que se pueda inducir por vía de remisión la disciplina jurídica aplicable (J.B. Jordano, 1953: 68). Por lo que en criterio de Vega, cuando la Ley no sólo menciona el contrato, sino que, además, establece un régimen jurídico aplicable, aunque sea por aplicación de normas de otros contratos, podemos inferir que estamos en presencia de un contrato típico (J. Vega, 2002: 68).

variedades en estudio.²⁷⁰ Como sabemos el contrato se configura como atípico cuando a pesar de tener un nombre específico claramente fijado, es decir, que se lo individualiza en el tráfico (ya sea en la doctrina, la jurisprudencia, como también en algunas leyes) no cuenta sin embargo con una disciplina normativa propia, la cual resulta inexistente en los Códigos y en las leyes especiales.²⁷¹

De conformidad con el art. 1.255 C.c. la autonomía de la voluntad y la libertad de pactos hacen posible la celebración de toda clase de negocios jurídicos, con la única limitante de que se respeten las normas imperativas, la moral y el orden público. Debido a ello, existen contratos que poseen características que devienen de pactos propios con modalidad uniforme para cada tipo de operación, que los distinguen de otra clase de convenciones subsistentes en el Ordenamiento legal con los que presentan cierta conexión y que emergen en calidad de contratos “*sui generis*” sustantivos.²⁷²

Por lo tanto, diremos que cuando las normas legales no han contemplado la regulación de un nuevo instituto jurídico (ya sea debido a que las propias normas legales están en condiciones de llenar el vacío normativo, ya sea porque las personas involucradas en el negocio aún no han demandado la intervención del legislador), irrumpe el fenómeno de la atipicidad.²⁷³ Debido a que la ausencia normativa puede ser absoluta o relativa, es posible agrupar estos contratos del modo siguiente:²⁷⁴

a) Atípicos puros.- Son aquellos contratos desprovistos de todo régimen legal y no

²⁷⁰ Señala Puig Brutau que la diferencia entre contrato típico y atípico no deja de ser relativa en el siguiente sentido: No existe un contrato cuya tipicidad signifique tanta riqueza de previsiones normativas que de su contenido no pueda brotar ningún problema no previsto; a la inversa, tampoco es fácil señalar contratos que sean tan completamente atípicos que no permitan recurrir a las previsiones normativas ya establecidas con referencia a otros contratos, por lo que -continúa- se hace necesario diferenciar entre contrato propiamente atípico que no encaja en ninguna de las figuras con específica regulación legal, y el contrato atípico en el sentido de tener un contenido mixto o complejo, por presentarse con esta combinación de elementos diferentes (J. Puig, 1978: 453).

²⁷¹ J.L. Lacruz Berdejo, *Elementos de Derecho Civil*, vol. II, Barcelona, 2ª ed., 1987, p. 247.

²⁷² J. Garrigues Díaz-Cañabate, *Contratos bancarios*, Madrid, 2ª ed., 1975, p. 39.

²⁷³ Conforme explican Díez-Picazo y Gullón, tanto en el ámbito del Derecho civil pero sobretudo el mercantil, ha ocurrido que la mayor parte de sus instituciones han tenido su génesis en la práctica mercantil, en tanto que su regulación jurídica ha ocurrido “*a posteriori*”. Hoy en día el cometido de creación de nuevas formas contractuales no representa mayor dificultad, toda vez que se emplean los tipos legales existentes, añadiéndoles prestaciones o pactos novedosos que los transforman para responder a propósitos disímiles (total o parcialmente) de los contemplados por el legislador, o combinan dos o más tipos de los conocidos con idéntica finalidad. Luis Díez-Picazo y Antonio Gullón, *Sistema de Derecho Civil*, vol. II, Madrid, Tecnos, 7ª ed., 1995, p. 37.

²⁷⁴ (J. Vega, 2002: 69).

concuerdan - en ninguno de sus elementos - con los contratos regulados;²⁷⁵

b) Unidos, múltiples o mixtos.- Son aquellos contratos que armonizan distintos tipos contractuales o varias prestaciones singulares reguladas en tipos contractuales diversos;²⁷⁶ y

c) Atípicos “sui generis”.- Contratos que poseyendo causa única y mencionados por la Ley, se hallan desprovistos de un ordenamiento sustantivo propio, salvo alguna alusión legal que relativiza su atipicidad, mudándolos en atípicos “sui generis”.

Para el caso en estudio, resulta evidente que no puede catalogarse como contrato atípico puro a la certificación reconocida, toda vez que existen referencias legales que explicitan algún efecto de su régimen jurídico; así como tampoco es posible comprender que constituya un contrato unido, conexo o múltiple, dado que no se estructura en base a la yuxtaposición o unión de varios contratos típicos diversos entre sí, en los que cada cual preserva su particularidad²⁷⁷ - aunque enlazados por ciertos factores - sino que se configura como un contrato unitario, si bien compuesto por ingredientes simultáneamente típicos y atípicos, pero cuya característica denota una causa única.²⁷⁸

Por lo expuesto debemos entonces establecer si la certificación reconocida se configura como un contrato mixto, dado que - a tenor de su normatividad por remisión - está conformado por factores típicos y atípicos. Para ello debemos tomar en cuenta que la doctrina a momento de estudiar el contrato mixto “*lato sensu*”, efectúa las siguientes sub-categorizaciones:²⁷⁹

²⁷⁵ Sobre la tipicidad y atipicidad de los contratos consultar: M. Albaladejo, *Compendio de Derecho Civil*, Barcelona, 3ª ed., 1976, pp. 212 y ss.; ídem: *Derecho Civil*, Barcelona, 7ª ed., 1982, pp. 67 y ss. // A. De Cossío, *Instituciones de Derecho Civil*, Madrid, 1977, pp. 244 y ss. // (J.L. Lacruz, 1987: 252 y ss.).

²⁷⁶ Sobre contratos llamados unidos, múltiples o mixtos, consultar: D. Espín Canovas, *Manual de Derecho Civil Español*, Madrid, Revista de Derecho Privado, 5ª ed., 1978, pp. 363-364 // (J.L. Lacruz, 1987: 252 y ss.) // (M. Albaladejo, 1976: 212 y ss.) // (J.Puig, 1978: 448 - 459).

²⁷⁷ (J.L. Lacruz, 1987: 252).

²⁷⁸ Sobre contratos unidos véase (M. Albaladejo, 1976: 216).

²⁷⁹ (J. Vega, 2002: 70).

a) Contratos combinados o gemelos.- Constituyen una combinación de diferentes tipos contractuales con obligaciones de las partes obtenidas de uno o de otros;

b) Contratos de doble tipo o híbridos.- Cuando se acomodan en dos o más figuras contractuales; y

c) Contratos mixtos “sensu stricto”.- Cuando alguno de los factores fundamentales del contrato captura las particularidades de otro tipo contractual.

Aparentemente y “*prima facie*”, la certificación reconocida podría acomodarse dentro de la categorización de contrato mixto “*sensu stricto*”, en tanto aceptemos que no existe una pluralidad de contratos ligados entre sí sino un contrato unitario con parte de sus efectos normados. No obstante, el contrato de certificación reconocida - integralmente concebido - se enmarca solamente dentro de un tipo único, constituyendo precisamente este aspecto su distinción con los contratos mixtos, dado que, conforme sostiene algún sector doctrinal, aun en la esfera de los contratos típicos algunos se encuentran constituidos por componentes de otros contratos. Con todo cáigase en cuenta que éste no es el caso de los contratos mixtos.²⁸⁰

Los razonamientos que hasta acá venimos esgrimiendo, nos llevan a discernir que las variedades analizadas resultan siendo inválidas a momento de circunscribir el contrato de certificación reconocida. Ello nos lleva a continuar nuestra exploración a partir de la clasificación esbozada por otros segmentos de la doctrina respecto de la tipicidad parcial o “*sui generis*” de algunos contratos, por la cual se diferencia entre:

- a) Uniones de contratos;²⁸¹
- b) Contratos mixtos “*lato sensu*”;²⁸² y

²⁸⁰ Garriguez, entiende como contratos mixtos aquellos que aparecen en la compleja vida mercantil moderna como conglomerados, no designados legalmente con ningún nombre, de diversos contratos reconocidos por la ley. Hay contrato mixto -señala- cuando concurren en un contrato único diversas prestaciones características de otros contratos típicos. J. Garriguez, *Curso de Derecho Mercantil (revisión de Sánchez Calero)*, Madrid, 8ª ed., 1983, p. 34.

²⁸¹ Esta categoría estaría conformada por los contratos múltiples, que admiten tres modalidades: a) unión meramente externa de varios contratos, que mantienen su independencia; b) conexión con dependencia recíproca o unilateral que suponen distintos contratos queridos como uno solo, y c) unión alternativa, en la que la ligazón de contratos supone que el cumplimiento de una condición supondrá concluido uno u otro.

c) Contratos típicos con prestaciones o regulación subordinadas de especie distinta.²⁸³

Debido a las explicaciones previamente anotadas, debemos descartar que la certificación reconocida se identifique con las uniones de contratos, así como tampoco se ubica dentro del género de contrato mixto “*lato sensu*”.²⁸⁴ Mucho menos encuadra dentro de la clasificación de contrato típico con prestaciones o regulación subordinadas de especie distinta, ya que constituye un contrato único, cuyo contenido principal - integralmente concebido - se enmarca solamente dentro de un tipo único, aunque presente prestaciones supeditadas al fin principal que se modulan por otra u otras categorías contractuales.

A modo de conclusión, razonamos que si por contrato atípico puro comprendemos aquel que, pese a no contar con regulación legal propia de orden material, posee una denominación jurídica plenamente moldeada en el tráfico, debemos inferir que el contrato de certificación reconocida no constituye un contrato atípico puro. Resulta evidente que su génesis en el tráfico económico se ha debido a la práctica de los agentes económicos, lo que le ha conferido su tipicidad social. Con carácter posterior, la certificación reconocida se ha aludido en ciertas disposiciones legales. En todo caso, su alusión no perjudica a la aplicación de un régimen mercantil o civil.

Lo que sucede, es que existen determinadas figuras jurídicas no tipificadas que presentan peculiaridades y variedades como consecuencia de pactos originales de tenor uniforme para cada clase de operación, que les distinguen de otros contratos contemplados en el régimen jurídico con los que presentan un grado de vinculación²⁸⁵, y que inclusive se hallan insinuados adyacentemente por disposiciones legales, pero que se constituyen no obstante como contratos atípicos *sui generis*. Este es, a nuestro entender, el caso de la

²⁸² Que darían lugar a los denominados contratos combinados o gemelos, contratos mixtos “*sensu stricto*” y contratos híbridos o de doble tipo, los cuales ya hemos examinado anteriormente.

²⁸³ L. Ennécerus, *Tratado de Derecho Civil*, vol. II, Barcelona, 2ª ed., 1959, p. 6.

²⁸⁴ La doctrina también los denomina conexos o unidos. Véase (J.L. Lacruz, 1987: 252).

²⁸⁵ (J. Garriguez, 1975: 39).

certificación reconocida.

IV. Marco jurídico.-

4.1.- Legislación aplicable.-

De conformidad con el art. 1.255 C.c. *“Los contratos pueden establecer los pactos, cláusulas y condiciones que tengan por conveniente, siempre que no sean contrarios a la leyes, a la moral ni al orden público”*. En consecuencia, en base al principio de libertad contractual consagrado en el artículo enunciado el contrato se encuentra regido, en primer lugar, por lo previsto por las partes al contratar, siempre que dicha reglamentación sea respetuosa de la ley, la moral y el orden público.²⁸⁶

En todo caso resulta necesario establecer, por un lado, las normas imperativas a las que habrá de someterse la certificación reconocida y, por otro, las normas dispositivas que en caso de ausencia de regulación por las partes, serán aplicables al contrato.

Con relación al primer aspecto, las normas imperativas aplicables al contrato objeto de estudio se encuentran fundamentalmente contenidas dentro del marco de la siguiente normativa española y comunitaria europea:

4.1.1.- Normativa española.-

En primer lugar resultan siendo aplicables las normas contenidas en Código Civil, aprobado por R.D. del 24 de julio de 1.889, particularmente las contenidas en el Libro Cuarto *“De las obligaciones y contratos”*, conjuntamente con las disposiciones del Código de Comercio de 1885, especialmente las contenidas en el Libro Primero *“De los comerciantes y del comercio en general”*.

²⁸⁶ *“La libertad contractual que el artículo implícitamente proclama es la manifestación más acusada del principio de autonomía de la voluntad, verdadera razón de ser del negocio jurídico. La voluntad libre y manifestada de las personas (concertadas) se erige en regla fundamental que determina el contenido de los contratos...el Derecho de los contratos está transido por el principio de autonomía de la voluntad aun con las limitaciones que el principio establece”*. José Almagro Nosete, *“Comentarios al art. 1255 C.c.”*, en Ignacio Sierra Gil de la Cuesta, comp., *Comentario del Código Civil*, T. 6, Barcelona, Bosch, 2006, p. 566.

Asimismo se deben observar las disposiciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico;²⁸⁷ Ley 59/2003, de 19 de diciembre, de firma electrónica; Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación; 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; Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal; Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio.

Por otra parte, el contrato en estudio se encuentra sujeto a las normas que devienen del Real Decreto 1165/2005, de 30 de septiembre, por el que se regula el distintivo público de confianza en los servicios de la sociedad de la información y de comercio electrónico, así como los requisitos y el procedimiento de concesión (BOE nº 241, de 8 de octubre de 2005); y las normas que emanan de la Orden Ministerial, de 21 de febrero de 2000, por el que se aprueba el reglamento de acreditación de los PSC.

4.1.2.- Normativa comunitaria europea.-

En el ámbito comunitario, el contrato de certificación reconocida se encuentra sujeto en primer lugar, a la observancia de las normas contenidas en 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, conjuntamente con las disposiciones emergentes de la 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.

²⁸⁷ Un estudio bastante completo de la Ley 34/2002 (LSSI) es abordado por Javier Plaza Penadés, “Los principales aspectos de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003; pp. 29-74 // Igualmente consultar Favio Farinella, “España y una completa regulación para Internet”, en *REDI: Revista Electrónica de Derecho Informático*, No. 47, España, Alfa-Redi, junio/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1494> / Los aspectos positivos, negativos y neutros de la LSSI, son deliberados por Alfonso Villahermosa Iglesias, “Luces y sombras de la LSSICE: la regulación de Internet”, en *REDI: Revista Electrónica de Derecho Informático*, No. 52, España, Alfa-Redi, noviembre/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1413>

Asimismo, se deben observar las normas contenidas en la Directiva 98/34/CE del Parlamento Europeo y del Consejo de 22 de junio de 1998, modificada por la Directiva 98/48/CE del Parlamento Europeo y del Consejo de 20 de julio de 1998, por la que se establece un procedimiento de información en materia de las normas y reglamentaciones técnicas.

Finalmente resultan particularmente importantes, la Directiva 2006/123/CE del Parlamento Europeo y del Consejo de 12 de diciembre de 2006, relativa a los servicios en el mercado interior y la Directiva 93/13/CEE del Consejo de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores.

La normativa española y comunitaria previamente enunciada, constituye en consecuencia el marco jurídico aplicable al contrato de certificación reconocida, con la advertencia que en ningún caso, podrá ser desplazado por la regulación establecida por el PSC en las condiciones generales reguladoras del contrato. Su concreta aplicación será estudiada en las distintas partes subsiguientes de la presente investigación.

4.2.- Integración del contrato.-

Es necesario considerar que de conformidad con lo dispuesto en el art. 1.258 C.c., el contenido del contrato se extiende más allá de lo expresamente pactado por las partes contratantes, a *“todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley”*.

Conforme sostiene Almagro, “esta integración se superpone a la voluntad de las partes, de manera que, si del contrato resultan lagunas en la regulación, ya escapa a la voluntad de aquellas el modo de suplirlas, pues es la naturaleza del contrato la que sirve de referencia para establecer las consecuencias, desde el triple aspecto que recoge la norma. La naturaleza del contrato objetiviza los pactos puesto que este término ha de relacionarse con la

causa del contrato (objeto de consideración en su lugar), que, por encima de la integración subjetiva de los contratantes establece, con dimensión objetiva, el fin contractual”.²⁸⁸

La primera fuente de reglamentación contractual establecida en el art. 1.258 C.c. es la buena fe que, que conforme explica Díez-Picazo constituye un estándar jurídico, como un modelo de conducta social o la conducta que la conciencia social exige como necesaria en virtud de un imperativo ético dado. De modo que la buena fe es una fuente de creación de especiales deberes de conducta exigibles entre las partes contratantes, de acuerdo con el tipo de contrato y con la finalidad perseguida a través de él por las propias partes.²⁸⁹

En segundo lugar, los usos del tráfico constituyen el modo normal de proceder en el mundo de los negocios, se trata de la práctica habitual en los contratos de un determinado tipo procedente de las partes que otorgan tales contratos.²⁹⁰ El art. 1.258 C.c. ordena que los contratos obliguen a las consecuencias que sean conformes al uso y el art. 1.287 C.c., además de utilizar el uso como criterio interpretativo de las ambigüedades de los contratos, dice que suplirá en éstos la omisión de cláusulas que de ordinario suelen establecerse. Se trata pues, de un criterio de integración que se produce por remisión de la ley, el uso integra el contrato de un modo objetivo y con independencia de la voluntad de los otorgantes del contrato.²⁹¹ Los usos serán directamente aplicables salvo que las partes lo hayan excluido expresamente.

Finalmente, conforme explica Almagro, la función supletoria e integradora de las normas civiles resulta plenamente acorde con la naturaleza del Derecho Privado, de modo que la regulación general y la particular de los contratos, en cuanto no tengan el carácter de normas necesarias o de prohibición - que entonces actúan como límites infranqueables de la

²⁸⁸ José Almagro Nosete, “Comentarios al art. 1258 C.c.”, en Ignacio Sierra Gil de la Cuesta, comp., *Comentario del Código Civil*, T.6, Barcelona, Bosch, 2006, p. 590.

²⁸⁹ (L. Díez-Picazo, 1996: 362).

²⁹⁰ (L. Díez-Picazo, 1996: 360).

²⁹¹ (L. Díez-Picazo, 1996: 360).

voluntad de las partes - deben aplicarse a los contratos incompletos o insuficientes, de acuerdo con la tarea integradora que venimos estudiando.²⁹²

La ley a la que se refiere el art. 1.258 C.c. se trata tanto de la norma imperativa, que actúa limitando el contenido contractual, como de norma dispositiva. Como quiera que de modo preliminar ya tenemos señalado cuáles son las normas imperativas que serán aplicables al contrato de certificación reconocida, resta por establecer las normas dispositivas que integran el contrato.

Éstas serán, fundamentalmente, las normas y principios generales que modulan la regulación de los denominados contratos de actividad, y más concretamente, las que regulan el genérico *contrato de servicios*, toda vez que como ya tuvimos la oportunidad de estudiar, el contrato de certificación reconocida se integra dentro de las señaladas categorías doctrinales. También por supuesto, las normas dispositivas generales sobre obligaciones y contratos establecidas en el Libro I, Título IV del Código de Comercio y en el Libro IV del Código Civil.

4.2.1. La autorregulación del PSC en el contrato de certificación reconocida.-

La prestación de servicios de certificación de firma electrónica normalmente se encuentra sujeta, además de la observancia de las normas legales de carácter imperativo y dispositivo, a mecanismos de autorregulación de la actividad de los PSC.

Conforme explica Pérez, el fundamento principal de la capacidad para obligar de los sistemas de autorregulación es el consentimiento de las partes y las obligaciones que generan para adherirlos a los distintos sistemas (códigos de conducta, normas, mecanismos de resolución de conflictos, etc.), toda vez que el consentimiento, en base al art. 1.261 C.c. es una de las condiciones esenciales para la existencia y obligatoriedad de un contrato (arts. 1.091 y 1.278 C.c.).²⁹³

²⁹² (J. Almagro, Comentarios al art. 1258..., 2006: 591).

²⁹³ (M. Pérez, 2009: 101).

Respecto de los tipos de autorregulación existentes en la actualidad, es posible distinguir dos sistemas: la regulación sectorial y la individual. Pasaremos a explicar brevemente en qué consisten cada uno de ellos.

a) Regulación sectorial.-

En este caso la regulación proviene de la adopción de manera conjunta por parte de un grupo de sujetos con los mismos intereses, de las normas que regularán su actividad. Este tipo de regulación a su vez, se lleva a cabo a través de los siguientes mecanismos:

a.1.) Marcas basadas en normas o especificaciones.-

Las normas técnicas o especificaciones pueden tener tres orígenes según su elaboración: españolas, europeas o internacionales. Se refieren al cumplimiento de normas de carácter técnico y tecnológico tendientes a la normalización de la actividad. Revisten de importancia debido a que por medio de estas normas se fijan determinadas características técnicas de productos industriales, tales como duración, seguridad, fiabilidad, compatibilidad con otros productos o sistemas, etc.

La autorregulación de carácter eminentemente técnico se lleva a cabo por medio de los siguientes instrumentos: especificaciones técnicas, reglamentos técnicos, certificaciones y/o homologación.²⁹⁴

a.2.) Marcas basadas en códigos de conducta o guías.-

Los códigos de conducta conforme los define Maluquer De Motes, constituyen propuestas o principios que se llevan a cabo por la propia ley, por agrupaciones de empresarios o por empresas de un sector, con la finalidad de establecer unos principios y unas reglas de garantía y de cumplimiento, para todas las empresas que operan en el sector o

²⁹⁴ Para un estudio más detallado de estos instrumentos (M. Pérez, 2009: 104-110).

para empresas que forman parte y se encuentran agrupadas o incorporadas a una asociación.²⁹⁵

La finalidad de estos instrumentos reside en el deseo de un determinado sector por generar confianza en los clientes respecto de los productos o servicios que ofrecen. La elaboración, adhesión y cumplimiento de códigos de conducta adquiere notable importancia en la prestación de servicios de la Sociedad de la Información, en el entendido que posibilitan uniformizar las obligaciones de los prestadores de servicios, generan mayor confianza en los consumidores y se establece una mayor facilidad para la resolución de conflictos. Estos códigos de conducta se encuentran previstos en el art. 18 LSSI.²⁹⁶

b) Regulación individual.-

En este caso la regulación proviene de una sola persona, vale decir, constituyen obligaciones que se impone a sí mismo un sujeto para el desarrollo de su actividad y la contratación con terceros. A esta clase de autorregulación se la denomina comúnmente como “*prácticas*” y “*políticas*” de la prestación del servicio, siendo precisamente la que normalmente se presenta en el ámbito de la prestación de servicios de certificación de firma electrónica.

De hecho, la DFE hace referencia indirecta a este sistema auto regulatorio,²⁹⁷ en tanto que la normativa española contenida en el art. 19 LFE dispone que todos los PSC deben

²⁹⁵ Carlos J. Maluquer De Motes Bernet, “Los códigos de conducta como fuente del Derecho”, *Derecho Privado y Constitución*, nº17, enero-diciembre 2003, pp. 362-363.

²⁹⁶ El art. 18 LSSI dispone que: “1.Las Administraciones públicas impulsarán, a través de la coordinación y el asesoramiento, la elaboración y aplicación de códigos de conducta voluntarios, por parte de las corporaciones, asociaciones u organizaciones comerciales, profesionales y de consumidores, en las materias reguladas en esta Ley. La Administración General del Estado fomentará, en especial, la elaboración de códigos de conducta de ámbito comunitario o internacional. Los códigos de conducta podrán tratar, en particular, sobre los procedimientos para la detección y retirada de contenidos ilícitos y la protección de los destinatarios frente al envío por vía electrónica de comunicaciones comerciales no solicitadas, así como sobre los procedimientos extrajudiciales para la resolución de los conflictos que surjan por la prestación de los servicios de la sociedad de la información.2. En la elaboración de dichos códigos, habrá de garantizarse la participación de las asociaciones de consumidores y usuarios y la de las organizaciones representativas de personas con discapacidades físicas o psíquicas, cuando afecten a sus respectivos intereses. Cuando su contenido pueda afectarles, los códigos de conducta tendrán especialmente en cuenta la protección de los menores y de la dignidad humana, pudiendo elaborarse, en caso necesario, códigos específicos sobre estas materias. Los poderes públicos estimularán, en particular, el establecimiento de criterios comunes acordados por la industria para la clasificación y etiquetado de contenidos y la adhesión de los prestadores a los mismos.3.Los códigos de conducta a los que hacen referencia los apartados precedentes deberán ser accesibles por vía electrónica. Se fomentará su traducción a otras lenguas oficiales, en el Estado y de la Unión Europea, con objeto de darles mayor difusión”.

²⁹⁷ Así lo entendemos de la lectura del Anexo II, DFE que señala: “*k) antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios.*”

formular una Declaración de Prácticas de Certificación con carácter previo a ofrecer sus servicios, siendo obligación del PSC ponerlos a disposición del público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.²⁹⁸

Evidentemente, una de las obligaciones fundamentales del PSC es la redacción de las denominadas Declaración de Prácticas de Certificación (DPC)²⁹⁹ y las Políticas de Certificación (PC)³⁰⁰, a las cuales el cliente debe acudir por remisión, toda vez que se deja claramente establecido que ambos instrumentos formarán parte integral e indisoluble del contrato. La LMFE contempla implícitamente esta obligación al indicar que el PSC deberá *“actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas”* (art. 9.1.a.).

Asimismo, es necesario hacer notar que el PSC se encuentra igualmente obligado a informar sobre las modificaciones que sufran la DPC como las PC, tanto a los Solicitantes, Firmante/Suscriptores, a las Entidades de Registro que estén vinculadas a aquél, como a los Usuarios de los certificados.

A objeto de comprender el contenido de la DPC y las PC, acudiremos a las definiciones que de estos instrumentos hace un PSC español en concreto, CAMERFIRMA.³⁰¹

La Declaración de Prácticas de Certificación (CPS) es definida como un conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados. En general contiene información detallada sobre su sistema de seguridad, soporte, administración y

²⁹⁸ El Artículo 19 LFE establece el contenido de la Declaración de prácticas de certificación, de la siguiente manera:

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta ley 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.

2. La declaración de prácticas de certificación de cada prestador estará disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

²⁹⁹ La abreviación inglesa es CPS “Certificate Practice Statement” - Declaración de Prácticas de Certificación.

³⁰⁰ La abreviación inglesa es CP “Certificate Policy” - Política de Certificación.

³⁰¹ AC Camerfirma S.A. es un certificador legalmente establecido en España. Emite certificados empresariales para el territorio español dentro de la Jerarquía de *Chambers of Commerce Root (CCJ)*, dicha Jerarquía está diseñada para construir una red de confianza donde las Entidades de Registro son gestionadas por las Cámaras de Comercio, Industria y Navegación de España, teniendo como objetivo fundamental la emisión de certificados digitales de identidad empresarial.

emisión de los Certificados, además sobre la relación de confianza entre el o Tercero que confía y la Autoridad de Certificación. Pueden ser documentos absolutamente comprensibles y robustos, que proporcionan una descripción exacta de los servicios ofertados, procedimientos detallados de la gestión del ciclo vital de los certificados, etc.

Política de Certificación (CP) es el conjunto de reglas que definen la aplicabilidad de un certificado en una comunidad y/o en alguna aplicación, con requisitos de seguridad y utilización comunes, es decir, en general una Política de Certificación debe definir la aplicabilidad de tipos de certificado para determinadas aplicaciones que exigen los mismos requisitos de seguridad y formas de usos. Estos conceptos de Políticas de Certificación y Declaración de Prácticas de Certificación son distintos, pero aún así es muy importante su interrelación.³⁰²

Conforme aclara CAMERFIRMA, una Declaración de Prácticas de Certificación detallada no forma una base aceptable para la interoperabilidad de los PSC. Las Políticas de Certificación sirven mejor como medio en el cual basar estándares y criterios de seguridad comunes. En definitiva una Política define “*qué*” requerimientos de seguridad son necesarios para la emisión de cada tipo específico de certificado. La Declaración de Prácticas de Certificación nos dice “*cómo*” se cumplen los requerimientos de seguridad impuestos por la Política.³⁰³

Al respecto es necesario hacer notar que algunas empresas certificadoras manejan la DPC y las PC como dos cuerpos independientes, en tanto que otras, fusionan el contenido de ambas en un único documento; pero independientemente de redactarlas por separado o en texto único e integrado, lo importante es que el PSC cuente con estos instrumentos antes de ofertar sus servicios al público.

Conforme se tiene analizado, la DPC constituye el conjunto genérico de prácticas adoptadas por el PSC para la emisión de certificados, es decir, que sus previsiones son

³⁰² Conceptos extraídos de la DPC y PC de CAMERFIRMA, disponibles en <http://policy.camerfirma.com>

³⁰³ Aclaración extraída de la DPC y PC de CAMERFIRMA, disponibles en <http://policy.camerfirma.com>

normas generales (técnicas, de seguridad, de organización, etc.) que se aplican transversalmente a toda su actividad de certificación y, por ende, de manera general a todos los tipos de certificados que el PSC emite. En tanto que la PC, es el conjunto de reglas que definen la aplicabilidad de un tipo específico de certificado en una comunidad de usuarios.

En el contrato que nos ocupa, siendo el Firmante/Suscriptor un empresario mercantil, como se vio existen dos posibilidades: i) que se trate de un empresario mercantil colectivo; o ii) que sea un empresario mercantil individual. En ambos casos rige la misma DPC, pero la PC a aplicarse dependerá precisamente del tipo de certificado solicitado.

Puede tratarse de la solicitud de un simple certificado electrónico, o de un certificado reconocido; asumiendo, conforme venimos estudiando, que la opción del empresario solicitante es por un certificado reconocido, para el caso de que el Firmante/Suscriptor sea un empresario colectivo, serán de aplicación las PC de certificado reconocido emitido a personas jurídicas. En tanto que si el Firmante/Suscriptor es un empresario individual, le resultarán de aplicación las PC de certificado reconocido emitido a personas físicas.

En base a las explicaciones elaboradas precedentemente, para la integración del contrato de certificación reconocida resulta necesario tomar en cuenta, por último, precisamente las reglas contenidas en los denominados instrumentos de autorregulación en general, y particularmente, las ofrecidas en la DPC y las PC que el PSC ha elaborado individualmente. Entendemos que estas reglas deben integrar el contenido contractual y ello en aplicación de la buena fe contractual pues el Firmante/Suscriptor habrá confiado legítimamente en su aplicación.

Evidentemente, el contenido de la DPC y las PC adoptadas por el PSC pueden determinar, sin duda, que el Firmante/Suscriptor se haya decidido por éste y no por otro prestador del servicio de certificación. Estas normas servirán además de criterio de interpretación de las condiciones generales que rijan el contrato.

b.1.) Contenido de la DPC y las PC.-

A continuación procuraremos reflejar el contenido general de una típica DPC y PC. Así, estos documentos deben contener como mínimo las siguientes previsiones:³⁰⁴

A. Una introducción.-

En la que se establecen las consideraciones iniciales, la vista general del servicio e identificación de la comunidad y ámbito de aplicación. Se identifica y establecen los conceptos de Prestador de Servicios de Certificación (PSC), la Entidad de Registro (ER), el Firmante/Suscriptor, el Usuario que confía y el Solicitante. Asimismo se dispone el ámbito de aplicación y los usos del certificado, especificando los usos prohibidos y no autorizados. Finalmente se establece la dirección oficial de contacto con el PSC, que normalmente consiste en una dirección URL de Internet así como la dirección física de sus instalaciones desde la cual presta sus servicios.

a.1. Lista de acrónimos.- En este lugar el PSC elabora un listado de los acrónimos que emplea a lo largo de la DPC y las PC a objeto de una cómoda lectura de los mismos.

a.2. Lista de definiciones.- Asimismo, lo normal es que se incluya un listado de las definiciones y conceptos que el PSC emplea a lo largo de la DPC y PC.

B. Cláusulas Generales

b.1. Obligaciones.- Se especifican las obligaciones del PSC, de la ER, del Solicitante, del Tercero que confía y de la Entidad Repositorio.

b.2. Responsabilidad.- Se fijan los casos de exoneración de responsabilidad por parte del PSC, así como se establecen sus límites de responsabilidad en caso de pérdidas por transacciones. Finalmente se introducen las previsiones de responsabilidad financiera del PSC.³⁰⁵

³⁰⁴ Elaborado en base a la DPC y PC de CAMERFIRMA, disponibles en <http://policy.camerfirma.com>

³⁰⁵ El PSC que emite certificados reconocidos, por disposición del art. 20.2. LFE debe disponer de un seguro de responsabilidad civil que contemple sus responsabilidades, para indemnizar por daños y perjuicios que se puedan ocasionar a los usuarios de sus servicios: el Firmante/Suscriptor, el Usuario que confía, y a otros terceros, por un importe conjunto de 3.000.000 de euros.

b.3. Interpretación y ejecución.- En este acápite se establece cuál será la legislación aplicable al contrato de certificación, los medios de notificación y el procedimiento a seguirse en caso de resolución de disputas. Normalmente se establece un procedimiento arbitral, de manera que toda controversia o conflicto que se derive del contrato sea resuelta definitivamente mediante el arbitraje de derecho de un árbitro, que podría ser por ejemplo en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral.

b.4. Tarifas.- En esta parte se fijan las tarifas de emisión de certificados y de su renovación. Asimismo se establecen las previsiones referentes a las tarifas de acceso a los certificados, tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados (normalmente éstas son gratuitas), y las tarifas por el acceso al contenido de las Prácticas y Políticas de Certificación (éstas por disposición legal deben ser siempre gratuitas). Finalmente se fijan las políticas de reintegros que tiene el PSC.

b.5. Publicación y repositorios.- Se fijan las políticas y procedimientos para la publicación de información del PSC así como sus términos y condiciones, el modo de difusión de los certificados, la frecuencia de publicación y los controles de acceso que se fijan.

b.6. Auditorias.- El PSC establece la frecuencia con la que llevará a cabo las auditorías a su gestión, identificando y calificando al auditor responsable de llevarla a efecto, especificando la relación que existe entre el auditor y el PSC, los tópicos cubiertos por la auditoria y las previsiones para la auditoria en las ER.

b.7. Confidencialidad.- Apartado en el que se describe qué tipo de información se va a mantener confidencial y qué tipo de información será considerada como no confidencial. Por otra parte se establecen previsiones para la divulgación de información, así como para los casos de revocación y/o suspensión de certificados, definiendo el procedimiento de envío de

la información solicitada por autoridad competente, en los casos y forma establecidos legalmente.

b.8. Derechos de propiedad intelectual.- Apartado en el que el PSC establece que la propiedad intelectual de la DPC y las PC le pertenecen de forma exclusiva.

C. Identificación y Autenticación

c.1. Registro inicial.- En este sector se especifican los tipos de nombres que se admitirán en el certificado, previsiones respecto a los pseudónimos, las reglas utilizadas para interpretar varios formatos de nombres, disposiciones sobre unicidad de los nombres así como los procedimientos de resolución de disputas de nombres. Por otra parte, se establece el reconocimiento, autenticación y función de las marcas registradas, los métodos de prueba de la posesión de la clave privada, los pasos a seguir para conseguir la autenticación de la identidad de un individuo o la organización y su vinculación.

c.2. Renovación y revocación de la clave.- Aquí se fijan las reglas y procedimientos a seguirse tanto para la renovación como para la revocación de la clave privada (los datos de creación de firma), la reemisión después de una revocación y el modo de efectuar la solicitud de su revocación.

D. Requerimientos Operacionales

d.1. Solicitud de certificados.- Este apartado está destinado a fijar los procedimientos técnicos a seguir para la solicitud y emisión de un certificado, así como las disposiciones que hacen a la aceptación de certificados.

d.2. Suspensión y revocación de certificados.- Normalmente se efectúan una serie de aclaraciones previas, luego se establecen las causas de revocación de un certificado y los documentos justificativos, definiendo quién puede solicitar la revocación, explicando el procedimiento de solicitud de revocación y el periodo de revocación. Por otra parte se fijan las causales de suspensión de un certificado y se define el procedimiento para la solicitud de

suspensión, especificando los límites del periodo de suspensión. Asimismo, se dispone la frecuencia de emisión de Listas de Revocación de Certificados (LRC), los requisitos de comprobación de LRC, la disponibilidad de comprobación on-line de la revocación, los requisitos de la comprobación on-line de la revocación. Igualmente se informa de otras formas de divulgación de información de revocación disponibles, los requisitos de comprobación para otras formas de divulgación de información de revocación y los requisitos especiales de revocación por compromiso de las claves.

d.3. Procedimientos de Control de Seguridad.- Se establecen los tipos de eventos que son registrados, la frecuencia de procesado de los periodos de retención para los LOGs³⁰⁶ de auditoria, los métodos de protección de los LOGs de auditoria y los procedimientos de backup de los LOGs de auditoria. Por otra parte, se define el sistema de recogida de información de auditoria, los mecanismos de notificación al sujeto y causa del evento, junto con un análisis de vulnerabilidades.

d.4. Archivo de registros.- Se especifican el tipo de archivos registrados, el periodo de retención para el archivo, la protección del archivo y los procedimientos de backup del archivo. También se explican los requerimientos para el sellado de tiempo de los registros, el sistema de recogida de información de auditoria y los procedimientos para obtener y verificar información archivada.

d.5. Cambio de clave.- En este sector se explica que antes de que el uso de la clave privada del PSC caduque, se realizará un cambio de claves.

d.6. Recuperación en caso de compromiso de la clave o desastre.- Se describe los casos en que la clave de una entidad se compromete y el procedimiento a seguirse para la recuperación del sistema en caso que ello ocurriera, definiendo la instalación de seguridad después de un desastre natural u otro tipo de desastre.

³⁰⁶ De acuerdo a Oxford Dictionary la definición de LOG es: "Registro oficial de eventos durante un periodo de tiempo en particular. Para los profesionales en seguridad informática un log es usado para registrar datos o información sobre quién, qué, cuándo, dónde y por qué (who, what, when, where y why, W5) un evento ocurre para un dispositivo en particular o aplicación."; tomado de http://www.wikilearning.com/monografia/control_administracion_e_integridad_de_logs-que_es_un_log/3485-2

d.7. Cese del PSC.- En este sector el PSC establece los procedimientos a seguir en caso que cesen sus actividades y el modo en que se transferirán los certificados vigentes a otro PSC.

E. Controles de Seguridad Física, Procedimental y de Personal

e.1. Controles de Seguridad física.- Las disposiciones que hacen a este sector, se refieren a las previsiones que toma el PSC respecto a la ubicación y construcción de sus instalaciones, el modo de acceso físico a las mismas y las restricciones que se establecen al respecto por razones de seguridad. Igualmente se explicita el modo de alimentación eléctrica y aire acondicionado, las previsiones contra exposición al agua, protección y prevención de incendios, así como el sistema de almacenamiento de información.

e.2. Controles procedimentales.- Se explican los roles de confianza que se asigna al personal del PSC, el número de personas requeridas por cada tarea así como la identificación y autenticación para cada rol.

e.3. Controles de seguridad de personal.- Se definen los requerimientos de antecedentes, calificación, experiencia y acreditación del personal que trabaja en la empresa certificadora, fijando los procedimientos de comprobación de antecedentes, los requerimientos de formación, la frecuencia de la actualización de la formación y la secuencia de rotación de tareas. También es usual que se fijen las sanciones al personal por acciones no autorizadas y los requerimientos de contratación de personal. Finalmente se delimita el tipo de documentación proporcionada al personal.

F. Controles de Seguridad Técnica

f.1. Generación e instalación del par de claves.- Éste junto con el siguiente, definitivamente constituyen los acápites más importantes de toda DPC y PC, razón por la que analizaremos este segmento con el debido detenimiento, pues se establecen los procedimientos seguros para la generación del par de claves del PSC³⁰⁷ así como la generación del par de claves del

³⁰⁷ La generación de las claves del PSC se deben efectuar en un dispositivo que cumpla estándares mínimos de seguridad.

Firmante/Suscriptor³⁰⁸, especificando el modo en que se hará entrega de la clave pública del Firmante/Suscriptor al PSC³⁰⁹ y la entrega de la clave pública del PSC a los Usuarios del certificado³¹⁰. Por otra parte, se establece el tamaño y periodo de validez de las claves del PSC así como el tamaño y periodo de validez de las claves del Firmante/Suscriptor³¹¹, junto a los parámetros de generación de la clave pública tanto del PSC como del Firmante/Suscriptor, explicando el modo en que se efectuará la comprobación de la calidad de los parámetros Hardware/software de generación de claves y los fines del uso de la clave privada.

f.2. Protección de la clave privada.- Se establece que el PSC deberá realizar los esfuerzos que razonablemente estén a su alcance, para confirmar que tanto las claves privadas suyas (con las que firma el certificado digital) como las que pertenecen al Firmante/Suscriptor, continúan siendo confidenciales y mantienen su integridad.

f.3. Estándares para los módulos criptográficos.- En este segmento se describen los procedimientos que se van a seguir para la custodia de la clave privada (tanto del PSC³¹² como del Firmante/Suscriptor³¹³), se establece la manera en que el PSC efectuará la copia de seguridad de su clave privada³¹⁴ (no la del Firmante/Suscriptor pues está expresamente

³⁰⁸ Las claves del pueden ser creadas en por el mismo mediante dispositivos hardware o software autorizados por el PSC o pueden ser creadas por el PSC usualmente en formato software PKCS#12, usando para su generación el algoritmo de clave pública RSA con una longitud de 1024 bits.

³⁰⁹ El envío de la clave pública al PSC para la generación del certificado cuando el circuito así lo requiera, se realiza mediante un formato estándar preferiblemente en formato PKCS#10 o X509 autofirmado.

³¹⁰ El certificado del PSC y su fingerprint (huella digital) estarán a disposición de los usuarios en su página Web.

³¹¹ Las claves privadas del están basadas en el algoritmo RSA con una longitud de 1024 bits. El periodo de uso de la clave pública y privada varía en función del tipo de certificado.

³¹² La clave privada de firma del PSC debe ser mantenida y usada en un dispositivo criptográfico seguro que cumpla mínimos requerimientos de seguridad. Normalmente se requiere un control multi-persona para la activación de la clave privada del PSC, por el cual se necesitan de al menos dos (2) a cuatro (4) personas para la activación de las claves, lo que se denomina: “*Proceso m de n*”.

³¹³ La clave privada del Firmante/Suscriptor se puede almacenar en un dispositivo software o hardware. Cuando se almacene en formato software el PSC ofrecerá las instrucciones de configuración adecuada para un uso seguro en las aplicaciones reconocidas. El PSC debe proceder a publicar los dispositivos permitidos para la generación y custodia de las claves en su dirección URL. En todo caso, la información respecto al tipo de creación y custodia de claves está incorporada en el propio certificado digital permitiendo al Usuario y tercero que confía actuar en consecuencia. El PSC no debe almacenar ni copiar la clave privada del usuario cuando esta es generada por el propio PSC, es decir aquella entregada en soporte software. Para certificados en soporte hardware es el usuario quien genera y custodia la clave privada en la tarjeta criptográfica entregada por el PSC, quien únicamente almacenará una copia de la clave privada del Firmante/Suscriptor cuando esta se use “exclusivamente” para cifrado de datos.

³¹⁴ El PSC realiza una copia de back up de las claves privadas que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de esta necesita al menos de la participación de dos personas. Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

prohibido por el art. 18.a) LFE)³¹⁵ y los procedimientos para el archivo de la clave privada (tanto del PSC³¹⁶ como del Firmante/Suscriptor³¹⁷). Conjuntamente se definen los mecanismos para la introducción de la clave privada en el módulo criptográfico;³¹⁸ el método de activación de la clave privada;³¹⁹ el método de desactivación de la clave privada;³²⁰ y finalmente el método de destrucción de la clave privada;³²¹ en todos los casos anteriores se hace alusión a la clave privada tanto del PSC como del Firmante/Suscriptor.

f.4. Otros aspectos de la gestión del par de claves.- Se establecen las disposiciones que hacen al archivo de la clave pública del PSC³²². Asimismo, se dispone sobre el periodo de uso para las claves públicas y privadas del Firmante/Suscriptor.³²³

f.5. Controles de seguridad informática.- En esta sección se definen los requerimientos técnicos de seguridad informática específicos así como la valoración de la seguridad informática.

f.6. Controles de seguridad del ciclo de vida.- Se describen los controles de desarrollo del sistema, los controles de gestión de la seguridad, la gestión de seguridad, la clasificación y

³¹⁵ En todo caso, las claves de Firmante/Suscriptor en software pueden ser almacenadas para su posible recuperación en caso de contingencia, en un dispositivo de almacenamiento externo separado de la clave de instalación tal como se indica en los manuales de instalación de claves en software. Las claves de Firmante/Suscriptor en hardware no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

³¹⁶ Las claves privadas del PSC normalmente son archivadas por un periodo no inferior a **10 años** después de la emisión del último certificado. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada del PSC en el dispositivo criptográfico inicial.

³¹⁷ El Firmante/Suscriptor podrá almacenar las claves entregadas en software durante el periodo de duración del certificado, posteriormente deberá destruirlas asegurándose antes de que no tiene ninguna información cifrada con la clave pública. Solo en caso de certificados de cifrado el Firmante/Suscriptor podrá almacenar la clave privada el tiempo que crea oportuno. En este caso el PSC también guardará copia de su clave privada asociada al certificado de cifrado.

³¹⁸ Las claves del PSC se crean en el interior de los dispositivos criptográficos. En tanto que las claves en software de los Firmante/Suscriptores se crean en los sistemas del PSC y son entregadas al Firmante/Suscriptor normalmente en un dispositivo software PKCS#12. Finalmente, las claves en hardware de los Firmante/Suscriptores se crean dentro del dispositivo criptográfico entregado por el PSC al Firmante/Suscriptor

³¹⁹ El acceso a la clave privada del Firmante/Suscriptor se realiza por medio de los denominados “*Datos de activación*”, que son datos privados, como PIN’s o contraseñas empleados para la activación de la clave privada, que conocerá solamente el Firmante/Suscriptor y que evitara tenerlo por escrito. En tanto que las claves del PSC se activan, como se tiene dicho, por un “*Proceso m de n*”.

³²⁰ La clave privada del Firmante/Suscriptor quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de lectura. Cuando la clave esté en soporte software, podrá ser desactivada mediante el borrado de dichas claves de la aplicación correspondiente en la que estén instaladas. Para la desactivación de la clave privada del PSC se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.

³²¹ Anteriormente a la destrucción de las claves se emitirá una revocación del certificado de las claves públicas asociadas a las mismas. Se destruirán físicamente o reinicializarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de las claves privadas del PSC. Para la eliminación se seguirán los pasos descritos en el manual del administrador del equipo criptográfico. Finalmente se destruirán de forma segura las copias de seguridad. Las claves del Firmante/Suscriptor en software se podrán destruir mediante el borrado de estas siguiendo las instrucciones de la aplicación que las alberga. Las claves del Firmante/Suscriptor en hardware podrán ser destruidas mediante un software especial en los puntos de Registro (ER) o ante el propio PSC.

³²² El PSC en cumplimiento de lo establecido por el artículo 20.f) LFE debe mantener sus archivos por un periodo mínimo de quince (15) años.

³²³ Un certificado no debería ser usado después del periodo de validez del mismo aunque el Usuario que confía pueda usarlo para verificar datos históricos teniendo en cuenta que no existirá un servicio de verificación válido para ese certificado.

gestión de información y bienes, las operaciones de gestión, la gestión del sistema de acceso, la gestión del ciclo de vida del hardware criptográfico y finalmente las previsiones sobre la evaluación de la seguridad del ciclo de vida del certificado.

f.7. Controles de seguridad de la red.- Se refiere a los mecanismos adoptados por el PSC para proteger el acceso físico a los dispositivos de gestión de red. En todo caso, la información confidencial que se trasfiere por redes no seguras debe realizarse de forma cifrada mediante uso de protocolos SSL.³²⁴

f.8. Fuentes de Tiempo.- Se especifica los procedimientos de sincronización de tiempos.³²⁵

G. Perfiles de Certificado, LRC y OCSP

g.1. Perfil de Certificado.- Se establece el perfil del certificado³²⁶, el número de versión³²⁷, las extensiones del certificado³²⁸, se describen los Identificadores de objeto (OID)³²⁹ de los algoritmos, se determinan las restricciones de los nombres³³⁰ y finalmente se describe el Identificador de objeto (OID) de la Política de Certificación.³³¹

g.2. Perfil de LRC.- Se especifica el número de versión de la LRC y sus extensiones.

g.3. Perfil de OCSP.- Se especifica el perfil empleado para el servicio OCSP.

H. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

h.1. Autoridad de las políticas.- Se especifica a la entidad que desempeñara las funciones de autoridad de las Prácticas y Políticas de certificación, que normalmente recae en el departamento jurídico del PSC, siendo el responsable de su administración.

³²⁴ Contracción del vocablo inglés “*Secure Socket Layer*”. Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.

³²⁵ Por ejemplo CAMERFIRMA tiene un procedimiento de sincronización de tiempo coordinado con el ROA Real Instituto y Observatorio de la Armada en San Fernando vía NTP. También obtiene una fuente segura vía GPS y sincronización vía Radio.

³²⁶ El perfil mayormente empleado al presente está en conformidad con el estándar X.509 versión 3 y al RFC 3280 “*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*”.

³²⁷ Como consecuencia de lo anterior, son certificados X.509-Versión 3.

³²⁸ Se fijan de conformidad a cada tipo de certificado en la PC asociada al mismo.

³²⁹ El OID constituye un Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.

³³⁰ Los nombres contenidos en los certificados deben estar restringidos a “*Distinguished Names*” X.500, que son únicos y no ambiguos.

³³¹ En el caso de CAMERFIRMA, todos los certificados de usuario tienen un identificador de política que se ajusta al siguiente modelo: **1.3.6.1.4.1.17326.10.X.Y.Z.**; donde: X = tipo de certificado; Y = Soporte Hardware o Software; Z = Generación de la clave PSC o Firmante/Suscriptor

h.2. Procedimientos de especificación de cambios.- En este acápite, el PSC establece qué tipo de elementos pueden cambiar sin necesidad de notificación³³², así como los cambios que requieren notificación enumerando una lista de elementos, los mecanismos de notificación³³³, el periodo de comentarios que puedan efectuar al PSC los Firmante/Suscriptores y/o Usuarios, especificando los mecanismos de tratamiento de dichos comentarios.³³⁴

h.3. Publicación y copia de la política.- En cumplimiento de la obligación contenida en el art. 19 LFE, en esta sección se establece que una copia de la DPC y las PC estarán disponibles de manera gratuita, por escrito o en formato electrónico, en este último caso en la dirección URL del PSC.

h.4. Procedimientos de aprobación de la DPC.- En esta sección, se establece que la publicación de las revisiones de la DPC y las PC debe ser aprobada por un órgano competente de la empresa certificadora, normalmente la Gerencia General.

V.- Sinopsis.-

Desde el punto de vista descriptivo podemos definir al contrato de certificación reconocida de firma electrónica, como aquel en el que el PSC se obliga a generar y entregar un certificado reconocido, debiendo publicarlo en un directorio de acceso público para su consulta, proporcionando simultáneamente los servicios que faciliten la validación o verificación del mismo, con la finalidad de identificar fehacientemente y en sentido amplio al Firmante/Suscriptor en el tráfico virtual, como requisito imprescindible para generar en el tráfico virtual un entorno seguro y confiable. Por su parte, el cliente o Firmante/Suscriptor se obliga a pagar, en la mayoría de los casos, un precio que consistirá en la entrega de una suma de dinero.

³³² Normalmente son las correcciones tipográficas o de edición o los cambios en los detalles de contacto.

³³³ Todos los cambios propuestos que puedan afectar sustancialmente a los Firmante/Suscriptores de la DPC y las PC normalmente serán notificados por e-mail a los Firmante/Suscriptores y serán inmediatamente publicados en la dirección URL del PSC para conocimiento de cualquier tercero interesado, incluidos los Usuarios del certificado.

³³⁴ Normalmente cualquier acción tomada como resultado de unos comentarios quedan a la discreción del PSC y su departamento jurídico, constituido como autoridad de las políticas.

Desde un punto de vista jurídico podemos identificarlo por las notas esenciales que lo caracterizan, constituyendo las siguientes: se trata de un contrato consensual, mercantil, bilateral sinalagmático, oneroso conmutativo, configurando una relación obligatoria duradera y de tracto continuo, sujeto a condiciones generales, perfeccionado por adhesión, revistiendo la calidad de contrato obligatorio y que no se establece como *intuitu personae*.

Es un contrato en el que tangencialmente aparecen combinados los elementos propios de los contratos típicos de servicios y obra, confluyendo prestaciones de dar, hacer y no hacer, por lo que dependiendo el caso, unas veces se configuran como obligaciones de resultado y otras, constituyen obligaciones de medios. Este negocio jurídico, además, se encuentra directamente vinculado con la prestación complementaria por parte del PSC de una serie de otros servicios concatenados y relacionados con la firma electrónica (v.gr. servicios de sellado de tiempo, acuse de recibo, homologación de certificados, etc.).

No obstante lo señalado, consideramos que la certificación reconocida constituye un contrato autónomo y principal, que dispone de causa única, por lo que tiene vida propia. No obstante que denota algunas similitudes aparentes con otros contratos típicos, sin embargo, la comprensión de su naturaleza permite inferir que se trata de un contrato distinto e independiente del cual devienen relaciones obligacionales distintivas.

La función principal que cumple este negocio jurídico en el ámbito empresarial es la identificación - en sentido amplio - de los operadores económicos en el tráfico virtual, como requisito imprescindible para generar un entorno seguro, brindando niveles óptimos de seguridad a quienes intervienen en redes abiertas de comunicación a objeto de efectuar comercio electrónico en sentido estricto, lo que deviene en la generación de confianza, particularmente por parte de los Usuarios del certificado reconocido. En definitiva, seguridad y confianza son los ingredientes que determinan la causa de este contrato, de modo que las

partes dan cause a intereses legítimos y los resultados que buscan establecer, son también lícitos desde el punto de vista del ordenamiento legal.

La circunstancia de que el contrato se materialice a través de un modelo tipo del que surgirán una sucesión de operaciones o servicios relacionados con la firma electrónica, no determina que se establezca como un contrato complejo. Invariablemente debemos concebirlo como un contrato único con pluralidad de objeto y unidad de causa. La probabilidad de que en la práctica pueda encontrarse vinculado a otros contratos típicos de obra y servicios, no le niega la autonomía contractual que defendemos y sostenemos.

Descartada la asimilación del contrato de certificación reconocida de firma electrónica dentro de cualquiera de los tipos legales con los que cabría alguna semejanza (contrato de mandato, arrendamientos de obra o servicios), no obstante de constituir un contrato nominado, hemos proclamado su atipicidad, a pesar de que se encuadre dentro de los contratos de actividad o se adscriba más precisamente al genérico *contrato de servicios*, pues estas categorías constituyen una calificación eminentemente doctrinal más no legal, por lo que podemos calificarlo finalmente como contrato atípico de naturaleza «*sui generis*», surgido en el ámbito de la empresa para gestionar las operaciones de comercio electrónico en sentido estricto.

Por todas las consideraciones previamente mencionadas consideramos que la presente investigación resulta oportuna y necesaria, dado que nos permite aportar soluciones a muchos problemas de índole jurídica de especial trascendencia en la teoría general de las obligaciones y contratos, y de gran importancia práctica, así como establecer la naturaleza y el marco jurídico del contrato de certificación reconocida.

Debemos asimismo poner de manifiesto que el estudio del contrato plantea cuestiones jurídicas de gran importancia práctica, como por ejemplo, el estudio de las Declaraciones de Prácticas y Políticas de Certificación elaboradas por los PSC, los deberes de información

precontractual en la formación del contrato, el contenido propiamente contractual, el régimen de responsabilidad en el que se desenvuelve la certificación, entre otras.

El estudio de este contrato demanda igualmente, por un lado, identificar de manera general a los distintos sujetos que intervienen en las actividades de certificación, determinando la posición jurídica y el rol que desempeñan en el contrato de certificación reconocida y, por otro, establecer de modo particular la capacidad que requieren las partes contractuales a objeto de celebrar este negocio, para finalmente estudiar los elementos objetivos y formales del contrato, labor que acometeremos en nuestro siguiente Capítulo.

CAPÍTULO TERCERO

ELEMENTOS DEL CONTRATO

I. Nociones previas.-

Conforme se ha sostenido preliminarmente las firmas electrónicas pueden ser utilizadas en variados escenarios y para un número ilimitado de propósitos. Unas veces serán empleadas exclusivamente dentro de sistemas basados en acuerdos voluntarios de Derecho privado, celebrados entre un número determinado de participantes (denominados “*con acuerdo previo*”). Otras veces pueden ser empleadas en sistemas que no se basan en dichos acuerdos y se celebran entre un número indeterminado de participantes (denominados “*sin acuerdo previo*”).

En el primer caso, las partes pueden convenir el empleo de certificados electrónicos para respaldar sus firmas electrónicas y dar mayor seguridad a sus actividades, o simplemente pueden prescindir de ellos, estableciendo contractualmente el modo en que se reconocerán mutuamente los efectos de los mecanismos tecnológicos utilizados para firmar electrónicamente. En el segundo caso, es decir cuando participa un número indeterminado de personas y no existen en consecuencia acuerdos previos para el reconocimiento de sus firmas electrónicas, resulta imprescindible el empleo de certificados electrónicos.

En ese sentido, el contrato de certificación de firma electrónica se presenta en sistemas *con acuerdo previo*, pero fundamental e imprescindiblemente en sistemas *sin acuerdo previo* para el uso de firmas electrónicas. Puede tener como partes contractuales a personas físicas o jurídicas, de derecho público o privado, siendo en este último caso las normas del derecho comercial y/o las del derecho civil las que regirán el contrato, lo cual dependerá en última instancia de la condición de comerciantes, o no, de las partes contratantes. En cualquiera de los supuestos señalados, el intercambio electrónico de datos

puede acontecer por redes de comunicación cerradas (v.gr. EDI cerrado)³³⁵ o abiertas (v.gr. Internet). Se puede contratar la emisión de un simple certificado electrónico (o no reconocido) o de un certificado reconocido.

Por otra parte, piénsese que la persona que solicita un certificado electrónico lo hace en función de un interés por efectuar actos seguros de comercio electrónico. Como se ha estudiado en el Capítulo Primero, el término comercio electrónico posee dos acepciones:

i) En sentido amplio, el cual se refiere a todo intercambio de datos por medios electrónicos ya sea que se encuentre relacionado - o no - con la actividad comercial estrictamente, por lo que no necesariamente da lugar a una contratación electrónica, caso de las declaraciones impositivas en línea por ejemplo, o cualquier otro tipo de relacionamiento electrónico con particulares o los órganos de la administración a fines no comerciales, lo que Martínez prefiere denominar genéricamente como *intercambio o transmisión electrónica de datos*, para evitar confusiones precisamente con la segunda acepción del término;

ii) En sentido estricto, el cual abarca exclusivamente a las transacciones comerciales electrónicas, las cuales pueden dar lugar a contrataciones en línea o simplemente consistir en la ejecución de pagos electrónicos.³³⁶

Conforme se tiene adelantado, de todos los hipotéticos casos que pueden dar lugar a una contratación de certificación de firma electrónica, a fines de la presente investigación se ha procedido a delimitar el ámbito de estudio al contrato de certificación electrónica: i) Donde tanto el Firmante/Suscriptor como el PSC son ambos empresarios comerciales; ii) En el que la intención del empresario Firmante/Suscriptor estriba en efectuar transacciones comerciales electrónicas seguras (comercio electrónico en sentido estricto) haciendo uso de su firma electrónica en sistemas que no se basan en acuerdos voluntarios de Derecho privado

³³⁵ Con relación a la tecnología EDI es necesario recordar una precisión, en sentido que posee dos versiones: el *close EDI* o EDI cerrado conforme fue concebido inicialmente para operar en redes cerradas de comunicación, y el reciente *open EDI* o EDI abierto, que permite actuar en redes abiertas, tal el caso de Internet (J. Echavarría, 2001: 27).

³³⁶ (A. Martínez, 2001: 29-30).

y se celebran entre un número indeterminado de participantes; en los que los datos se transmiten por redes abiertas de comunicación, razón que motiva la adquisición de un certificado electrónico que respalde dicha firma a objeto de avalar su plena identidad ante sus clientes en la red, siendo su intencionalidad además, dotar a su firma y los documentos electrónicos suscritos con ella de la validez y eficacia jurídica que la ley reconoce a las firmas manuscritas y los documentos privados respectivamente, es decir, equivalente funcional; iii) Lo que da lugar a la emisión de un certificado reconocido.

En otras palabras y a objeto de contextualizar nuestro plan de estudio, partiremos del supuesto que un empresario (individual o colectivo), que desea efectuar negocios comerciales valiéndose de una red abierta (*Internet*), con un número indeterminado de potenciales clientes, es decir actuando en un sistema *sin acuerdo previo*, deberá acudir a un PSC, quien es un empresario que se dedica típica y profesionalmente a la actividad de certificación prestando servicios al público, a objeto que le emita un certificado reconocido con el cual avalará su plena identidad ante sus clientes en la red, dotando a su firma y los documentos electrónicos suscritos con ella de la validez y eficacia jurídica, que la ley reconoce a las firmas manuscritas y los documentos privados respectivamente, estando facultado para contratar electrónicamente y así desarrollar negocios de comercio electrónico (en sentido estricto), cuyo objeto contractual consistirá en bienes de naturaleza tangible o intangible.

Los primeros se articulan a través de contratos de compraventa o suministro (*comercio electrónico indirecto*); en tanto que los segundos, mediante contratos de cesión de derechos y/o contratos de prestación de servicios (*comercio electrónico directo*).

Con las consideraciones previas, señalaremos que el contrato de certificación reconocida se articula en torno a elementos objetivos: i) el certificado reconocido; ii) los datos de creación y de verificación de firma electrónica; iii) los dispositivos de creación y de verificación de firma electrónica; a cuyo alrededor, a su vez, se interrelacionan tres elementos

subjctivos: i) el Prestador de Servicios de Certificación (PSC), tercera parte de confianza - entre el Firmante/Suscriptor y el Usuario del certificado - quien normalmente actúa por medio de las denominadas Entidades de Registro (ER); ii) el Firmante/Suscriptor (titular de la firma y el certificado reconocido); y iii) el Usuario del certificado (verificador de la firma electrónica).

Por consiguiente nuestro propósito en este acápite consiste, por un lado, en identificar de manera general a los distintos sujetos que intervienen en las actividades de certificación, determinando la posición y el rol que desempeñan en el contrato de certificación reconocida y, por otro, establecer en particular la capacidad que requieren las partes contractuales a objeto de celebrar el contrato, para finalmente estudiar los elementos objetivos y formales del contrato.

Para ello efectuaremos un análisis respecto de las disposiciones que la normativa comunitaria europea y española prevén de modo general en torno a la temática planteada, así como respecto de la reglas particulares que rigen la prestación de servicios de certificación de firma electrónica, en procura de alcanzar una mejor comprensión y discernimiento de la materia objeto de estudio.

II. Elementos personales o subjetivos.-

2.1. El Prestador de Servicios de Certificación (PSC).-

El art. 2. de la LFE define al Prestador de Servicios de Certificación, como *“la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica”*.³³⁷ El PSC en consecuencia puede prestar diferentes servicios, aunque lógicamente su función básica es la emisión de certificados. La LFE no obstante, deja abierta la posibilidad de que los PSC no expidan certificados al público y que presten otros servicios en relación con la firma electrónica.

³³⁷ La DFE lo define en el art. 2.11 “proveedor de servicios de certificación: la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica”. En tanto que la LMFE establece en su art. 2.e. “Por prestador de servicios de certificación se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas”.

Es importante resaltar además, que desde nuestro punto de vista el PSC se configura como un auténtico prestador de Servicios de la Sociedad de la Información.³³⁸

Asimismo como se tiene dicho, el PSC puede ser una persona física o jurídica, de derecho público o privado, lo que nos plantea un gran abanico de posibilidades respecto de su condición,³³⁹ mismas que procuraremos reflejar en el Cuadro (A) de la página siguiente.

Nótese en consecuencia, que en base a las delimitaciones planteadas para el específico contrato que se estudia, el PSC es normalmente una entidad jurídica, de derecho privado y comercial (empresario colectivo), dedicada a la emisión de certificados reconocidos de clave pública, mismos que vinculan un par de claves con una persona determinada (el Firmante/Suscriptor) de forma segura, cubriendo así la necesidad de servicios de terceras partes de confianza en el comercio electrónico de los tenedores de pares de claves asimétricas.

Para la prestación de sus servicios se halla sujeto al cumplimiento de las disposiciones contenidas en la LFE, de conformidad a lo establecido en su art. 1 “*Esta ley regula la... prestación de servicios de certificación*” y el art. 2, que dispone “*Esta ley se aplicará a los prestadores de servicios de certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España*”.³⁴⁰

³³⁸ Así lo manifiesta también Pérez al señalar que “*Los prestadores de servicios de certificación... son además de prestadores de servicios de la sociedad de la información* (las negrillas son nuestras) *personas que prestan servicios relacionados con la firma electrónica, siendo su labor más representativa la de expedir certificados electrónicos.*” (M. Pérez, 2002: 931).

³³⁹ Aparte de la inicial denominación como “Autoridad de Certificación” que se dio a los PSC, surgió la de “*Notarios electrónicos*”, con lo cual se agravó aun más la confusión en cuanto al ámbito de sus competencias y facultades, toda vez que aparentemente, se estaba confiriendo a los certificadores facultades de orden público para dar fe de las actuaciones que la ley ha reservado a los Notarios. Por ello, es necesario aclarar, que los certificadores (al menos en inicio) son personas de derecho privado, cuyas atribuciones se circunscriben a dicho ámbito. Cosa diversa es que los Notarios puedan ejercer sus competencias valiéndose de los medios electrónicos y tecnológicos, para lo cual, será necesario que el ordenamiento legal de un Estado, establezca las previsiones normativas que regulen dicho supuesto. Decimos que al menos en inicio, porque posteriormente distintas legislaciones de firma electrónica confirieron facultades de certificación a personas de orden público, a objeto de su interrelación con los ciudadanos, lo que se ha venido a denominar “*e-administration*”. (v.gr. en España el Departamento CERES, dependiente de la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda “FNMT-RCM”, organismo público al que, en virtud del art. 81 de la Ley 66/97, de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social, se atribuye la facultad de prestar servicios de seguridad para las comunicaciones a través de técnicas y medios electrónicos, informáticos y telemáticos de las personas físicas y jurídicas con las Administraciones Públicas. O más recientemente, la Dirección General de la Policía - dependiente del Ministerio del Interior- quien es competente para emitir el Documento Nacional de Identidad electrónico -DNIe- actuando como entidad de certificación).

³⁴⁰ La DFE establece respecto a su ámbito de aplicación, lo siguiente: “La presente Directiva crea un marco jurídico para la firma electrónica y para determinados **servicios de certificación** con el fin de garantizar el correcto funcionamiento del mercado interior.” (Las negrillas son nuestras).

Cuadro "A"
Personas que pueden constituirse hipotéticamente en PSC

Certificado	PSC	Contexto	Derecho Privado		Derecho Público	Certificación
			Ámbito Civil	Ámbito Comercial		
<p>Emite un Certificado Electrónico (Art. 6.1. LFE)</p> <p align="center">o</p> <p>Emite un Certificado Reconocido (Art. 11 LFE)</p>	Persona Natural	En todos los casos el tratamiento de los datos personales que precisen los PSC se sujetará a lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (art. 17 LFE)	Particular	Empresario mercantil individual		<p>1ª Opción:</p> <p>Puede que goce de una certificación, conforme las disposiciones del art. 26 de la LFE</p>
	Persona Jurídica	<p>En todos casos los PSC se encuentran en la obligación de informar y colaborar con el Ministerio de Ciencia y Tecnología (art. 30 LFE)</p> <p>En todos casos los PSC se encuentran en la obligación de observar las normas contenidas en la Ley 34/2000 sobre Servicios de la Sociedad de la Información, en todo lo que les fuere aplicable (art. 1 y ss. LSSI)</p>	<p>Asociaciones</p> <p>Fundaciones</p> <p>Sociedades civiles</p>	<p>Empresario mercantil colectivo</p> <p>Sociedades personalistas:</p> <ul style="list-style-type: none"> - Colectivas - Comanditarias <p>Sociedades de capital:</p> <ul style="list-style-type: none"> - Anónimas - Comanditaria por acciones - Limitadas 	<p>Entidades de la Administración que están autorizadas para emitir certificados destinados:</p> <p>Al público:</p> <ul style="list-style-type: none"> - FNMT-RCM <p>Emite certificados para el ámbito tributario</p> <p>Al ciudadano:</p> <ul style="list-style-type: none"> - Ministerio del Interior - Policía Nacional <p>Emite certificados para el relacionamiento electrónico del ciudadano con las entidades de la administración, a través del DNI electrónico.</p> <p>A la propia administración:</p> <ul style="list-style-type: none"> - Para el relacionamiento de las entidades públicas entre sí, o de éstas con el ciudadano. 	

Razón por la cual, las disposiciones legales contenidas en la LFE deben ser observadas e incorporadas por el PSC en el contrato de certificación reconocida que venimos estudiando.

Por consiguiente y tomando en cuenta el ámbito objetivo de la LFE, lo primero que se debe distinguir en un entorno electrónico que por definición es globalizado, es entre PSC nacionales, comunitarios e internacionales.³⁴¹

A los efectos de la aplicación de la LFE se entenderá que un PSC:

<p>Está establecido en España</p>	<p>cuando su residencia o domicilio social se halle en territorio español,</p> <p>siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y dirección de sus negocios,</p> <p>en otro caso, se atenderá al lugar en que se realice dicha gestión o dirección (art. 2.3)</p>
<p>Opera mediante un establecimiento permanente situado en territorio español</p>	<p>cuando disponga en él, de forma continuada o habitual, de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad (art. 2.4).</p>
<p>Presunción de establecimiento en España</p>	<p>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,</p> <p>la mera utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio no implicará, por sí sola, su establecimiento (art. 2.5)</p>

2.1.1.- Importancia de la cláusula de Mercado Interior.-

El mercado interior europeo se fundamenta en la inexistencia de obstáculos que puedan de algún modo limitar, impedir o restringir el principio de la *libre circulación*, en

³⁴¹ (M.A. Davara, 2004: 624). Al respecto, analizaremos más adelante la incidencia en la prestación de servicios de certificación de la Directiva 2006/123/CE del Parlamento Europeo y del Consejo, de 12 de diciembre de 2006, relativa a los servicios en el mercado interior, más conocida simplemente como Directiva “Servicios” o “Bolkestein”.

todos los ámbitos que inciden en el desarrollo económico de la UE. El referido principio da origen a dos libertades fundamentales: la *libertad de establecimiento* y la *libre prestación de servicios*.³⁴²

En ese entendido, todo prestador de servicios podrá prestar libremente sus servicios actuando conforme al ordenamiento jurídico del Estado miembro donde se hallare establecido, lo que se conoce como “*cláusula del mercado interior*” o también “*principio del país de origen*”. Tanto la DFE, la DCE, la LFE y la LSSI deben interpretarse en base a la referida cláusula, de esta manera se pretende garantizar la prestación de servicios conforme el art. 49 del Tratado Constitutivo de la Comunidad Europea (TCE).

En base al principio de libertad de establecimiento y de conformidad con las disposiciones de los arts. 43 (pfo. 2) y 48 (pfo. 1) del TCE, toda persona comunitaria podrá establecerse de manera estable y permanente para desarrollar una actividad no asalariada de naturaleza económica en el territorio de la UE, en las mismas condiciones que el Estado de destino establece para sus propios nacionales.³⁴³

Asimismo, la libre prestación de servicios constituye el derecho de los ciudadanos europeos y de las sociedades de poder prestar sus servicios en el territorio de otro Estado Miembro de manera eventual o esporádica. De hecho el art. 49 TCE prohíbe expresamente cualquier obstáculo o restricción a la libre prestación de servicios, y es en este punto donde

³⁴² Un análisis sobre el establecimiento y la Ley aplicable a las entidades de certificación de firma electrónica, es abordado por María Pérez Pereira, “Establecimiento y Ley Aplicable al Prestador de Servicios de Certificación en España”, en *REDI: Revista Electrónica de Derecho Informático*, No. 26, Madrid, Alfa-Redi, septiembre/2000, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=551>

³⁴³ Reflejamos el contenido de las disposiciones del TCE citadas, conforme la versión consolidada del Tratado de Amsterdam (de 2 de octubre de 1997) y que entró en vigor desde el 1 de mayo de 1999:

“Art. 43º.- En el marco de las disposiciones siguientes, quedarán prohibidas las restricciones a la libertad de establecimiento de los nacionales de un Estado miembro en el territorio de otro Estado miembro... La libertad de establecimiento comprenderá el acceso a las actividades no asalariadas y su ejercicio, así como la constitución y gestión de empresas y, especialmente, de sociedades, tal como se definen en el segundo párrafo del artículo 48, en las condiciones fijadas por la legislación del país de establecimiento para sus propios nacionales, sin perjuicio de las disposiciones del capítulo relativo a los capitales.”;

“Art. 48.- Las sociedades constituidas de conformidad con la legislación de un Estado miembro y cuya sede social, administración central o centro de actividad principal se encuentre dentro de la Comunidad quedarán equiparadas, a efectos de aplicación de las disposiciones del presente capítulo, a las personas físicas nacionales de los Estados miembros...”

“Art. 49.- En el marco de las disposiciones siguientes, quedarán prohibidas las restricciones a la libre prestación de servicios dentro de la Comunidad para los nacionales de los Estados miembros establecidos en un país de la Comunidad que no sea el del destinatario de la prestación...”

entran en juego dos aspectos relacionados con los PSC, la aplicación de un sistema de autorizaciones o licencias y la aplicación de un sistema de acreditaciones o evaluación.

Con relación al régimen de prestación de los servicios de certificación, la norma establece que los mismos no se encuentran sujetos a autorización previa, debiendo efectuarse en modalidad de libre competencia. Asimismo, se determina la prohibición de establecerse restricciones para los servicios de certificación que provienen de algún otro Estado miembro del Espacio Económico Europeo (art. 5.1. LFE).

Esta disposición se encuentra también prevista en la DFE, la cual a momento de regular el acceso al mercado, dispone que los Estados miembros no deben condicionar la prestación de servicios de certificación a la obtención por parte de los PSC de autorizaciones previas (art. 3.1. DFE). Por otra parte, la DFE faculta a los Estados miembros a establecer o mantener sistemas voluntarios de acreditación, cuya finalidad consista en mejorar los niveles de provisión de los servicios de certificación. En estos casos, la DFE establece que las condiciones que un Estado implemente a momento de adoptar los referidos sistemas, deben necesariamente cumplir con los siguientes requisitos: ser objetivas, transparentes, proporcionadas y no discriminatorias. Finalmente se prohíbe expresamente que los Estados limiten el número de proveedores de servicios de certificación acreditados amparándose en la DFE (art. 3.2. DFE).

No obstante lo mencionado, la DFE respecto a los PSC que expiden al público certificados reconocidos, insta a los Estados a efectuar los esfuerzos necesarios para establecer mecanismos adecuados que posibiliten la supervisión de los PSC que se hallan establecidos en su territorio (art. 3.3. DFE).

En ese sentido, el legislador español adoptando las previsiones de la norma comunitaria dispuso inicialmente en el Real Decreto-Ley 14/1999, 17 de septiembre, de firma electrónica, el establecimiento de procedimientos de *acreditación* de los PSC, mismos

que eran regulados en su art. 6 y definidos en el art. 2, apartado m).³⁴⁴ Cuatro años después a tiempo de sancionar la LFE en vigencia, contempla sistemas de *certificación* (en lugar de acreditación) de los PSC, los cuales son regulados en el art. 26.³⁴⁵ Y en eso, el legislativo Ibérico es respetuoso con los principios postulados en la DFE, pues en tanto que estos sistemas de certificación se configuren como absolutamente voluntarios, son perfectamente compatibles con el principio de libre competencia y libre acceso para la prestación de servicios de certificación.

El art. 26.1. LFE define la certificación de un PSC como un procedimiento de carácter estrictamente voluntario, mediante el cual una entidad pública o privada que se encuentre debidamente cualificada emana una declaración en beneficio de un PSC, por la que se pone de manifiesto que dicho PSC satisface la observancia de ciertos requisitos de calidad y seguridad muy específicos en la prestación de sus servicios al público.³⁴⁶

El hecho que un PSC proceda a certificarse, desde el punto de vista comercial trae aparejadas una serie de ventajas toda vez que actuará en el mercado y frente a sus posibles clientes, como un certificador más fiable y otorgando niveles de seguridad mucho más elevados que el que ofrece su competencia representada por los PSC no certificados, en la medida que se ha sometido a un procedimiento voluntario de control por parte de entidades independientes que ha culminado con la concesión pública de una acreditación.

Pero lo que debe quedar claro, es que el reconocimiento de eficacia jurídica que

³⁴⁴ “Acreditación voluntaria del prestador de servicios de certificación”: resolución que establece los derechos y obligaciones específicos para la prestación de servicios de certificación y que se dicta, a petición del prestador al que le beneficie, por el organismo público encargado de su supervisión.

³⁴⁵ Al respecto Martínez aclara que en la LFE se ha optado, no sólo por un cambio terminológico (certificación en lugar de acreditación) sino por un cambio de orientación más profundo. Explica que mientras el RDL14/1999 optaba por un sistema de acreditación voluntaria de naturaleza pública, en el sentido de que, tras la intervención evaluadora por partes de entidades independientes, correspondía a la administración la concesión formal de tal acreditación, en la LFE se produce un cambio de orientación que implica la admisión de certificaciones de origen estrictamente privado (A. Martínez, 2004: 426). Desde nuestro punto de vista, esto es totalmente factible, pues el art. 2.13 de la DFE conceptúa a la acreditación como un permiso concedido, ya sea por un organismo público, ya sea por uno de naturaleza privada.

³⁴⁶ La DFE define en el art. 2.13. «acreditación voluntaria»: todo permiso que establezca derechos y obligaciones específicas para la prestación de servicios de certificación, que se concedería, a petición del proveedor de servicios de certificación interesado, por el organismo público o privado encargado del establecimiento y supervisión del cumplimiento de dichos derechos y obligaciones, 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.

otorga tanto el legislador comunitario como el español a una firma electrónica (cualquiera sea su naturaleza), no se encuentra condicionado de ninguna manera a la certificación de un PSC. En otras palabras, allá donde exista una firma electrónica, provenga de un PSC certificado o no, ésta debe ser reconocida y apreciada otorgándole el valor jurídico y eficacia que corresponda (art. 5.2. DFE; art. 26.4. LFE).

Ingresando en la esfera del procedimiento por el cual opera la certificación, el art. 26.2. LFE establece la legitimación activa y pasiva para la solicitud y concesión de la certificación, disponiendo que la certificación de un PSC puede *“ser solicitada por éste y podrá llevarse a cabo, entre otras, por entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo”*.

Finalmente el art. 26.3. LFE hace alusión a las normas que rigen los procedimientos de certificación, disponiendo que en éstos puedan emplearse *“normas técnicas u otros criterios de certificación adecuados. En caso de utilizarse normas técnicas, se emplearán preferentemente aquellas que gocen de amplio reconocimiento aprobadas por organismos de normalización europeos y, en su defecto, otras normas internacionales o españolas”*.

Para cerrar el tema de la certificación de los PSC, debemos volver a remarcar que su solicitud es totalmente voluntaria, y, en ningún caso, la ausencia de ésta impide el ejercicio de la actividad de prestación de servicios de certificación.

2.1.2. Incidencia de la “Directiva Servicios o Bolkestein” (DSMI) en la prestación de servicios de certificación.-

El 12 de diciembre de 2006, el Parlamento Europeo y el Consejo sancionaron la Directiva 2006/123/CE relativa a los servicios en el mercado interior (DSMI), más conocida simplemente como “Directiva Servicios” o “Bolkestein”.³⁴⁷ Se enmarca en el contexto de la

³⁴⁷ Frederik Frits Bolkestein es un político holandés que entre 1999 y 2004 fue miembro de la Comisión Europea, encargado del mercado interno y de la Unión Aduanera. Como comisario europeo para el mercado interno durante la presidencia de Romano Prodi, propuso y

“Estrategia de Lisboa”,³⁴⁸ cuyo propósito fundamental radica en reforzar normas comunitarias previas a objeto de consolidar definitivamente³⁴⁹ un mercado interior de servicios³⁵⁰ en Europa a través de la supresión de los obstáculos a la libre circulación de los servicios y a la libertad de establecimiento de los prestadores de servicios³⁵¹, para lo cual plantea cuatro objetivos fundamentales, a saber:

- i) facilitar la libertad de establecimiento (Capítulo III) y la libertad de prestación de servicios (Capítulo IV, Sección 1) en la UE; lo cual, en el caso específico de los servicios de certificación de firma electrónica viene a reforzar el contenido del art.3 “*Acceso al mercado*” y art.4 “*Principios del mercado interior*” de la DFE; así como del art. 2 “*Prestadores de servicios de certificación sujetos a ley*” y art.5 “*Régimen de prestación de los servicios de certificación*”, de la LFE.

En tanto que tratándose de los genéricos servicios de la sociedad de la información, robustece las disposiciones comprendidas en el art.3 “*Mercado interior*” y art.4 “*Principio de no autorización previa*” de la DCE; así como del art. 6 “*No sujeción a autorización previa*” y art.7 “*Principio de libre prestación de servicios*”, de la LSSI.

- ii) reforzar los derechos de los destinatarios de los servicios en su calidad de usuarios de dichos servicios (Capítulo IV, Sección 2);

defendió esta directiva, a la que, por simplicidad, suele hacerse referencia con su nombre. Información obtenida de: http://es.wikipedia.org/wiki/Frits_Bolkestein

³⁴⁸ Con el objetivo propuesto de crear una novedosa “*sociedad de la información para todos*”, la Comisión europea procedió en 1999 a poner en marcha la iniciativa “*eEurope*”, el cual representaba un programa destinado a difundir en la mayor medida posible las tecnologías de la información. Así se pone de manifiesto mediante Comunicación, de 8 de diciembre de 1999, relativa a una iniciativa de la Comisión para el Consejo Europeo extraordinario a efectuarse en Lisboa el 23 y 24 de marzo de 2000: “*eEurope - Una sociedad de la información para todos*” [COM (1999) 687]. Disponible en: http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=es&type_doc=COMfinal&an_doc=1999&nu_doc=687

³⁴⁹ La consolidación definitiva a la que hacemos alusión viene explicada y justificada en el Considerando 64 de la DSMI, el cual expresa: “*Con el fin de crear un auténtico mercado interior de servicios es necesario que se supriman las restricciones a la libertad de establecimiento y a la libre circulación de servicios que aún persisten en las legislaciones de algunos Estados miembros y que son incompatibles con los artículos 43 y 49, respectivamente, del Tratado. Las restricciones prohibidas en la presente Directiva afectan especialmente al mercado interior de servicios y deben desmantelarse de forma sistemática lo antes posible.*”

³⁵⁰ Resulta importante hacer notar que la DSMI incluye únicamente aquellos servicios que se realizan por una contrapartida económica, toda vez que los servicios de interés general no están cubiertos por la definición del artículo 50 del TCE, razón por la cual no se encuentran contemplados dentro su ámbito de aplicación.

³⁵¹ Y así lo hace saber el art. 1ro. de la DSMI al determinar como “Objeto” de la misma: el establecimiento de disposiciones generales “*necesarias para facilitar el ejercicio de la libertad de establecimiento de los prestadores de servicios y la libre circulación de los servicios, manteniendo, al mismo tiempo, un nivel elevado de calidad en los servicios.*”

- iii) fomentar la calidad de los servicios (Capítulo V); y
- iv) establecer una cooperación administrativa efectiva entre los Estados miembros (Capítulo VI).

Asimismo, la DSMI dedica su art. 4 para efectuar una serie de definiciones de las cuales resaltaremos las tres que más nos interesan; en ese entendido, el numeral 1) del referido artículo entiende por servicio “*cualquier actividad económica por cuenta propia, prestada normalmente a cambio de una remuneración, contemplada en el artículo 50 del Tratado*”; definición que encaja precisamente con la prestación de servicios de certificación reconocida que venimos estudiando.

Por otra parte, el numeral 2) define al prestador (del servicio) como “*cualquier persona física con la nacionalidad de un Estado miembro o cualquier persona jurídica de las contempladas en el artículo 48 del Tratado y establecida en un Estado miembro, que ofrezca o preste un servicio*”; noción que a efectos de nuestro estudio halla perfecta cabida al Prestador de Servicios de Certificación de firma electrónica.

Finalmente el numeral 3) conceptualiza como destinatario (del servicio) a “*cualquier persona física con la nacionalidad de un Estado miembro o que se beneficie de los derechos concedidos a estas por los actos comunitarios, o cualquier persona jurídica de las contempladas en el artículo 48 del Tratado y establecida en un Estado miembro, que utilice o desee utilizar un servicio con fines profesionales o de otro tipo*”; enunciado que para nuestra investigación resulta siendo continente del Firmante/Suscriptor, ya sea que se trate de un empresario individual, como cuando sea un empresario colectivo.

Como quiera que no es objeto de esta investigación efectuar un estudio detallado del contenido de la referida Directiva, nos limitaremos simplemente a indicar los artículos que poseen mayor trascendencia e incidencia respecto de los servicios de certificación de firma

electrónica. En ese entendido, consideramos como de mayor relevancia y observancia a efectos del contrato en estudio, el contenido de los siguientes artículos:

Art. 9 “Regímenes de autorización” y art. 16 “Libre prestación de servicios”.-

Por los cuales se dispone que los Estados miembros se encuentran obligados a honrar el derecho de los prestadores a suministrar servicios en un Estado miembro diverso de aquel en el que se encuentran establecidos, debiendo garantizar el Estado en que se proporciona el servicio: tanto la libertad de acceso (llamada también de establecimiento) como el libre ejercicio de la actividad de servicios dentro de su ámbito territorial.³⁵²

Art. 22 “Información sobre los prestadores y sus servicios”.-

Por la cual se obliga a que los Estados efectúen todos los esfuerzos necesarios a objeto de garantizar que los prestadores pongan a disposición del destinatario: determinada información mínima indispensable para la prestación del servicio.

Así, destaca que debe informarse - entre otras cosas - respecto de las condiciones y cláusulas generales empleadas por el prestador (art. 22.1.f.); el precio del servicio cuando se encuentre fijado previamente (art.22.i.); las principales características del servicio (art.22.1.j.). Igualmente, los Estados miembros deben hacer lo necesario para que el destinatario posea fácil acceso a dicha información mínima, a través de medios electrónicos mediante una dirección comunicada oportunamente por el prestador (art.22.2.c.). En todo caso, los Estados miembros aseguran que la mencionada información se encuentre disponible para el destinatario de forma previa a la celebración del contrato o, cuando no haya contrato por escrito, antes de la prestación efectiva del servicio (art. 22.4.)

En consecuencia, nótese que las obligaciones de información contempladas en el art.

22 comentado deben ser incorporadas a los deberes de información que recaen sobre el PSC

³⁵² El Considerando 65 de la DSMI contribuye a aclarar en qué consiste la proclamada libertad de establecimiento o de acceso, que no es otra cosa que la igualdad de trato, por la cual queda prohibido cualquier forma de discriminación cuyo fundamento resida en la nacionalidad de un Estado miembro, o cualquier otra clase de discriminación indirecta fundada en razones que lleven al mismo resultado. Por otra parte, con relación a la libre circulación de servicios, el Considerando 78 de la DSMI establece que a fin de garantizar tanto a los destinatarios como a los prestadores el hecho de poder, respectivamente, beneficiarse de servicios o prestarlos, en toda la Comunidad sin considerar los límites fronterizos, se debe esclarecer la medida en que es factible que el Estado en el que se presta el servicio pueda imponer sus propios requisitos.

previstos en la DFE (apartado k) del Anexo II), así como los señalados en el Ordenamiento español a través de la LFE (art.18.b. numerales 1 al 5) y la LSSI (arts. 9 y 10).

Art. 23 “Seguros y garantías de responsabilidad profesional”.-

Por esta disposición se establece que los Estados miembros podrán hacer lo necesario para que los prestadores cuyos servicios presenten un riesgo directo y concreto para el destinatario o un tercero, suscriban un seguro de responsabilidad profesional adecuado y en relación con la naturaleza y el alcance del riesgo, o de cualquier otra forma ofrezcan una garantía equivalente. En consecuencia nótese que se complementa lo establecido en el apartado h) del Anexo II de la DFE y el art. 20.2. de la LFE.

Art. 26 “Política de calidad de los servicios”.-

Conforme a las previsiones de este articulado, los Estados miembros - en colaboración con la Comisión - podrán adoptar acciones que tiendan a incentivar a que los prestadores aseguren de forma voluntaria la calidad de sus servicios, en particular a través de la certificación o evaluación de sus actividades por parte de organismos independientes o acreditados (art. 26.1.a.). Disposición que por otra parte integra las previsiones en cuanto a esta temática contempladas en el art. 3 de la DFE, así como los arts. 26 y 27 de la LFE.

Artículo 27 “Resolución de litigios”.-

En este apartado, la DSMI dispone que los Estados miembros deben adoptar las medidas convenientes para que los prestadores que se encuentren sometidos a un código de conducta o que formen parte de una asociación u organismo profesional, en los que se contemplen mecanismos de resolución extrajudicial de conflictos, pongan en conocimiento del destinatario respecto de esta situación, mencionándolo en los documentos en los que presenten las características sus servicios, debiendo además, señalar el modo de acceder a la información en la cual se explica: tanto las particularidades como las condiciones de empleo del referido mecanismo alternativo de resolución de controversias (art. 27.4.). Nótese que el

artículo en estudio perfecciona las disposiciones en cuanto a esta temática, previstas en el apartado k) del Anexo II de la DFE así como el art. 18.b.5. de la LFE y el art. 33.b. de la LSSI.

Artículo 37 “Códigos de conducta a escala comunitaria”.-

Finalmente esta normativa refiere que los Estados miembros - en colaboración con la Comisión - deben adoptar las acciones pertinentes a objeto de incentivar el desarrollo a escala comunitaria, de códigos de conducta que faciliten la prestación de servicios o el establecimiento de un prestador en otro Estado miembro, de conformidad con el Derecho comunitario, debiendo hacer los esfuerzos correspondientes para que dichos códigos sean accesibles a distancia y por vía electrónica. Aspecto que evidentemente contribuye a reforzar las disposiciones contenidas en los arts. 10.1.g. y 18 de la LSSI.

Cabe asimismo señalar, que el marco contractual a través del cual se presten los servicios no es objeto de la “Directiva Servicios”, toda vez que las relaciones contractuales entre el prestador de servicios y el cliente de servicios exceden de su ámbito y aplicación. Con relación a las obligaciones contractuales y extracontractuales del prestador de servicios (así como del cliente, a pesar del silencio de la norma al respecto) se hace una remisión a las normas del Derecho internacional privado.

La autora Villanueva comprende que las referidas normas, hoy por hoy, estarían integradas por:³⁵³ los “*Principios de Derecho Europeo de los Contratos*” (PELC) y los “*Principios de Derecho Europeo. Contratos de Servicios*” (PEL-SC), que integran el denominado Marco Común de Referencia (MCR) en el Derecho Europeo; los principios UNIDROIT, y por los llamados Convenio de Roma I - en el Reglamento sobre Ley aplicable a

³⁵³ (C. Villanueva, *El servicio como...*,2009: 130-131).

las obligaciones contractuales³⁵⁴ - y Convenio de Roma II - en el Reglamento relativo a la Ley aplicable a las obligaciones extracontractuales³⁵⁵ -.

2.1.3. Incidencia de la Ley 17/2009, de 23 de noviembre (LASE), en la prestación de servicios de certificación.-

De conformidad con lo establecido en el art. 44.1. DSMI, el Estado español poseía plazo hasta antes del 28 de diciembre de 2009 para efectuar la transposición correspondiente al derecho interno, mediante las normas legales, reglamentarias y administrativas que resulten necesarias.

En virtud de ello, sancionó la Ley 17/2009, de 23 de noviembre, sobre el libre acceso a las actividades de servicios y su ejercicio (LASE), la cual se complementa con el contenido de la Ley 25/2009, de 22 de diciembre, de modificación de diversas leyes para su adaptación a la LASE (más conocida como Ley Ómnibus).

La finalidad de la LASE, conforme se explicita en su art. 1, reside en *“establecer las disposiciones generales necesarias para facilitar la libertad de establecimiento de los prestadores y la libre prestación de servicios, simplificando los procedimientos y fomentando, al mismo tiempo, un nivel elevado de calidad en los servicios, así como evitar la introducción de restricciones al funcionamiento de los mercados de servicios que, de acuerdo con lo establecido en esta Ley, no resulten justificadas o proporcionadas”*.

En ese entendido, el art. 4.1. LASE dispone la libertad de establecimiento, indicando que *“Los prestadores podrán establecerse libremente en territorio español para ejercer una actividad de servicios, sin más limitaciones que las establecidas de acuerdo con lo previsto en esta Ley”*.

En tanto que el art. 5 LASE dispone la libertad de acceso a la prestación de servicios señalando que *“La normativa reguladora del acceso a una actividad de servicios o del ejercicio*

³⁵⁴ Reglamento (CE) 593/2008 del Parlamento europeo y del Consejo, de 17 de junio de 2008, sobre la Ley aplicable a las obligaciones contractuales (Roma I). DOUE, núm. L177, de 4 de julio de 2008.

³⁵⁵ Reglamento (CE) 864/2007 del Parlamento Europeo y del Consejo, de 11 de julio de 2007, relativo a la Ley aplicable a las obligaciones extracontractuales (Roma II). DOUE, núm. L199, de 31 de julio de 2007.

de la misma no podrá imponer a los prestadores un régimen de autorización, salvo excepcionalmente...”, disposición que se complementa con la contenida en el art. 12.1. LASE, la cual señala que “*Los prestadores establecidos en cualquier otro Estado miembro podrán prestar servicios en territorio español en régimen de libre prestación sin más limitaciones que las establecidas de acuerdo con lo previsto en esta Ley*”.³⁵⁶

Con relación a las obligaciones de los prestadores de servicios, el art.21 LASE indica que se podrá exigir a los prestadores de servicios, en norma con rango de ley, la suscripción de un seguro de responsabilidad civil profesional u otra garantía equivalente que cubra los daños que puedan provocar en la prestación del servicio, en aquellos casos en que los servicios que presten presenten un riesgo directo y concreto para la salud o para la seguridad del destinatario o de un tercero, o para la seguridad financiera del destinatario. En todo caso la garantía exigida deberá ser proporcionada a la naturaleza y alcance del riesgo cubierto.

Finalmente el art. 22.1. LASE impone a los prestadores de servicios la obligación de que con la debida antelación, pongan a disposición de los destinatarios una serie de informaciones de forma clara e inequívoca, antes de la celebración del contrato, o en su caso, antes de la prestación del servicio.³⁵⁷

³⁵⁶ El art. 12.3. LASE establece estos casos al disponer “*Excepcionalmente, podrá supeditarse el acceso de estos prestadores a una actividad de servicios o su ejercicio temporal en territorio español al cumplimiento de los requisitos que en cada caso determine la legislación sectorial aplicable, únicamente cuando estén justificados por razones de orden público, de seguridad pública, de salud pública o de protección del medio ambiente; y sean, de conformidad con el artículo 5 de esta Ley, proporcionados y no discriminatorios y de forma suficientemente motivada...*”.

³⁵⁷ La información que debe proporcionar el prestador es la siguiente:

Art. 22.2.- Los prestadores proporcionarán al destinatario, de forma fácilmente accesible, la información siguiente: a) Los datos de identidad, forma y régimen jurídico, número de identificación fiscal del prestador, dirección donde tiene su establecimiento, y los datos que permitan ponerse rápidamente en contacto con él y en su caso, por vía electrónica. b) Datos registrales del prestador del servicio. c) Los datos de la autoridad que, en su caso, haya otorgado la autorización. d) En las profesiones reguladas, la cualificación profesional y el Estado miembro en el que fue otorgada, así como, en su caso, el colegio profesional, la asociación profesional u organismo análogo en el que esté inscrito el prestador. e) Las condiciones y cláusulas generales, y las relativas a la legislación y jurisdicción aplicable al contrato. f) Garantías posventa adicionales a las exigidas por ley, en su caso. g) El precio completo del servicio, incluidos los impuestos, cuando el prestador fije previamente un precio para un determinado tipo de servicio. h) Las principales características del servicio o servicios que ofrezca. i) En su caso, el seguro o garantías exigidas, y en particular, los datos del asegurador y de la cobertura geográfica del seguro. j) En caso de que el prestador ejerza una actividad sujeta al IVA, el número de identificación fiscal. k) Lengua o lenguas en las que podrá formalizarse el contrato, cuando ésta no sea la lengua en la que se le ha ofrecido la información previa a la contratación. l) Existencia del derecho de desistimiento del contrato que pueda corresponder al consumidor, el plazo y la forma de ejercerlo.

Art. 22.3.- A petición del destinatario, los prestadores pondrán a disposición de aquél la siguiente información complementaria: a) Cuando el precio no lo fije previamente el prestador, el precio del servicio o, si no se puede indicar aquél, el método para calcularlo; o un presupuesto suficientemente detallado. b) Fecha de entrega, ejecución del contrato y duración. c) En el caso de las profesiones reguladas: referencia a las normas de acceso a la profesión en el Estado miembro de establecimiento y los medios para acceder a dichas normas. d) La información relativa a sus actividades multidisciplinares, posibles conflictos de interés y las medidas adoptadas para evitarlos. Esta información deberá figurar en todo documento informativo de los prestadores en el que se presenten de forma detallada sus servicios. e) Los posibles códigos de conducta a que, en su caso, esté sometido el prestador, así como la dirección en que dichos códigos se pueden consultar por vía electrónica y en qué idiomas están disponibles. f) Información detallada sobre las características y condiciones para hacer uso de los

De todo lo expuesto, resulta evidente que las disposiciones de la “*Directiva Servicios o Bolkestein*” y las provenientes de la LASE poseen una directa incidencia en los servicios de certificación de firma electrónica que venimos estudiando, por lo que sus normas deberán ser de observancia por parte de los PSC.

2.2. Las Entidades de Registro (ER).-

El PSC con carácter previo a la emisión de un certificado reconocido, debe proceder a cumplir una serie de obligaciones (art. 12 LFE), constituyendo sin duda alguna una de sus obligaciones más importantes la de comprobar la identidad y circunstancias personales de los solicitantes de certificados (art.12.a. LFE), con arreglo a lo dispuesto en el art. 13 LFE.

Para satisfacer dichas obligaciones, se requiere necesaria e imprescindiblemente la presencia personal de los Firmante/Suscriptores de certificados, salvo las excepciones previstas en el art. 13.4. incs. a) y b) LFE.³⁵⁸ En consecuencia, cuando el PSC despliega sus servicios en un ámbito geográfico amplio y disperso resulta complicado que pueda satisfacer estas actividades por sí solo, por ello es que actúa a través de las denominadas Entidades de Registro (ER), que son intermediarios distribuidos territorialmente que proporcionan el contacto directo con el solicitante o titular del certificado.

Las ER pueden formar parte estructural e integrante de la empresa certificadora y operan como unidades desconcentradas pero dependientes de la misma (a modo de agencias o sucursales), o pueden ser entidades completamente ajenas e independientes a la empresa certificadora con las que el PSC ha suscrito un contrato o convenio correspondiente, haciendo

medios extrajudiciales de resolución de conflictos cuando estén sujetos a un código de conducta o sean miembros de alguna organización profesional en los que se prevean estos mecanismos.

Art. 22.4.- Toda la información a que se refieren los apartados anteriores se pondrá a disposición del destinatario por el prestador, en alguna de las formas siguientes: a) En el lugar de prestación del servicio o de celebración del contrato. b) Por vía electrónica a través de una dirección facilitada por el prestador. c) Figurando dicha información en todo documento informativo del prestador que se facilite al destinatario y en el que se presenten de forma detallada sus servicios. d) Por vía electrónica a través de una página web.

³⁵⁸ Las excepciones contempladas en el art. 13.4. LFE son: a) Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya al prestador de servicios de certificación 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 al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años.

notar no obstante que en cualquiera de los casos la ER delegada actúa por cuenta y en nombre del PSC, es decir, en representación de aquél.

Dichos intermediarios son las Entidades de Registro (ER), que se encuentran reconocidas implícitamente en el art. 13.5. LFE, el cual señala que los PSC *“podrán realizar las actuaciones de comprobación previstas en este artículo por sí o por medio de otras personas físicas o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación”*.

Las ER son instituciones auxiliares del certificador que fundamentalmente proporcionan un servicio local al conjunto de Firmante/Suscriptores del PSC. Entre ellos podemos mencionar los siguientes:

- a) Proceden al registro de los solicitantes de certificados, efectuando la captación y llenado de los datos, así como ejecutan el registro de la baja y cambio de atributos de los Firmante/Suscriptores.
- b) Su labor más importante consiste en la plena identificación y autenticación de Firmante/Suscriptores, dado que en este trascendental paso recae la seguridad y confianza de todo el sistema.
- c) Las ER efectúan la autorización de solicitudes de emisión de certificados y, en su caso, de generación de claves y recuperación de claves almacenadas.
- d) Efectúan la aceptación y autorización de las peticiones de suspensión y/o revocación de certificados, pero tomando en cuenta que técnicamente no es la ER quien revoca o suspende certificados, sino que es el PSC quien adopta en última instancia dichas determinaciones, por lo que recae sobre él toda la responsabilidad por la administración del sistema tecnológico y, por ende, de los certificados.

Las ER son por consiguiente entidades de plena confianza de un PSC, respecto de quienes éste último posee una potestad administrativa o ha suscrito previamente como se tiene dicho, un acuerdo o contrato que regula la relación entre ellos, estableciendo claramente los deberes, obligaciones y responsabilidades de la ER frente al PSC. La función fundamental de la ER consiste en atender la solicitud de certificados por parte del Firmante/Suscriptor, aprobar peticiones de certificados, o ayudar al PSC según corresponda en la suspensión, revocación y/o extinción de certificados.

Por consecuencia, debe quedar absolutamente claro que las ER no adoptan las decisiones esenciales de emisión, suspensión, revocación y/o extinción de un certificado, las cuales únicamente están reservadas al PSC. Pero es evidente (dado que la comprobación de la identidad y demás información de un solicitante de certificado es crucial para la fiabilidad del certificado emitido) que dichos intermediarios desempeñan un rol imprescindible a objeto de generar los niveles óptimos y deseados de seguridad, propios de un sistema de certificados de clave pública.

En ese sentido y por los motivos expuestos, resulta vital que la relación entre la ER y el PSC se encuentre articulada de manera absolutamente clara y delimitada, particularmente con relación a la responsabilidad del PSC frente al Firmante/Suscriptor, los Usuarios que confían y eventualmente terceros por las actuaciones de la ER.

2.3. El Firmante/Suscriptor y titular del certificado reconocido.-

El Firmante/Suscriptor es la contraparte contractual del PSC en el contrato de certificación reconocida. Denominado también como titular o sujeto del certificado reconocido, es la persona que detenta la titularidad de la clave privada (datos de creación de firma) que se corresponde con la clave pública (datos de verificación de firma) contenida en el certificado reconocido, mismo que es emitido por el PSC.

Asimismo como se tiene dicho, el Firmante/Suscriptor puede ser una persona física o jurídica, de derecho público o privado, lo que nos plantea al igual que en el caso anterior un gran abanico de posibilidades respecto de su condición, mismas que procuraremos reflejar en el Cuadro (B) de la página siguiente.

Para el caso que venimos estudiando donde hemos partido del supuesto que las partes contratantes son empresarios, diremos que el Firmante/Suscriptor es el empresario de naturaleza física o jurídica (es decir individual o colectivo) a favor de quien el PSC emite el certificado reconocido en virtud de la relación contractual que existe entre ambos.

Cuando se trata de un empresario individual, éste puede solicitar el certificado reconocido de manera directa o también puede efectuar la solicitud por medio de un representante que se encuentre suficientemente autorizado, para lo cual deberá probar sus poderes para solicitar y aceptar el certificado.

En tanto que tratándose de empresarios colectivos, la solicitud necesariamente debe efectuarse a través de un representante que se encuentre debidamente acreditado al efecto, demostrando el poder suficiente que emana de la persona jurídica a la cual representa a objeto de solicitar y aceptar el certificado.

Cuando el Firmante/Suscriptor es una persona jurídica, una de las cuestiones que se plantea es si las firmas digitales se pueden utilizar para vincular a personas jurídicas y, si ello es posible, bajo qué condiciones. En ese entendido debemos señalar que existen varios modelos teóricamente posibles de vinculación electrónica de una persona jurídica, de los cuales reflejaremos los dos más frecuentes:³⁵⁹

- a) Persona física como titular del certificado vinculante para la persona jurídica.- De conformidad con este modelo, el titular del certificado es una persona física con poder de representación de la persona jurídica (v.gr el administrador de la empresa).

³⁵⁹ (A. Martínez, 2001: 165-170).

Cuadro "B"
Personas que pueden revestir hipotéticamente la condición de Firmante/Suscriptor

Certificado	SUBSCRIPTOR	Contexto	Derecho Privado		Derecho Público
			Ámbito Civil	Ámbito Comercial	
Es titular de un Certificado electrónico (simple) o Es titular de un Certificado Reconocido	Persona Natural	En todos los casos el Firmante Suscriptor está sometido a condiciones generales, por lo que son aplicables las normas de la Ley 7/1998 sobre Condiciones Generales de la Contratación.	Particular	Empresario mercantil individual	
	Persona Jurídica	Cuando el Firmante Suscriptor reviste la condición de consumidor o usuario, resultan de aplicación además las normas de la Ley 26/1984 General para la Defensa de los Consumidores y Usuarios.	Asociaciones Fundaciones Sociedades civiles	<p>Empresario mercantil colectivo</p> <p>Sociedades personalistas:</p> <ul style="list-style-type: none"> - Colectivas - Comanditarias <p>Sociedades de capital:</p> <ul style="list-style-type: none"> - Anónimas - Comanditaria por acciones - Limitadas <p>Personas jurídicas en formación e irregulares</p> <p>Si la sociedad en formación es de capital y tras haberse otorgado la escritura de constitución social no se inscribe en el RM, se considera irregular, sujetándose a las reglas de:</p> <ul style="list-style-type: none"> - La sociedad colectiva, si persigue la realización de actos de comercio - La sociedad civil, si no persigue la realización de actos de comercio (art.16 LSA) 	<p>Entidades de la Administración en general que están autorizadas para relacionarse electrónicamente mediante certificados provenientes:</p> <ul style="list-style-type: none"> - De una persona de derecho público - De una persona de derecho privado

En este caso la firma digital de la persona física que efectúa negocios electrónicos en nombre de la sociedad, resulta vinculante para la persona jurídica conforme a las normas particulares de representación de sociedades y conforme expresa la Exposición de Motivos de la LFE “...*ésta debe estar amparada en un documento público que acredite fehacientemente dicha relación de representación así como la suficiencia e idoneidad de los poderes conferidos al representante.*”

El poder de representación podría hacerse constar en el certificado, situación que nos coloca ante un certificado de atributos, razón por la que se deben adoptar medidas para asegurar el mantenimiento de las facultades de representación durante toda la vigencia del certificado reconocido.³⁶⁰

- b) Persona jurídica como titular del certificado.- De acuerdo con este modelo se emite un certificado a nombre de la persona jurídica, pero debido a que se requiere finalmente que una persona física efectuó materialmente la firma en forma digital, es necesario hacer constar en el certificado el poder que la autorizada a firmar digitalmente en nombre de la sociedad titular del certificado, quien formalmente es la poseedora de la correspondiente clave privada.

Resumiendo, en el primer caso el titular de un certificado es una persona física con poder de representación legal de una persona jurídica; mientras que para el segundo modelo, en el certificado aparece como titular una persona jurídica junto con la persona física autorizada para digitar materialmente la firma de la persona jurídica.

Al respecto es pertinente efectuar algunas precisiones terminológicas a objeto de evitar confusión. El art. 6.2. LFE introduce el concepto de firmante, definiéndolo como “*la persona que posee un dispositivo de creación de firma y que actúa en nombre propio o en*

³⁶⁰ Martínez explica que cuando el atributo (el poder de representación) consta en el certificado, posee el inconveniente práctico de que la sociedad tendrá que revocar el certificado cada vez que cese una persona en el cargo de administrador, y tendrá que solicitar la emisión de un nuevo certificado. Asimismo, plantea el problema de la responsabilidad del PSC respecto de la inclusión de tal elemento, la eventual revocación de tal poder, y las posibles divergencias entre el contenido del certificado y el Registro Mercantil respecto de la existencia, subsistencia y extensión del mismo. Apol-Lònia Martínez Nadal, “Problemática jurídica de los certificados de atributos en el comercio electrónico. En especial, su discordancia con el registro mercantil. Propuestas de solución”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003; pp. 659-709.

nombre de una persona física o jurídica a la que representa”.³⁶¹ De conformidad con este concepto, salta la duda respecto a cuál de los modelos expuestos precedentemente ha seguido la ley española y, en definitiva, si la noción de Firmante/Suscriptor que hemos venido manejando en esta investigación, coincide o no, con la definición de “*firmante*” contenida en la LFE.

En un primer momento, pareciera que la noción de firmante (de la LFE) y Firmante/Suscriptor que venimos empleando no coinciden. Recuérdese que la definición que manejamos de Firmante/Suscriptor hace alusión a una persona física o jurídica; en tanto que la noción que maneja la LFE del firmante parece traer aparejada la necesaria condición de persona física de éste, sobre todo cuando establece que el firmante es quien *posee un dispositivo de creación de firma*. Lógicamente que resulta difícil imaginarse cómo una persona jurídica dada su inmaterialidad y su condición, en definitiva de ficción jurídica, pueda *poseer* dicho dispositivo.

De esta manera, aparentemente el legislador español parece inclinarse por el modelo de la vinculación de personas jurídicas a través de la firma de personas físicas con poder de representación suficiente, especialmente si comprendemos la exigencia de posesión como tenencia física, material e inmediata.

No obstante, si reparamos en la redacción del art. 6.2. LFE, el mismo se refiere al firmante simplemente como “*persona*” de modo genérico y sin especificar que sea física o jurídica, dando a entender por consiguiente, que el legislador español concibe al firmante como persona física o jurídica y que la posesión del dispositivo de creación de firma debe ser

³⁶¹ La DFE define su art. 2.3.: “*firmante*”: *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 persona física o jurídica a la que representa*. En tanto que la LMFE señala en su art. 2.d): *Por “firmante” se entenderá 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*.

comprendida como una detentación formal y mediata.³⁶² Con lo cual, nos encontramos ante el segundo modelo de vinculación electrónica de una persona jurídica; a idéntica conclusión llegamos, si efectuamos una lectura e interpretación integral de la LFE, particularmente del art. 3 numerales 1, 2 y 3.

Por lo que, ante las dudas planteadas, podemos concluir señalando que la noción de Firmante/Suscriptor que utilizamos en esta investigación resulta finalmente coincidente a la definición de firmante contenida en el art. 6.2. LFE. Asimismo, se concluye que en la legislación española subsisten y conviven los dos modelos expuestos de vinculación electrónica de una persona jurídica, lo que indudablemente acarrea una doble ventaja.³⁶³

Establecida la posibilidad que la persona jurídica revista la categoría de firmante, por consiguiente de Firmante/Suscriptor de un certificado reconocido según la terminología por nosotros empleada y, en general, la utilizada en el tráfico por las empresas de certificación, cabe analizar el contenido del art. 7 de la LFE que se refiere precisamente a los certificados electrónicos de personas jurídicas.³⁶⁴

De conformidad con el contenido del artículo enunciado, los administradores, representantes legales y voluntarios con poder bastante se encuentran facultados para solicitar certificados electrónicos de personas jurídicas (art.7.1. LFE),³⁶⁵ siendo responsabilidad de la persona física solicitante la salvaguarda de los datos de creación de firma asociados al certificado, cuyo titular es la persona jurídica a la que representan, es decir, el Firmante/Suscriptor. Por esta razón la norma dispone que la identificación del solicitante deba ser incluida en el certificado electrónico (art.7.2. LFE).

³⁶² Martínez recuerda que en el comercio tradicional una persona jurídica puede actuar en nombre y representación de una persona jurídica, haciendo notar, que esta misma situación, sin embargo, en el ámbito del comercio electrónico puede suponer una cierta complejidad práctica (A. Martínez, 2004: 120). Y ello es evidente, pero no obstante el grado de dificultad práctica que conlleva, es en todo caso una posibilidad que el legislador español considera posible.

³⁶³ La Exposición de Motivos de la LFE contribuye a aclarar definitivamente el tema cuando expresa que “...los certificados electrónicos de personas jurídicas no alteran la legislación civil y mercantil en cuanto a la figura del representante orgánico o voluntario y no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación.”

³⁶⁴ Prácticamente la mayor parte de los PSC comerciales, tanto en sus contratos como en las Declaraciones de Prácticas y Políticas de Certificación, emplean el término Firmante/Suscriptor para referirse a su contraparte contractual

³⁶⁵ En estos casos, el art. 7.1. de la LFE establece que los certificados electrónicos de personas jurídicas no pueden afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

En estos casos el Firmante/Suscriptor se encuentra autorizado para establecer límites adicionales, por razón de la cuantía o de la materia para el uso de su firma electrónica, los cuales deben constar necesariamente el certificado electrónico; uso que por otra parte, puede dar lugar a la contratación de bienes y/o servicios que sean propios o concernientes al giro de su negocio o tráfico ordinario (art. 7.3. LFE).

Finalmente, la LFE dispone que los actos o contratos en los que la firma del Firmante/Suscriptor ha sido utilizada conforme a los límites anteriormente señalados, se entienden hechos por el propio Firmante/Suscriptor; pero si el empleo de la firma transgrede dichos límites, el Firmante/Suscriptor únicamente queda reatado frente a terceras personas en caso de asumirlos como propios o cuando hubieren sido celebrados en su provecho. Por el contrario, cuando el Firmante/Suscriptor no los asuma como propios o cuando se emplea la firma electrónica en su perjuicio, las consecuencias de dichos actos debe asumirlos la persona física responsable de la custodia de los datos de creación de firma (el solicitante del certificado), quien se encuentra en todo caso facultado, para repetir contra quien los hubiera utilizado (art. 7.4. LFE).³⁶⁶

2.4. El Usuario del certificado reconocido.-

En primer lugar se debe dejar establecido, que el Usuario del certificado reconocido es un tercero respecto de la relación contractual existente entre el PSC y el Firmante/Suscriptor. Denominado también como usuario de clave pública, verificador o parte que confía en el certificado, es la persona (física o jurídica, de derecho público o privado, empresario o consumidor) que mantiene una relación contractual con el Firmante/Suscriptor,

³⁶⁶ Muchas de las dudas respecto de los alcances y usos que se pueden dar a los certificados de personas jurídicas, son claramente dilucidados en la Exposición de Motivos de la LFE, razón por la cual y dada su importancia aclarativa nos permitimos transcribir en sus partes sobresalientes: “...Por último, de cara a terceros, limita el uso de estos certificados a los actos que integren la relación entre la persona jurídica... y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad...de modo paralelo a cómo nuestro más que centenario Código de Comercio regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento. Con la expresión «giro o tráfico ordinario» de una entidad se actualiza a un vocabulario más acorde con nuestros días lo que en la legislación mercantil española se denomina «establecimiento fabril o mercantil». Con ello se comprenden las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de actividad de la entidad y las actividades de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares.”

en el ámbito del comercio electrónico en sentido estricto, en virtud de la relación subyacente al intercambio electrónico.

A objeto de validar la firma electrónica del Firmante/Suscriptor (más concretamente los datos de creación de firma, que en un sistema de cifrado asimétrico están materializados en la clave privada) con que aquél ha firmado los documentos electrónicos que hacen a su relación comercial, accede a la clave pública del Firmante/Suscriptor por medio de una copia del certificado reconocido, la cual debe ser colocada a su disposición por el PSC por medios electrónicos y telemáticos, normalmente a través de la LRC (*Lista de Revocación de Certificados*) o el servicio OCSP (*Protocolo de Estado de Certificado en línea*) del PSC.

De esa manera el Usuario se encuentra en posibilidad de actuar basándose en la confianza que emana de ese certificado y la clave pública que contiene, la cual vincula al Firmante/Suscriptor de modo exclusivo permitiendo la correspondiente comprobación de identidad (autenticación).

La LFE se refiere al Usuario muy vagamente, concretamente en el art. 23.4. denominándolo “*destinatario de los documentos firmados electrónicamente*”, en tanto que la DFE omite cualquier referencia a éste. La LMFE se ocupa de él en su art. 2.f) designándolo como *parte que confía*, entendiéndose que es la persona “*que pueda actuar sobre la base de un certificado o de una firma electrónica*”.

El Usuario del certificado reconocido se encuentra indeterminado al momento que entre el PSC y el Firmante/Suscriptor se suscribe el contrato de certificación reconocida, éste únicamente se individualiza, el instante que acude al PSC a objeto de solicitar una copia del certificado reconocido a fin de efectuar la autenticación y verificación de la firma del Firmante/Suscriptor.

Conforme se ha sostenido el Usuario del certificado es la parte contractual del Firmante/Suscriptor, revistiendo calidad de tercero en la relación contractual entre el PSC y

el Firmante/Suscriptor, por lo que - en principio - no parece tener de forma general ningún vínculo contractual con el PSC; no obstante, desde el momento en que el Usuario del certificado accede al servicio de consulta sobre la vigencia de los certificados publicado por el PSC, a objeto de verificar el contenido y estado del mismo (vigente, suspendido o extinguido), se ve forzado a cumplir una serie de obligaciones, por lo que cabría pensar que se configura el surgimiento de otra relación también contractual y directa con el PSC, aspecto que será objeto de análisis a momento de tocar la temática del contenido contractual.

Lo que si resulta evidente, es que - ora *ex lege*, ora vía contractual - se otorga al Usuario del certificado una auténtica facultad, consistente en la potestad que éste posee para dirigirse al PSC y acceder a una copia del certificado reconocido.

Por consecuencia nótese que requieren del PSC para su seguridad, ya que la verificación de la firma del mensaje electrónico que han recibido del Firmante/Suscriptor, la efectuarán fundándose y confiando en el certificado reconocido emitido por el PSC. Por esta razón es que uno de los asuntos vitales del sistema de certificados consiste en determinar la responsabilidad que puede derivar del PSC frente a los Usuarios que confían en un certificado emitido por aquél.

III. La capacidad de las partes.-

Con la tarea previamente acometida de identificar a las partes contractuales del contrato de certificación reconocida, resulta necesario conocer la capacidad que éstas deben poseer para celebrar válidamente el contrato. Para ello, efectuaremos inicialmente una breve exposición con relación a la regulación de la capacidad de obrar en el ordenamiento jurídico español.

3.1. La capacidad general de obrar.-

En primer lugar se debe distinguir la capacidad jurídica de la capacidad de obrar. La primera hace referencia a la aptitud o idoneidad de la persona para ser titular de derechos y

obligaciones; en el caso de las personas físicas ésta se adquiere desde el nacimiento, aspecto que determina el inicio de la personalidad según dispone el art. 29 C.c.³⁶⁷. En el caso de personas jurídicas su personalidad empieza desde el instante mismo en que, con arreglo a derecho, hubiesen quedado válidamente constituidas (corporaciones, asociaciones y fundaciones de interés público) y a las que la ley conceda personalidad propia (asociaciones de interés particular, sean civiles, mercantiles o industriales), conforme señala el art. 35 C.c..

Por otra parte, la capacidad de obrar es la aptitud reconocida por el ordenamiento jurídico para actuar con eficacia en el mundo del Derecho, misma que se concreta en la posibilidad de llevar a cabo una serie de actos jurídicos. En el ordenamiento español, la capacidad de obrar plena se adquiere con la mayoría de edad (art. 322 C.c.), misma que se alcanza a los 18 años (art. 315 C.c. y art. 12 CE).

En principio y en términos generales ambos empresarios -Firmante/Suscriptor y PSC- deben tener capacidad general para contratar. No obstante, a objeto de reconocer de una mejor manera los específicos requisitos y circunstancias que deben concurrir para considerar su capacidad y legitimación, resulta más adecuado proceder al estudio por separado de la capacidad que cada una de las partes debe revestir a objeto de participar en este negocio jurídico.

3.2. Capacidad del Prestador de Servicios de Certificación (PSC).-

a) Cuando es empresario mercantil individual.-

Para calificar al PSC como empresario mercantil individual deberá cumplir los requisitos exigidos en el art. 1.2. C.com., estos son, tener capacidad legal y ejercer el comercio en nombre propio y de forma habitual (art.1.1. C.com.). En este caso es de aplicación la regla general de capacidad, por cuya virtud, para celebrar contrato de certificación es preciso tener capacidad de obrar plena (art. 1.263 C.c.). Por tanto ser mayor

³⁶⁷ La personalidad es la cualidad inherente a la persona como tal: es la condición de persona; es una situación jurídica subjetiva, una cualidad reconocida por el Derecho al ser humano (persona física) y a ciertas organizaciones humanas (personas jurídicas). El concepto de personalidad es coincidente con el de capacidad jurídica, que es la aptitud legal para ser titular de derechos subjetivos y de deberes jurídicos (X. O'Callaghan, 2001: 82).

de 18 años y no sufrir ninguna restricción en ella por efecto de resolución judicial, debiendo tener capacidad legal para ejercer habitualmente el comercio, y sólo se les reconoce a los mayores de edad que tengan la libre disposición de sus bienes, es decir, que no estén incapacitados ni quebrados o concursados no rehabilitados (art. 4 C.com.).

Como se tiene dicho, la capacidad del comerciante individual para prestar el servicio de certificación se rige por las reglas generales: mayoría de edad y libre disposición de sus bienes (art. 4 C.com.). Si el comerciante es una persona casada deberá contar con el consentimiento expreso o presunto de su cónyuge para ejercer el comercio (arts. 6 a 8 C.com.), mientras que para vincular la responsabilidad tanto del patrimonio ganancial como del patrimonio privativo del otro cónyuge es preciso su consentimiento expreso (arts. 1.367, 1.322 y 1.440 C.c. y art. 9 C.com.).

b) Cuando es empresario mercantil colectivo.-

Si el PSC es empresario mercantil colectivo, en estos casos constituye una persona jurídica la que tiene la condición de comerciante y actuará como certificador. La certificadora es aquella empresa que tiene por actividad típica y habitual la prestación de servicios de certificación de firma electrónica, de manera que se dedica profesionalmente a esta actividad, por lo que en la escritura pública de constitución se hará constar en su objeto social como actividad societaria propia.

Actúa por medio de sus administradores que son los representantes orgánicos de las sociedades mercantiles. Al ser sociedades mercantiles revisten alguna de las siguientes formas de personificación jurídica: sociedades personalistas (Colectivas y Comanditarias) y las de capital (Anónimas, Comanditaria por acciones y Limitadas).

La personalidad jurídica les es atribuida no únicamente como consecuencia del cumplimiento de los requisitos generales para la constitución de sociedades mercantiles, entre los que figura la obligatoria inscripción en el Registro Mercantil (art. 16 C.com., art. 81 y

ss.RRM) sino que, para que esta persona exista deberán concurrir los requisitos específicos de forma y publicidad previstos por las leyes, distinguiéndose entre los exigidos para las sociedades personalistas (colectivas, art. 125 y ss. C.com. y art. 209 RRM;³⁶⁸ y comanditarias, art. 145 y ss. C.com. y art. 212 RRM) y las de capital (con carácter gral.: art. 94 ss. RRM; Anónimas, art. 19 y ss. RDL 1/2010³⁶⁹ y 114 RRM; Comanditaria por acciones art. 19 y ss. RDL 1/2010; Limitadas art. 19 y ss. RDL 1/2010, art. 175 RRM).

Consideraciones finales:

Podemos concluir señalando que el PSC será en la mayoría de los casos un empresario que lleve a cabo esta actividad con el ánimo de lucro, ya sea en calidad de empresario individual, bien a través de una sociedad. En el primer caso, el PSC poseerá plena capacidad de obrar pues, como se ha visto, ésta se requiere para ejercer el comercio. En tanto que si la actividad se realiza a través de una sociedad mercantil será ésta la que, una vez constituida válidamente, tenga personalidad jurídica y capacidad de obrar para actuar en el mercado y celebrar los contratos propios de su actividad.

La realidad del tráfico demuestra no obstante, prácticamente la inexistencia de empresarios mercantiles individuales en calidad de certificadores, predominando en consecuencia los PSC constituidos como sociedades mercantiles bajo la modalidad de Sociedad Anónima. Comprendemos que esto es así, debido fundamentalmente a que este tipo de negocio requiere de fuertes inversiones de capital, tanto para montar la infraestructura tecnológica de clave pública sobre la que descansa la administración de un sistema de certificados reconocidos, como para asumir los potenciales riesgos propios y derivados de la actividad de certificación, ya sea frente al Firmante/Suscriptor como frente a terceras partes, entre ellos los Usuarios que confían en el certificado.

³⁶⁸ Reglamento del Registro Mercantil, aprobado por Real Decreto 1784/1996, de 19 de julio.

³⁶⁹ Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el Texto Refundido de la Ley de Sociedades de Capital.

Por otra parte hay que hacer notar que en todos los casos el PSC se encuentran en la obligación legal: i) de informar y colaborar con el Ministerio de Ciencia y Tecnología (art. 30 LFE) y ii) de observar las normas contenidas en la Ley 34/2000 sobre Servicios de la Sociedad de la Información, en todo lo que les fuere aplicable (art. 1 y ss. LSSI).

3.3. Capacidad del Firmante/Suscriptor.-

a) Cuando es empresario mercantil individual.-

Si el Firmante/Suscriptor es empresario mercantil individual es preciso tener capacidad de obrar plena, debiendo tener capacidad legal y ejercer el comercio en nombre propio y de forma habitual, siendo de aplicación lo indicado en el apartado 3.2. a).

b) Cuando es empresario mercantil colectivo.-

La capacidad del empresario mercantil colectivo para ser Firmante/Suscriptor, depende del cumplimiento de los requisitos legales para la atribución de personalidad jurídica y de las facultades atribuidas a quien actúe en su representación, conforme se tiene indicado en el apartado 3.2. b).

Observaciones finales:

Resulta pertinente señalar asimismo que en todos los casos: i) el contrato está sujeto a condiciones generales, por lo que le resultan aplicables las normas de la Ley 7/1998, sobre Condiciones Generales de la Contratación; ii) el tratamiento de los datos personales del Firmante/Suscriptor que precisen los PSC se sujetará a lo dispuesto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal (art. 17 LFE).

IV. Elementos objetivos.-

4.1. El certificado reconocido.-

La LMFE comprende por “certificado” a todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma (art. 2.b. LMFE).

A su turno, la DFE concibe el certificado como *“la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta”* (art. 2.9. DFE). Más adelante añade la definición de certificado reconocido, en sentido de constituir *“el certificado que cumple los requisitos establecidos en el anexo I y es suministrado por un proveedor de servicios de certificación que cumple los requisitos establecidos en el anexo II”* (art. 2.10. DFE).

Como se tiene adelantado, la LFE establece que un certificado electrónico es aquel documento que vincula unos datos de verificación de firma a un firmante (el Firmante/Suscriptor) y confirma su identidad, debiendo encontrarse necesariamente firmado por medios electrónicos por un PSC (art. 6.1. LFE).

Los certificados reconocidos para ser considerados como tales, deben previamente cumplir una serie de requisitos adicionales de los que se exigen para la emisión de un certificado electrónico simple u ordinario³⁷⁰ (en este último caso contenidos en los arts. 17, 18 y 19 LFE), dichas exigencias consisten entre otras cosas: en ser expedidos por un PSC que cumpla los requisitos establecidos en la LFE en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes, como en cuanto a la fiabilidad y las garantías de los servicios de certificación que presten (art.11.1. LFE). Los mencionados requisitos adicionales se hallan normados fundamentalmente en los arts. 11, 12, 13 y 20 LFE, de los que nos ocuparemos con detalle más adelante. Sobre el contenido del art.11 LFE, ver cuadro “C” de la página siguiente.

El certificado reconocido opera en el contexto de la criptografía asimétrica, por lo que técnicamente es un certificado de clave pública (o certificado digital), en el que la clave

³⁷⁰ La notoria ventaja de los certificados reconocidos - debido a que las firmas que avalan cuentan con la presunción de validez otorgada por el art. 3.4. LFE - lleva a J.F. Ortega a preguntarse el sentido y utilidad que devienen de los certificados no reconocidos, pues *“...no gozando de esta presunción. ¿a quién le interesa aunque su precio de emisión sea inferior, poseer un certificado de estas características? ¿Qué cuota de mercado ocuparán estos certificados? La respuesta es el amplio margen de mercado que queda en los grupos cerrados.... Así, una entidad bancaria puede constituirse en prestador de servicios de certificación y emitir a cada uno de sus empleados y clientes un certificado no reconocido. Al recibir estos certificados, los titulares de los mismos reconocen contractualmente los efectos jurídicos de las firmas electrónicas basadas en los certificados no reconocidos emitidos por dicho prestador (el banco)...”* (J.F. Ortega, 2004: 406).

pública del Firmante/Suscriptor se asocia de manera segura a su clave privada. Se encuentra firmado digitalmente por el PSC, que ha confirmado previamente la identidad (u otros atributos, como poderes de representación en el caso de certificados de personas jurídicas) del Firmante/Suscriptor, por ello se denominan también “*certificados identificativos*”, por cuanto vinculan un nombre a una clave pública.³⁷¹

Cuadro “C”
Requisitos para la existencia de un certificado reconocido

Art. 11 de la Ley 59/2003 y Anexo I de la Directiva de firma electrónica
<p>Los certificados reconocidos incluirán, al menos, los siguientes datos: (art. 11.2. LFE)</p> <ul style="list-style-type: none"> - Indicación de que se expiden como tales. - El código identificativo único del certificado. - La identificación del PSC que expide el certificado y su domicilio. - La firma electrónica avanzada del PSC que expide el certificado. - La identificación del firmante: <ul style="list-style-type: none"> • Personas físicas: por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca. • Personas jurídicas: por su denominación razón social y su código de identificación fiscal. - Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante. - El comienzo y el fin del período de validez del certificado. - Los límites de uso del certificado - Los límites del valor de las transacciones para las que puede utilizarse el certificado. - Cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite. (art. 11.3. LFE) - Si admiten una relación de representación: una indicación del documento público que acredite de forma fehaciente: (art. 11.4. LFE) <ul style="list-style-type: none"> • 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.

³⁷¹ (A. Martínez, 2001: 145-147).

Por otra parte, el contenido de un certificado reconocido según la Recomendación X.509 v.3 de Unión Internacional de Telecomunicaciones (UIT), es la siguiente:³⁷²

- a) - DN - Contracción de los vocablos ingleses “*Distinguished Name*” cuyo significado en español es “Nombre Distintivo”. Constituye la identificación univoca de una entrada dentro de la estructura de directorio X.500. El DN está compuesto por el nombre común (CN) de la entrada más una serie de atributos que identifican la ruta seguida dentro de la estructura del directorio X.500 para llegar a dicha entrada.
- b) - CN - Contracción de los vocablos ingleses “*Common Name*” cuyo significado en español es “Nombre Común”. Es un atributo que forma parte del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500 utilizado para nombrar la entrada correspondiente al objeto.
- c) - OU - Contracción de los vocablos ingleses “*Organizational Unit*” cuyo significado en español es “Unidad Organizativa”. Es un atributo que forma parte del Nombre Distintivo de un objeto dentro de la estructura de directorio X.500.
- d) - O - Es una abreviatura del vocablo inglés “*Organization*” cuyo significado en español es “Organización”. Es un atributo que forma parte del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500 utilizado para nombrar la entrada correspondiente al objeto.
- e) - C - Es una abreviatura del vocablo inglés “*Country*” cuyo significado en español es “País”. Es un atributo que forma parte del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500 utilizado para nombrar la entrada

³⁷² - X.500: Estándar desarrollado por la UIT que define las recomendaciones del Directorio. Se corresponde con el estándar ISO/IEC 9594-1: 1993. Da lugar a la serie de recomendaciones siguientes: X.501, X.509, X.511, X.518, X.519, X.520, X.521 y X.525.

- X.509: La Recomendación - Norma Internacional x.509 de la UIT junto con otras Recomendaciones - Normas Internacionales (v.gr. ISO/CEI 9594-8), ha sido elaborada para facilitar la interconexión de los sistemas de procesamiento de información con el fin de proporcionar servicios de directorio. Trata algunos de los requisitos de seguridad en los ámbitos de autenticación, y otros servicios de seguridad mediante la introducción de un conjunto de marcos sobre los que se pueden basar servicios completos. De forma específica, define marcos para las Infraestructuras de Clave Pública: i) certificados de clave pública; ii) certificados de atributo y iii) servicios de autenticación. Al respecto consultar José Fernando Irabien Chedraui, “La Estandarización Internacional en el Ámbito de la Certificación Digital”, en *REDI: Revista Electrónica de Derecho Informático*, No. 64, México, Alfa-Redi, noviembre/2003, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1266>

correspondiente al objeto.

- f) - Número del certificado - Es el código identificativo único del certificado que esta representado por un valor entero, único dentro del sistema del PSC, que está asociado inequívocamente con un *Certificado* expedido por aquél. En presencia de dos certificados distintos pero asociados a la misma identidad y sin confirmación de revocación para ninguno, permite identificar el más reciente gracias al número de serie y revocar de oficio el anterior.
- g) - OID - Contracción de los vocablos ingleses “*Object Identifier*”, cuyo significado en español es “Identificador de Objeto”. Consiste en un valor de naturaleza jerárquica y comprensivo de una secuencia de componentes variables aunque siempre constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto de OID.

4.2. Datos y Dispositivos de creación de firma electrónica.-

4.2.1. Los datos de creación de firma.-

Son los datos únicos, como códigos o claves criptográficas privadas que el Firmante/Suscriptor utiliza para crear firmas electrónicas, coinciden desde un punto de vista técnico - en función de su generación y utilización - con la clave criptográfica asimétrica privada, que es aquella destinada a permanecer en secreto (arts. 24.1. LFE; 2.4. DFE; 6.3.a. y 6.3.b. LMFE). Además debemos aclarar que una clave es la secuencia de símbolos que controlan las operaciones de cifrado (la pública) y descifrado (la privada). Normalmente se rigen por los estándares criptográficos de *Clave Pública* producida por RSA Laboratorios, y aceptados internacionalmente como estándares (*PKCS: Public-Key Cryptography Standards*).³⁷³

³⁷³ RSA: Acrónimo de Ronald Rivest, Adi Shamir y Leonard Adleman inventores del sistema criptográfico de clave asimétrica referido (1977). Criptosistema de clave pública que permite el cifrado y la firma digital.

4.2.2. El dispositivo seguro de creación de firma.-

Es un elemento que sirve para aplicar los datos de creación de firma, el cual debe cumplir con los requisitos establecidos en las normas específicas de aplicación en España (arts. 24.2. y 24.3. LFE); así como las recogidas en el Anexo III de la DFE (arts. 2.5. y 2.6. DFE).³⁷⁴

El elemento mayormente empleado a estos propósitos es la Tarjeta criptográfica, que constituye un dispositivo seguro de creación de firma, la cual puede ser empleada para generar los datos de creación y de verificación de firma o para importar tales datos, e inclusive, es posible también almacenar el certificado reconocido.

Normalmente los PSC recomiendan para el uso del certificado expedido, la utilización de una Tarjeta criptográfica para evitar la posibilidad de duplicación de los datos de creación y verificación de firma y poseer un mejor control de los mismos; físicamente se corresponde con la *Tarjeta Inteligente* (también conocida como tarjeta de circuitos integrados)³⁷⁵ o el *Token* USB criptográfico de amplia difusión en el mercado.³⁷⁶

Así, la Tarjeta criptográfica con método de generación de claves en la propia Tarjeta criptográfica, imposibilita el uso o exportación de los datos de creación de firma fuera de la Tarjeta. La posibilidad de usar tarjetas inteligentes con criptoprocador como soporte físico de los servicios de certificación a los Firmante/Suscriptores, facilita su interacción con el PSC e incrementa considerablemente el nivel de seguridad de sus aplicaciones.

³⁷⁴ Tanto la LFE como la norma comunitaria señalan que se considera como seguro, al dispositivo de creación de firma que ofrece, al menos, las siguientes garantías: a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto; b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento; c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros; y d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

³⁷⁵ Conforme explica Umaña, normalmente es una tarjeta de plástico u otro material a la que, a diferencia de las tarjetas débito y crédito tradicionales (las cuales llevan una banda magnética), se le ha incorporado lo que comúnmente se llama un “chip” o unidad de procesamiento, que permite procesar información, y no solo almacenarla (A.F. Umaña, 2003: 441).

³⁷⁶ Un token es un dispositivo físico similar a un llavero que permite almacenar gran cantidad de información, incluyendo la clave privada de un suscriptor, y que se conecta al puerto USB del computador (A.F. Umaña, 2003: 441) / Se rigen por el *PKCS#11 (Cryptographic Token Interface Standard)*: Estándar Criptográfico de Clave Pública producido por RSA Laboratorios, y aceptado internacionalmente como estándar, que define un interfaz de programación independiente de la tecnología de base, para utilizar tokens criptográficos (por ejemplo, tarjetas inteligentes criptográficas) como medio de autenticación.

Al mismo tiempo que permite la generación interna de claves criptográficas, impide el acceso desde al exterior a las mismas, siendo realizadas todas las operaciones criptográficas con manejo de claves o, en su caso, datos de creación de firma en el interior de la propia Tarjeta. Las claves o, en su caso, datos de creación de firma no pueden ser usados ni copiados desde el exterior.

El estándar de tarjetas en el mercado ofrece claves RSA de hasta 2048 bits como algoritmo de clave cúbica, SHA-1³⁷⁷ para el Hasing³⁷⁸, y Triple-DES³⁷⁹ para el cifrado simétrico. El sistema operativo de la tarjeta sigue las especificaciones PC/SC³⁸⁰ y ofrece a las aplicaciones interfaz PKCS#11. La Tarjeta viene dotada de protección de acceso mediante PIN³⁸¹, y admite más de 15 Certificados estándar X.509.v3 de tamaño de clave de 1024 bits, con independencia del PSC que emita los Certificados.³⁸²

4.3. Datos y Dispositivos de verificación de firma electrónica.-

4.3.1. Los datos de verificación de firma.-

Son los datos, como códigos o claves criptográficas públicas que el Usuario del certificado reconocido utiliza para verificar la firma electrónica del Firmante/Suscriptor, coinciden - desde un punto de vista técnico - en función de su generación y utilización con la clave criptográfica asimétrica pública, que es aquella destinada a ser divulgada (arts. 25.1. LFE; 2.7. DFE).

³⁷⁷ *Secure Hash Algorithm* (algoritmo seguro de resumen -hash-). Desarrollado por el NIST y revisado en 1994 (SHA-1). El algoritmo consiste en tomar mensajes de menos de 264 bits y generar un resumen de 160 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es prácticamente nula. Por este motivo se usa para dotar de *Integridad* a los documentos durante el proceso de firma electrónica.

³⁷⁸ Una *Función hash* es una operación que se realiza sobre un conjunto de datos de cualquier tamaño de tal forma que se obtiene como resultado otro conjunto de datos, en ocasiones denominado “resumen” o “*Hash*” de los datos originales, de tamaño fijo e independiente del tamaño original que, además, tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es prácticamente imposible encontrar dos mensajes distintos que tengan un resumen *Hash* idéntico.

³⁷⁹ Sistema de cifrado simétrico que surge como una evolución del DES (*Data Encryption Standard* - Estándar de Cifrado de Datos) descrito en el FIPS 46-3 (*Federal Information Processing Standard*) que desarrolla el DEA (*Data Encryption Algorithm* - Algoritmo de Cifrado de Datos) también definido en el estándar ANSI X9.32.

³⁸⁰ Contracción de los vocablos ingleses “*Personal Computer/Smart Card*” cuyo significado en español es “Computadores Personales/Tarjetas Inteligentes”. Es una especificación desarrollada para facilitar la interoperatividad necesaria para permitir que la tecnología de Tarjetas de Circuitos Integrados también conocida como Tarjetas Inteligentes puedan ser eficientemente utilizadas en entornos de computadores personales.

³⁸¹ Contracción de los vocablos ingleses “*Personal Identification Number*” cuyo significado en español es “Número de Identificación Personal”. Es un número específico para ser únicamente conocido por la persona que tiene que acceder a un recurso que se encuentra protegido por este mecanismo.

³⁸² Las nociones técnicas enunciadas han sido minuciosamente recopiladas de la Declaración de Prácticas de Certificación de la FNMT-RCM, versión al 4 de enero de 2011 y disponibles en la dirección URL www.cert.fnmt.es

4.3.2. El dispositivo de verificación de firma.-

Es un elemento que sirve para aplicar los datos de verificación de firma, que debe cumplir con los requisitos establecidos en las normas específicas de aplicación en España (arts. 25.2. y 25.3. LFE); así como las recogidas en el Anexo IV de la DFE (art. 2.8. DFE).³⁸³

Conforme lo que se tiene dicho para el dispositivo seguro de creación de firma, la Tarjeta criptográfica constituye también un dispositivo de verificación de firma, que puede ser empleada para generar los datos de creación y de verificación de firma o para importar tales datos, e inclusive, es posible también almacenar el certificado reconocido.

4.4. El dispositivo de generación de datos de creación de firma (de claves).-

También conocido como dispositivo de generación de claves, es un programa o un aparato informático o sus componentes específicos, destinados a ser utilizados para la prestación de servicios de firma electrónica por el PSC o para la creación o verificación de firma electrónica. En el art. 2.12. DFE es definido como “*producto de firma electrónica*”.³⁸⁴

V. Elementos formales.-

La certificación reconocida como se tiene analizado con carácter previo, es un contrato consensual que no necesita ningún requisito especial en cuanto a la forma para que produzca plenos efectos jurídicos, por lo que se rige por lo establecido en el art.51 del C.com. en relación con los artículos 1.278 y 1.279 del C.c..³⁸⁵ En otras palabras, la certificación reconocida no es un contrato formal, toda vez que para su perfeccionamiento - a través de la

³⁸³ Tanto la LFE como la norma comunitaria señalan que durante el proceso de verificación de firma, deberá garantizarse, con suficiente certeza, que: a) Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma; b) Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente; 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; 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; e) Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente; f) Que pueda detectarse cualquier cambio relativo a su seguridad. Finalmente el art. 25.4. de la LFE, establece que 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, podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza.

³⁸⁴ Programas y dispositivos que hacen posible el sistema de firma (creación de claves y certificados, tarjetas y lectores de tarjetas, subprogramas para sistema de correo, etc. (M. Tintó, 2001: 786).

³⁸⁵ Al respecto, Prats señala que el principio general en el Derecho privado español es el de libertad de forma “*principio espiritualista*”. En ese sentido, explica que la forma no se exige para la válida constitución de una relación jurídica (arts. 1.278. 1.279 c.c. y 51 C.com.), excepto en las ocasiones en que una disposición normativa así lo prevea de modo expreso. Por consecuencia, infiere, que con carácter general, la forma en un contrato persigue efectos demostrativos o probatorios de su existencia y del contenido de sus estipulaciones (L. Prats, 2001: 89).

conjunción de la oferta y la adhesión del solicitante como declaraciones de voluntad de las partes (arts. 1.258 y 1.262 C.c.) - no se exige el otorgamiento de la adhesión contractual por medio de una forma especial.

Una de las particularidades más relevantes es la necesidad de solicitar previamente al PSC la prestación del servicio. Conforme estudiaremos con más detalle posteriormente, entre la fase de preparación o formación y perfeccionamiento del contrato, se presentan una serie de etapas que se verifican unas veces en línea (*on line*) y otras fuera de línea (*off line*). Se inicia mediante comunicaciones electrónicas entre el solicitante de un certificado reconocido (ulterior Firmante/Suscriptor del mismo) y el PSC, para posteriormente producirse el apersonamiento del futuro Firmante/Suscriptor ante las oficinas del PSC o una Entidad de Registro delegada, donde se procederá al registro y llenado por escrito de la solicitud del certificado de identidad reconocido.

En la solicitud se exigirá una exhaustiva y detallada información personal que faculte la plena identificación del solicitante. No nos olvidemos que la identificación indubitada del Firmante/Suscriptor y titular del certificado reconocido, exige su personación ante el PSC o la Entidad de Registro (ER) delegada por aquél portando su DNI, y en el caso de personas jurídicas los documento acreditativos de la representación del solicitante del certificado.

Una vez que el PSC acepta la solicitud del interesado, se procede a la firma y la documentación del contrato en sí, es decir, que normalmente y finalmente desemboca en la firma de un contrato escrito rubricado de puño y letra por ambas partes.

Si bien como hemos aseverado se trata de un contrato consensual, por lo que su perfección depende únicamente del consentimiento de las partes, no obstante y a pesar de que en ningún caso supondrán requisito alguno en orden a la constitución de las obligaciones, sí que se pueden apreciar en la práctica ciertas formalidades que tienen como objetivo fundamental servir como medio de prueba ante un eventual conflicto. Por lo tanto, y a pesar

de regir plenamente en relación con este contrato el principio de libertad de forma, el espiritualismo ya consagrado en el Ordenamiento español, merece la pena comentar de qué manera se documenta la relación que ahora analizamos.

Respecto al momento de la perfección, lo normal en estos contratos tal y como se verifica en la práctica es que la comunicación de la oferta, la adhesión a la misma y su posterior comunicación al oferente se produzcan sin solución de continuidad a través de la firma del contrato en un solo acto.

Es decir que presentado el contrato por el PSC o la Entidad de Registro delegada al cliente, en el cual se contienen las condiciones generales junto a las condiciones particulares del contrato, éste, tras su lectura (cuyo contenido habrá sido puesto previamente en su conocimiento, particularmente los documentos denominados: Declaración de Prácticas de Certificación y las Políticas de Certificación asociadas el certificado reconocido de identidad que se solicita) procederá a la adhesión y comunicación de la misma a la contraparte. Celebrado así el contrato comienzan a verificarse los efectos que del mismo se desprenden a través del cumplimiento de las obligaciones a que ambas partes se comprometen (art. 1.258 C.c.).

De las indicaciones del modo en que el contrato de certificación reconocida se verificará y de la propia existencia de una pluralidad de formularios de contratos, se observa cómo el tráfico ha generalizado que el contrato y sus modificaciones o adiciones se formalicen por escrito, es decir que el contrato de certificación reconocida es un contrato que reviste la forma escrita.³⁸⁶

³⁸⁶ Blanch indica al respecto, que entre el signatario o suscriptor de los servicios y el PSC se realiza un contrato que es el que permite la realización de la firma electrónica, especificando dicho contrato la vinculación entre los documentos firmados electrónicamente y quien realiza la firma electrónica, y señala los derechos, obligaciones y responsabilidad de las partes, especificando respecto del contrato que *“Este documento es firmado autógrafamente* (las negrillas son nuestras) *y no sólo asocia una clave pública a un sujeto sino que también asevera que éste ha aceptado voluntariamente su trascendencia y tiene bajo su custodia la clave privada correspondiente.”* Ma. Rosa Blanch Domeque, “La fe pública judicial en el sistema de firma electrónica. Autoridades de certificación”, en María del Carmen Bernal López, comp., *Jornadas sobre Actos de comunicación: Nuevas Tecnologías*, Madrid, 2001; en Estudios Jurídicos. Secretarios Judiciales, VI-2001, Madrid, S.A. de Fotocomposición, 2001, p.814.

Este modo de procederse en el tráfico plantea no obstante, la cuestión del alcance que haya de darse a dichas exigencias a la hora de determinar si estamos, como hemos apuntado, ante un contrato consensual o, contrariamente, ante un contrato formal.

En este sentido parece derivarse que la exigencia de forma se establece con el alcance que normalmente se le da en materia de contratos, es decir, como una exigencia *ab probationem* (según prescriben los arts. 1.278 a 1.280 y 1.300 a 1.314 del C.c. y el art. 51 del C.com.), al igual que toda la contratación moderna que se verifica por escrito a los efectos probatorios pero no constitutivos, pero sin que implique que haya de entenderse como una exigencia de forma *ad solemnitatem*, lo cual sería contrario al principio general de libertad de forma consagrado en el Ordenamiento y carecería de justificación desde una perspectiva jurídica, ya que se busca seguridad pero no introducir elementos formales en la celebración del contrato.

El contrato de certificación reconocida existe cualquiera que sea la forma seguida por las partes para su celebración, aunque necesidades de prueba y, sobre todo, la complejidad que el contrato presenta - cuyo contenido básico aparece configurado a través de las Condiciones Generales elaboradas por las empresas certificadoras - lleven a su celebración por escrito.

Éste generalmente y como es habitual se va a realizar llenándose un formulario que se extenderá y firmará por duplicado, de manera que uno de los ejemplares quede en poder del PSC (o la Entidad de Registro que luego lo remitirá al PSC) y el otro en poder del cliente. En este documento se detallarán todos aquellos datos del cliente que sean relevantes en relación con el contrato de referencia (identificación, DNI, domicilio, etc.) así como las características del certificado que esta solicitando (reconocido). Asimismo se especificará el plazo de vigencia del certificado como el precio a satisfacer, que suele variar en función del tipo de certificado que se solicita.

Por último, en este mismo documento y a no ser que se adjunten en pliego aparte, suelen figurar las denominadas condiciones generales del contrato; aquellas que se aplican indiscriminadamente a una pluralidad de clientes, que son redactadas unilateralmente por el PSC y respecto de las cuales el posible Firmante/Suscriptor carece de margen alguno de maniobra, quedándole únicamente la posibilidad de asumirlas o rechazarlas globalmente.

Es el documento en el que se contienen los elementos esenciales del contrato (recoge el contrato de certificación reconocida) estableciendo los derechos y obligaciones que las partes asumen y la modalidad de certificado por la que se ha optado, así como el período de duración y garantías establecidas; conteniendo una remisión a las Prácticas y Políticas de Certificación asociadas al certificado que el cliente declara expresamente conocer y aceptar.

Dichos documentos se encargarán de disciplinar cuál va a ser el contenido del contrato, teniendo en todo caso que sujetarse a las disposiciones que figuran en la LCGC así como en el TRLGDCU, cuando se contrata con consumidores; ambas intentan prever posibles abusos amparados en la predisposición, para lo cual articulan un completo sistema de control respecto de la aparición de cláusulas abusivas y/o nulas.

CAPÍTULO CUARTO

FORMACIÓN, PERFECCIONAMIENTO Y CONTENIDO CONTRACTUAL

I. Discernimiento inicial.-

En el presente apartado nos ocupa la evaluación de las distintas etapas que hacen al contrato de certificación reconocida, desde la fase de formación, pasando por su perfeccionamiento y ejecución, procediendo el estudio pormenorizado del contenido contractual.³⁸⁷

Conforme se tiene adelantado la certificación reconocida se articula fundamentalmente en torno a un elemento objetivo: el certificado reconocido, a cuyo alrededor a su vez se interrelacionan tres elementos subjetivos: el PSC, el Firmante/Suscriptor y el Usuario del certificado, situación que configura el surgimiento de una serie de obligaciones o deberes de conducta para los distintos sujetos implicados en la actividad certificadora.

Establecidas las cosas de este modo, resulta de vital importancia determinar el origen (legal, contractual o extracontractual), el contenido así como el alcance de dichos deberes. Efectivamente, resulta conveniente sistematizar con precisión el conjunto de conductas que hacen a cada una de las entidades subjetivas involucradas, teniendo claro a qué obligaciones en concreto se encuentran reatados.

La utilidad práctica de este ejercicio radica finalmente en el hecho que, precisadas las obligaciones y establecido el origen de las mismas, estaremos en condiciones de modular con mayor precisión el régimen de responsabilidad que atinge a cada una de las entidades subjetivas involucradas.

Cabe adelantar que el estudio de los deberes que surgen para el PSC y el Firmante/Suscriptor no presenta mayores dificultades, pues éstos, en la etapa de tratos

³⁸⁷ Nos adscribimos a la posición mercantilista sostenida por Garrigues, por la que nos referimos a contenido del contrato en sentido amplio, comprendiendo como contenido del mismo las relaciones jurídicas que, a consecuencia de la perfección del contrato surgen entre las partes contratantes, vale decir, las obligaciones entre las partes. Joaquín Garrigues, *Curso de Derecho Mercantil*, vol. II, Imprenta Silverio Aguirre Torre, Madrid, 1962, p.3.

preliminares devienen básicamente del principio-deber de buena fe, que como sabemos amplifica su contenido con una serie de deberes de información y lealtad negocial; en tanto que en la etapa subsiguiente, al margen de configurarse como obligaciones legales, previstas en el contrato de certificación reconocida se modulan como verdaderas obligaciones contractuales.

La interrogante surge al momento de considerar las obligaciones que atingen al Usuario del certificado, las cuales tienen como origen directo - al menos en inicio - la ley, por lo que desde un principio debe quedar absolutamente claro que los deberes del Usuario del certificado no nacen del contrato de certificación reconocida, lo cual es lógico, pues los contratos únicamente obligan a las partes contratantes (principio de relatividad del contrato art. 1.257 C.c.), no pudiendo atribuirse obligaciones a un sujeto ajeno a la relación contractual.

Revistiendo las obligaciones del Usuario la categoría de auténticas obligaciones legales corresponderá analizar si es posible su contractualización con el PSC, posibilidad que exploraremos precisamente en el presente Capítulo.

II. Formación del contrato.-

Conforme enseña la doctrina la formación de un contrato puede revestir básicamente dos modalidades: i) ser instantánea o momentánea; ii) ser sucesiva o progresiva. La formación del contrato es instantánea cuando su preparación es consecuencia de un único acto de los contratantes, de manera que no existe ningún acto previo toda vez que no requiere de una elaboración o discusión preliminar.

De otra parte, la formación es progresiva cuando existe un período de tiempo en el que los contratantes previamente negocian y discuten una serie de aspectos, para finalmente perfeccionar el contrato en sí. Díez-Picazo sostiene que en este tipo de negocios jurídicos el contrato se va formando *ex intervallo temporis*; su característica estriba en el hecho que la

formación del contrato no es consecuencia de un acto único sino de una serie concatenada de varios actos previos, en los cuales pueden intervenir no únicamente las partes contratantes, ya que es posible la participación de otros sujetos que coadyuvan para la obtención del propósito buscado por aquellos: perfeccionar un contrato.³⁸⁸

En el caso concreto de la certificación reconocida observamos que las distintas fases o etapas en el *iter* del contrato, que van desde la fase de preparación o formación (que culmina con el perfeccionamiento) y ejecución del contrato, son efectuadas unas veces en línea (*on line*) y otras fuera de línea (*off line*). En este punto resulta muy importante aclarar que en el caso de solicitud de certificados identificativos - que es el tipo de certificado que venimos estudiando - esta alternabilidad del medio (*on line/off line*) en las distintas fases entre la formación y perfeccionamiento del contrato, puede dar lugar a que el consentimiento contractual se produzca: fuera de línea (*off line*) o en línea (*on line*).

En el primero de los supuestos, vale decir cuando la adhesión del Firmante/Suscriptor no se produce en línea, nos encontramos ante una modalidad de contratación tradicional, que por lo demás no reviste mayores complejidades toda vez resultan aplicables las habituales normas generales que regulan las obligaciones y contratos.

En la segunda hipótesis estaríamos claramente ante una modalidad de contratación electrónica,³⁸⁹ siendo en consecuencia de aplicación además de las señaladas previamente, las normas comunitarias y españolas que regulan este tipo de contratos, fundamentalmente las contenidas en la DCE y LSSI. En todo caso se deja advertido que no es nuestro objetivo analizar con detalle la figura de la contratación electrónica, tarea que excede la finalidad de la presente investigación.

³⁸⁸ (L. Díez-Picazo, 1996: 267-270).

³⁸⁹ Lo cual evidentemente puede ocurrir en la medida que las Prácticas y Políticas de Certificación del PSC en concreto lo permitan. No obstante, lo habitual es que la contratación electrónica se presente en otro tipo de certificados que no sean identificativos, como por ejemplo los certificados de sitio seguro, que no identifican a un sujeto sino que relacionan una concreta dirección URL con un servidor determinado.

Asimismo cabe adelantarnos en precisar que una vez generado el certificado reconocido, lo que ocurre normalmente es que tanto su envío y descarga³⁹⁰ así como las ulteriores prestaciones relacionadas con la firma electrónica (publicación, servicios de suspensión, revocación y/o extinción de certificados, sellado temporal, servicios de validación o verificación, etc.) se producen en línea (*on line*). Esta situación configura que independientemente del medio en el que se perfecciona el contrato (electrónico o tradicional), o el canal por el que se emite y entrega el certificado (*on line/off line*), sustancialmente la ejecución de la certificación reconocida - globalmente considerada atendiendo al fin contractual - se lleva a cabo por medios electrónicos.

Además, tanto en la fase de formación como en la ejecución contractual habitualmente concurre la Entidad de Registro (ER), lo que denota la característica *sui generis* de este negocio jurídico.

Puede decirse entonces que el contrato se va formando *ex intervallo temporis*, toda vez que constituye una operación que reviste cierta complejidad técnica y demanda una serie de pasos previos, o en otras palabras, es un contrato de formación sucesiva en la que normalmente coadyuva un tercero (la ER) con las partes contractuales.

También es conveniente resaltar que durante las distintas fases del *iter* contractual no se produce ningún tipo de negociaciones o acuerdos previos entre las partes contratantes, toda vez que como se ha estudiado, la certificación reconocida es un contrato sujeto a condiciones generales y perfeccionado mediante adhesión, no existiendo posibilidad por parte del Firmante/Suscriptor de negociar los clausulados previamente redactados por el PSC. Pero lo que sí ocurre es que existen unas fases preliminares, entre las que podemos señalar: entrega

³⁹⁰ Decimos normalmente, puesto que puede también ocurrir que tras generar las claves, la ulterior emisión y entrega del certificado se produzca fuera de línea (*off line*). Esta situación acontece cuando el Firmante/Suscriptor que acude personalmente ante el PSC o la ER delegada a objeto de su identificación, a tiempo de recabar la tarjeta criptográfica obtiene también en ese mismo momento su certificado, el cual es almacenado en la propia tarjeta criptográfica que se le entrega en esta ocasión. Las claves son generadas al interior del dispositivo seguro de creación de firma (la tarjeta criptográfica), con lo que en este modelo no existe la emisión y envío del certificado en línea sino que la emisión y entrega cuentan con la presencia del Firmante/Suscriptor. Todo depende, como se tiene dicho, de las concretas prácticas y políticas de certificación que cada empresa maneja en el mercado. Pero lo evidente es que independientemente del modelo o canal que siga el PSC para emitir y hacer entrega del certificado, esencialmente los demás servicios relacionados con la firma electrónica se prestan en línea.

de información, adquisición de elementos de software, generación de claves criptográficas y otras como veremos luego con más detalle, que demandan de un período de tiempo entre la formación y el perfeccionamiento del contrato, para su posterior ejecución.

La contratación se lleva a cabo por consecuencia mediante un procedimiento o proceso de formación, entendidas las ideas de procedimiento y de proceso en palabras de Díez-Picazo: *como desarrollo de actividades que se llevan a cabo mediante una regular sucesión para la obtención de un determinado efecto jurídico.*³⁹¹

Con carácter previo al análisis de las etapas de formación del contrato objeto de estudio, debemos resaltar que los pasos a seguirse durante este periodo de preparación contractual pueden variar de un PSC a otro, ello depende fundamentalmente de las concretas Prácticas y Políticas de certificación que cada empresa certificadora maneja. Por consiguiente vamos a adoptar en este estudio un modelo prototipo y que resulta el más frecuente en el tráfico.

En los siguientes apartados se describirá el procedimiento de solicitud por el que se recaban y registran los datos personales de un Solicitante, se confirma su identidad y paralelamente se formaliza el contrato con el PSC para la posterior emisión de un certificado reconocido, previa realización de las validaciones pertinentes. Conforme se tiene enunciado, estas actividades - sobre todo en ambientes geográficos dispersos - son normalmente realizadas a través de las ER delegadas por el PSC.

2.1. Procedimiento de solicitud del Certificado.-

Para una mejor comprensión del procedimiento a seguir a efectos de solicitar y posteriormente obtener un certificado reconocido, se ha visto por conveniente sistematizar el análisis dividiendo las distintas fases por *Etapas*, con la advertencia ya mencionada que

³⁹¹ (L. Díez-Picazo, 1996: 270).

algunas de ellas se efectúan fuera de línea (*off line*) en tanto que otras se llevan a cabo en línea (*on line*), las cuales pasamos a describir y explicar.³⁹²

2.1.1. (Etapa I) Obtención de información.-

Lo primero que debe hacer el interesado en adquirir un certificado reconocido es lógicamente informarse de las distintas empresas certificadoras (PSC) que existen en el mercado, así como de los servicios y productos que ofrecen, los precios, sus prácticas y políticas de certificación, etc. (*habitualmente vía on line*) para finalmente decidirse por un PSC de reconocido prestigio y en quien confía.

2.1.2. (Etapa II) Obtención de elementos tecnológicos.-

Con la decisión tomada el interesado o peticionario debe proveerse con carácter previo a la fase de presolicitud de un certificado reconocido, de la tarjeta criptográfica y del software de generación o importación de los datos de creación y de verificación de firma en la Tarjeta (*procedimiento off line*).

Para ello existen dos opciones:

- a) Que obtenga dichos elementos de un proveedor ajeno al PSC, pero asegurándose que reúnan las características técnicas y de seguridad exigidas por el PSC seleccionado, siempre y cuando esta posibilidad se encuentre expresamente admitida en las Prácticas y Políticas de certificación del PSC.
- b) Que obtenga dichos elementos del propio PSC.

Conforme se tiene analizado, la tarjeta criptográfica es un dispositivo seguro de creación de firma que puede ser empleada para generar los datos de creación y de verificación de firma o para importar tales datos. Normalmente los PSC recomiendan para el uso del certificado expedido, la utilización de una tarjeta criptográfica a fin de evitar la

³⁹² Para configurar el procedimiento de solicitud y emisión del certificado electrónico, han sido consultadas las Declaraciones de Prácticas y Políticas de Certificación de diversos certificadoros españoles, tanto públicos como privados, entre los que cabe destacar: AC-Abogacía; ACE; ANF-AC; CAMERFIRMA; CICCP; ipsCA; ACCV; ANCERT; Banesto CA; FirmaProfesional; Izempe SA; FNMT-RCM (CERES), en las cuales nos basamos, a objeto de presentar en esta investigación un modelo prototípico en este tipo de operaciones. Dichos documentos pueden ser consultados en línea en la dirección URL de las respectivas entidades.

posibilidad de duplicación de los datos de creación y verificación de firma y poseer un mejor control de los mismos. Las tarjetas criptográficas de mayor empleo en el mercado son las denominadas “*Tarjetas inteligentes*” o los token USB criptográficos.

El peticionario puede requerir la simple descarga del certificado reconocido a este soporte, o la generación en el mismo del juego de claves, que posteriormente serán utilizadas como datos de creación y verificación de firma. En ambos casos además de la tarjeta criptográfica, el peticionario deberá obtener el software necesario para la importación y/o generación de las claves por la propia tarjeta.

En el procedimiento de obtención de certificados por parte del peticionario, el PSC facilitará - en el caso de emplearse como soporte del certificado la tarjeta criptográfica - los elementos necesarios para activar en la esfera del peticionario, el software pertinente para generar a través de su Navegador (v.gr. Netscape Communicator; Microsoft Internet Explorer; Mozilla Firefox; Safari u otros), las claves criptográficas que le permitan proteger la seguridad de sus comunicaciones a través de mecanismos de cifrado, así como autenticarse y firmar, constituyéndose en este último caso como datos de creación y de verificación de firma.

Asimismo, cuando el certificado se contenga en soporte convencional y no en tarjeta criptográfica, los datos de creación de firma también serán utilizados bajo el control del software de navegación web del que disponga el propio peticionario, enviando la clave pública que será utilizada como datos de verificación de firma al PSC con el fin de integrarla en un certificado.³⁹³ En cualquier caso e independientemente del soporte empleado para

³⁹³ Cuando el certificado reside en un soporte convencional de almacenamiento de software (disco duro, disquete, etc.), la generación de los datos de creación de firma y de los datos de verificación de firma se efectúan en el Navegador del Firmante/Suscriptor, mediante procedimientos alternativos al SSCD (*Secure Signature-creation Device*) para dotar de seguridad al proceso. Tanto los certificados como la clave privada serán custodiados por el Navegador y su sistema operativo, siendo almacenados en memoria no volátil. Habrá posibilidad en este caso de exportar los datos de creación de firma a otros soportes, cuya protección vendrá conferida por la utilización de palabras de acceso, mas conocidas como “passwords”. Información obtenida de la Declaración de Practicas de Certificación de la FNMT-RCM, disponible en <http://www.cert.fnmt.es>

almacenar el certificado, los datos de creación de firma deberán permanecer siempre bajo el exclusivo control del futuro Firmante/Suscriptor, no archivándose copia de ellos por el PSC.

Una vez obtenido este soporte y el software necesario para la operación que desee realizar, o bien, si el certificado se almacenara en un soporte convencional de almacenamiento de software, el peticionario procederá según se dispone a continuación.

2.1.3. (Etapa III) Presolicitud del certificado.-

El peticionario accede al sitio web del PSC a través de la dirección URL correspondiente, donde se mostrarán las instrucciones del proceso completo. Deberá introducir normalmente su DNI, NIF, NIE, o en el caso de personas jurídicas el CIF de la organización en el punto de recogida de datos dispuesto para ello. Posteriormente se generarán las claves pública y privada (*en Tarjeta criptográfica o en el navegador*) que serán vinculadas al certificado, el cual deberá ser solicitado en una Entidad de Registro delegada por el PSC. En este momento se asigna e indica al peticionario un código de solicitud (*procedimiento on line*).

Como se tiene dicho, con carácter previo el peticionario deberá consultar la Declaración de Prácticas y las Políticas de Certificación (*que contienen las condiciones generales de uso, derechos, obligaciones y límites de responsabilidad para las partes*) asociadas al certificado reconocido que desea obtener, en la dirección URL del PSC, las cuales pasaran a formar parte del contrato de certificación reconocida.

Es importante aclarar en esta etapa, que en ningún caso la continuación del procedimiento de presolicitud implica la conclusión de una contratación. Al realizar esta presolicitud se envía al PSC la clave pública generada para la posterior emisión del certificado reconocido, entregándose de forma automatizada la correspondiente prueba de posesión de la clave privada.

El PSC tras recibir esta información, comprobará mediante la clave pública del *petionario* del certificado la validez de la información de la presolicitud cifrada, comprobando únicamente que se corresponde con los datos facilitados por el *petionario*. Asimismo, esta operación servirá como indicador de la posesión y correspondencia de la pareja de claves criptográficas por parte del *petionario*.

Esta información no dará lugar a la generación de un certificado por parte del PSC en tanto que éste no reciba firmada la solicitud del certificado reconocido realizada por el *petionario* que, a partir de ese momento, cambia su condición de simple *petionario* o interesado pasando a tener la condición de “*Solicitante*” de un certificado reconocido.

2.2. Deberes de conducta en la preparación contractual.-

En la fase preliminar al perfeccionamiento del contrato de certificación reconocida básicamente devienen dos deberes principales para ambas partes contratantes: i) el deber de proceder conforme la buena fe, y ii) deberes de conducta e información recíprocos. Así por ejemplo, el solicitante y futuro Firmante/Suscriptor debe facilitar al PSC los datos relativos a su identificación, en tanto que el PSC debe informar entre otras cosas, las condiciones en las que presta el servicio; por otro lado, ambas partes deben actuar de buena fe facilitando información veraz y oportuna, ejecutando los distintos pasos de la manera debida y prudente con la intencionalidad de perfeccionar el contrato.

2.2.1. Principio-deber de buena fe.-

En el ámbito de la contratación como se ha mencionado, es plausible observar la existencia de un proceso contractual, es decir, aquel conjunto concadenado de acciones que conducen al cumplimiento del contrato. Este proceso está compuesto por tres etapas primordialmente; la etapa de formación (negociación o tratos preliminares), la etapa de perfeccionamiento (nacimiento) y la etapa de ejecución, cumplimiento o extinción.

Como es bien conocido el llamado principio-deber de *buena fe* se encuentra presente durante las tres etapas anteriormente mencionadas.³⁹⁴ Lo que se pretende a continuación es analizar la incidencia de la *buena fe* negocial en la primera etapa del *iter* contractual, es decir, en la llamada etapa preparatoria a la luz de la nueva concepción de la *buena fe* en las relaciones contractuales, vista como: diligencia y profesionalismo.

Posteriormente analizaremos el hecho que la obligación de actuar de buena fe en esta etapa del *iter* contractual, implica para ambas partes la puesta en marcha de una serie de deberes “...que se resumen en los principios de lealtad y corrección en la conducta, y que consisten básicamente en manifestar claramente las circunstancias personales u objetivas que puedan rodear las respectivas etapas, y un deber de informar sobre todas las circunstancias que puedan interesar a la contraparte: las peculiaridades de la legislación; las circunstancias que no puedan ser conocidas por el futuro contratante luego de un estudio profesional adecuado y que constituyen en cierta forma extensión de las obligaciones pre y postcontractuales”.³⁹⁵

El principio-deber de *Buena fe* se remonta a los albores del Derecho Romano y posteriormente en el aporte del Derecho Canónico al ámbito mercantil. A continuación y por su importancia procuraremos efectuar una somera referencia al surgimiento de esta institución. La doctrina considera que su origen se encuentra en el Derecho Romano.³⁹⁶ Si bien no se habla de buena fe en sentido gramatical, si se hace referencia a la denominada

³⁹⁴ Es preciso aclarar que cuando se habla aquí de buena fe, se está señalando la buena fe como principio, para lo cual se trae a colación lo que señala Díez-Picazo al respecto: “... el principio general de buena fe...no es ya un puro elemento de un supuesto de hecho normativo, sino que engendra una norma jurídica completa, qué, además se eleva a la categoría o al rango de un principio general del derecho: todas las personas, todos los miembros de una comunidad jurídica deben comportarse de acuerdo a la buena fe en sus reciprocas relaciones... Los derechos deben ejercitarse de buena fe; las obligaciones tiene que cumplirse de buena fe.” Luís Díez-Picazo, “Prólogo” en: Franz Wieacker, *El Principio General de Buena Fe*, (trad. De José Luís Carro), Madrid, Civitas, 1982, pp.11 y ss..

³⁹⁵ Jorge Oviedo Albán, *Consideraciones Sobre la Formación del Contrato en el Código de Comercio Colombiano*, Lima, Publicado en: Revista Jurídica del Perú, Año LIII, N° 50, Septiembre de 2003, p. 113 // Junto con el deber de información, también la doctrina señala otros deberes colaterales, o “deberes secundarios de conducta” el de secreto, custodia, colaboración, confiabilidad, y el deber de no abandonar sin justa causa las negociaciones, entre otras clasificaciones. Véase Ricardo Luís Lorenzetti, *Esquema de una teoría Sistemática del Contrato*, en Atilio Anibal Alterini; José Luís De Los Mozos; Carlos Alberto Soto, comp., *Contratación Contemporánea, Teoría General y principios, La Convención de las Naciones Unidas Sobre los Contratos de Compraventa Internacional de Mercaderías*, Bogota, Editorial Temis S.A., 2000, p. 21 y ss. // Francesco Messineo, *Doctrina General del Contrato*, vol. I, Buenos Aires, Ediciones jurídicas Europa-América, 1986, p. 309 y ss.

³⁹⁶ López Santamaría explica que la *fides* es un principio ético de honorabilidad, constituyendo el fundamento de la justicia y motor del Derecho contractual romano. Jorge López Santamaría, *Los Contratos, parte general*, vol. I, 3ª ed., Santiago, Editorial Jurídica de Chile, 1998, p. 47.

fides o “*fe, a secas, como virtud y comportamiento honesto, diligente, leal, a la que luego se le agregó el adjetivo calificativo de buena, especialmente con referencia a la posesión... que no tiene que confundirse con la denominada buena fe negocial*”.³⁹⁷

En la edad media con la aparición y expansión del Derecho Canónico por gran parte del viejo continente, se hablaba de la “espiritualización” del contrato, consistente en la valoración preeminente o exclusiva de la voluntad subjetiva de los contratantes, la cual tendría fuerza obligatoria por sí misma, pues por motivos éticos es menester que el hombre respete la palabra empeñada. Según se infiere de la suma teológica faltar a una promesa es un engaño, una mentira, y por consiguiente un pecado.³⁹⁸

Con lo expresado anteriormente, se puede confirmar que fue el Derecho Canónico el que continuó desarrollando la figura de la *fides* romana convirtiéndola en la institución que hoy en día se conoce con el nombre de Buena fe (*bona fides*), pues siguiendo la doctrina de Iglesia Católica el hombre es bueno por naturaleza, por lo que sus propios actos gozan de la presunción de buena fe, para lo cual hay que añadir que sólo el consentimiento basta para que se obligue sin necesidad de mediación de fórmulas sacramentales que vinculen a las partes.

Más adelante se puede observar que si bien es cierto que el derecho canónico realizó un gran aporte en torno al principio de *Buena fe*, es un error afirmar que fue este derecho el que introdujo y desarrolló completamente la institución, ya que frente al Derecho Canónico existía una gran limitante referente a que su ámbito de aplicación se circunscribía a los fieles católicos, por lo tanto no tenían mayor relevancia o fuerza vinculante con relación a otros sujetos intervinientes en las relaciones jurídicas contractuales. El conflicto entre comerciantes y clérigos por la aplicabilidad del derecho canónico a los contratos comerciales, no reflejó

³⁹⁷ Fernando Hinestrosa, *Salvamento de Voto*, Sala de Casación Civil y Agraria, Corte Suprema de Justicia, Bogotá, Sentencia del 7 de mayo de 1968, M.P. Dr. Guillermo Ospina Fernández, Gaceta Judicial N° CXXIV, p. 117 y ss.

³⁹⁸ (J. López, 1998: 56-57)

ninguna considerable diferencia de opinión con respecto a la subordinación del contrato a consideraciones morales.³⁹⁹

Además del aporte del *ius canonicum* en relación con el desarrollo del principio de Buena fe, es claro que este principio-deber, también se desarrolló como consecuencia de la agilidad del tráfico mercantil y la elaboración del principio de la consensualidad de los actos jurídicos, ya que para la época dentro de los mismos gremios de mercaderes se desarrollaron formas contractuales nunca antes vistas o reguladas por el Derecho Romano, ni por el Derecho Germano, y que únicamente podían entenderse a la luz del principio de la buena fe.

Durante toda la edad media y más específicamente durante los siglos XII y XIII, el desarrollo de las prácticas y usos comunes dentro de las agremiaciones, guildas y dentro de la comunidad mercantil dio origen a la denominada *Lex mercatoria*; dentro de dichas prácticas, se encontraban inmersos “*ciertos principios jurídicos básicos, compartidos por todos los sistemas legales de la época y que fueron adaptados a las necesidades especiales de la comunidad mercantil. Éstos incluían el principio de Buena fe, que se manifestó sobre todo en la creación de nuevos recursos de crédito (...)*”⁴⁰⁰

Analizados someramente los antecedentes de esta institución, diremos para comenzar, que el Código Civil español si bien instituye el principio general de la buena fe para el ejercicio de los derechos (art.7 C.c.) no consagra expresamente la prescripción de un deber de actuar conforme la buena fe en la etapa pre-contractual (aunque si exige la buena fe en la etapa de ejecución contractual art. 1.258 C.c.), sin embargo creemos que en dicho estatuto también se incluye el deber de observar la buena fe en los tratos preliminares - así no sea explícitamente - al reconocer el Código que todo el que cause un daño estará obligado a repararlo, cuestión que eventualmente puede suscitarse en dicha etapa del *iter* contractual (art. 1.101 C.c.)

³⁹⁹ J. Harold Berman, *La Formación de la tradición jurídica de Occidente*, México, Editorial Fondo de Cultura Económica, 1993, p. 362.

⁴⁰⁰ (J.H. Berman, 1993: 366-367).

Por otra parte, la regulación del Código de Comercio encuentra una mayor acogida en cuanto a precisión, ya que el art. 57 señala que los contratos de comercio “*se ejecutarán y cumplirán de buena fe, según los términos en que fueren hechos y redactados, sin tergiversar con interpretaciones arbitrarias del sentido recto, propio y usual de las palabras dichas o escritas, ni restringir los efectos que naturalmente se deriven del modo con que los contratantes hubieren explicado su voluntad y contraído sus obligaciones*”.

A título informativo mencionaremos las disposiciones preliminares incluidas en el Código Europeo de Contratos (CEC), también conocido como Proyecto de Pavía.⁴⁰¹ En este documento el principio de la buena fe es aplicable a las diferentes etapas del contrato y se materializa en la práctica, a través de la prescripción de diferentes deberes y reglas de conducta dentro del *iter* contractual.

Así, se observa que en la etapa previa del contrato el principio de la buena fe y lealtad se consagra en el art. 6 del modo siguiente: “*1. Cada parte es libre de iniciar tratos preliminares con el fin de celebrar un contrato, sin que se le pueda imputar ninguna responsabilidad en el caso de que aquél no se perfeccione, salvo si su comportamiento es contrario a la buena fe. 2. Actúa contra la buena fe la parte que inicia o prosigue tratos preliminares sin intención de llegar a la celebración del contrato.*”

Además el principio-deber de buena fe se concreta en el CEC con algunos deberes secundarios de conducta a saber:

i) deber de información, visto como el conjunto de circunstancias que adornan la realidad y muestran de una manera cierta la versión propuesta por la contraparte dentro de las negociaciones (art.7);

⁴⁰¹ Cabe aclarar que el Código Europeo de Contratos, conocido como Proyecto de Pavía (por tener en esta ciudad su sede la Academia de Jusprivatistas Europeos que lo ha patrocinado y gestado), o Proyecto Gandolfi (por alusión al nombre de su impulsor y coordinador); junto con sus paralelos, el Proyecto Lando y demás trabajos integrantes del Marco Común de Referencia, no revisten - por ahora - de ningún carácter oficial en la UE, pero por su carácter ilustrativo y orientador hemos visto por conveniente su análisis en esta investigación.

ii) deber de reserva o confidencialidad, se observa a partir de la utilización de la información suministrada generándose una especie de valor o precio sobre la información revelada el cual merece ser conservado (art.8);

iii) deber de corrección, por el que no se debe abandonar las negociaciones sin justa causa, visto a partir de la intención y finalidad que rodean a las partes con respecto al nacimiento de obligaciones contractuales (art.6.3.). Como puede constatarse, la intención de contratar se evidencia con la generación de una “...confianza razonable en cuanto a la celebración del mismo... (del contrato)”.⁴⁰²

Por otra parte podemos también mencionar como orientadores los Principios UNIDROIT (PUNIDROIT),⁴⁰³ que consagran en el art. 1.7 el Principio de Buena Fe y Lealtad junto a su carácter imperativo de la siguiente manera: “*Artículo 1.7 (Buena Fe y Lealtad Negocial): (1) Las Partes deben Actuar con Buena Fe y lealtad Negocial en el comercio internacional. (2) Las partes no pueden excluir ni restringir la aplicación de este deber.*” De esta manera la buena fe y lealtad negocial en sí mismos son inspiradores de los demás Principios UNIDROIT, permitiéndonos concluir que la buena fe y la lealtad se consideran como supra-principios. El inciso (1) de este artículo deja claro que en ausencia de una disposición específica en los Principios, las partes deben conducirse de acuerdo a la buena fe y observando lealtad negocial a lo largo de la vida del contrato, incluso durante el proceso de su formación.

En algunas oportunidades a lo largo del texto de los Principios se hace referencia solamente a la “Buena Fe”, mientras que en otras oportunidades se refiere a la “buena fe y lealtad negocial”. Debe entenderse que el concepto de “Buena Fe” siempre incluye al concepto de “Buena fe y lealtad negocial” que alude el artículo 1.7.

⁴⁰² Gabriel García Cantero, *La Traducción Española de la Parte General del Código Europeo de Contratos*, Bogotá, Ediciones Academia Colombiana de Jurisprudencia, 1ª ed., 2004, p.14.

⁴⁰³ UNIDROIT, *Principios Sobre los Contratos Comerciales Internacionales*, obra publicada por el Ministerio de Justicia y del Derecho, de la República de Colombia, en desarrollo del Plan de Armonización del Derecho Internacional Privado -PADIP-, Bogotá, 1997.

Finalmente acudiendo a los PELC, se observa que el art. 1:102 al establecer la libertad contractual prescribe que “(1) *Las partes son libres para celebrar un contrato y establecer su contenido, dentro del respeto de la buena fe...*”, reforzando el contenido de esta disposición más adelante en el art. 1:201 “(1) *Cada parte tiene la obligación de actuar conforme a las exigencias de la buena fe. (2) Las partes no pueden excluir este deber ni limitarlo.*”

A través de una interpretación integral, consideramos que las disposiciones de los PELC antes citados al igual que ocurre con los PUNIDROIT, se configuran como reglas orientadoras de conducta que no se limitan únicamente a regir la vida del contrato, ya que su aplicación puede extenderse incluso al proceso de su formación.

2.2.2. Deber de información sobre el contenido del contrato.-

Como se ha tenido oportunidad de señalar, el deber de información en la etapa pre-contractual constituye una amplificación del principio-deber de la buena fe, por el cual “*En virtud de su reconocimiento el Profesional debe dar a conocer al potencial contratante de manera clara y comprensible no sólo las condiciones y calidades del bien o servicio que ofrece o se le demanda sino los riesgos y precauciones que ha de tener en cuenta.*”⁴⁰⁴

En este caso, todo lo atinente con el deber de información en la etapa pre-contractual según la legislación vista conjuntamente puede resumirse acudiendo a la jurisprudencia comparada, en la idea desarrollada así por la H. Corte Suprema de Justicia de Colombia, la cual consagró:

“...dentro de los deberes de corrección y lealtad que se exige a toda persona que emprenda tratos negociales se encuentra el que atañe con las informaciones o declaraciones que está llamado a suministrar, cuando a ellas hay lugar, en relación con el objeto, circunstancias o particularidades del acuerdo en camino de consumación, y cuya importancia,

⁴⁰⁴ Sergio Rodríguez Azuero, *Contratos Bancarios, su significación en América latina*, Bogotá, Legis, 5ª ed., 2003, p. 181 y ss..

si bien variable, resulta sustancial para efectos de desembarazar el consentimiento del destinatario de artificios o vicios que lo afecten”.⁴⁰⁵

En el Derecho Español aunque existe un vacío legal en la legislación civil, por cuanto no hay una consagración que expresamente atribuya el deber de información, éste se llena por la construcción doctrinal que hace referencia de la buena fe *in contrahendo*, cuando se está en las tratativas contractuales, ubicándose en “*aplicaciones particulares dispersas en el articulado del Código Civil (art. 1590, 1717, 1765 y 804), sobre la base del art. 1902 del Código Civil (...)*”.⁴⁰⁶

No obstante como se tiene estudiado previamente, el legislador español introdujo en su Derecho nacional el contenido de la Directiva 93/13/CEE sobre las cláusulas abusivas en los contratos celebrados con consumidores a través de la Ley sobre Condiciones Generales de la Contratación (LCGC). En ella se establece un régimen común para consumidores y otros adherentes (profesionales o personas jurídicas), pero se limita el régimen especial de las cláusulas abusivas al supuesto en que el perjudicado sea consumidor (sin perjuicio, claro está, de la posibilidad de impugnación judicial de una cláusula de un contrato celebrado entre profesionales cuando resulte contraria a la *buena fe*, conforme al régimen general de nulidades, tal y como lo plantea la propia Exposición de Motivos).⁴⁰⁷

Asimismo, de la lectura del art. 5.1 LCGC se establece que existe la obligación del predisponente de informar expresamente de la existencia de condiciones generales del contrato y facilitar al adherente un ejemplar de las mismas, pues caso contrario, no podrá entenderse que ha existido una aceptación de su incorporación al contrato.

⁴⁰⁵ Corte Suprema de Justicia, Sala de Casación Civil, Sentencia de Abril 4 de 2001, M.P. Jorge Antonio Castillo Rugeles; citado por Carlos Morales Guillén, *Código Civil concordado y anotado con arreglo a la edición oficial*, vol. I, La Paz, Gisbert, 1994, 4ª. ed., pp. 640.

⁴⁰⁶ José Luís De Los Mozos, *El Principio de la buena fe (sus aplicaciones prácticas en el Derecho Civil Español)*, Barcelona, Bosch, 1965, p. 223.

⁴⁰⁷ Al respecto, consultar: Pablo Gimeno Díaz de Aauri, *Las Cláusulas Abusivas en las Condiciones Generales de la Contratación, Regulación y Requisitos*, Cuaderno de Derecho Mercantil, Año 2. N° 6, Marzo de 2004, ubicada en: <http://www.latinlex.net/cuadernos/mercantil/numero6/cuamerinopi.html>

2.2.3. Contenido de la información.-

El PSC conforme analizaremos a continuación, con carácter previo al perfeccionamiento del contrato tiene como deber de conducta transmitir un mínimo de información de forma gratuita, por escrito o por vía electrónica (art. 18.b) LFE).

De entrada debemos señalar que en la certificación reconocida las reglas aplicables relativas a la información y oferta contractual, dependerán del tipo de contrato de certificación que se celebre así como de la tutela específica que se conceda - o no - al Firmante/Suscriptor, no obstante resultan aplicables como mínimo común las reglas generales contenidas en los Códigos civil y de comercio.

La certificación reconocida conforme se ha venido sosteniendo, se halla ordenada por medio de clausulados predispuestos a los que el contratante presta su adhesión y en los que prácticamente la capacidad de negociación es nula. Por consiguiente, la oferta contractual debe ser conforme con las disposiciones de la LCGC (arts. 1 y 2) y su contenido debe permitir que el Firmante/Suscriptor adherente, antes de la manifestación de su consentimiento haya tenido oportunidad efectiva de conocer de modo completo el condicionado (art. 5.1 LCGC).

Asimismo, de conformidad a las disposiciones del art. 18.b. LFE coincidentes con las establecidas en el inciso k) del Anexo II de la DFE, se establece una obligación de información previa a la emisión del certificado sobre una serie de aspectos relevantes, que permitirán al futuro Firmante/Suscriptor (y en su momento también a los Usuarios del certificado) determinar la fiabilidad y solvencia del PSC.

El objetivo principal de estas obligaciones es que con carácter previo a la emisión del certificado, y por consiguiente antes de la celebración del contrato de certificación reconocida, el Solicitante y futuro Firmante/Suscriptor tenga absoluto conocimiento entre otras cosas: de las características del certificado (método de identificación, límites de uso),

las obligaciones que asume (en especial, obligación de custodia y de revocación) y las características del PSC (v.gr. si ha obtenido certificaciones técnicas de conformidad con las disposiciones del art. 26 LFE); en definitiva, la información que proporcione el PSC al Solicitante resulta de vital importancia a efectos que éste tome una decisión fundada a momento de celebrar el contrato.

Pasemos a analizar de modo más detallado el contenido de las referidas obligaciones precontractuales de información.

i) Información sobre clausulados predispuestos y Prácticas de certificación.-

El PSC tiene como primerísimo deber de conducta debida desde el momento mismo del inicio de los tratos preliminares, el de informar al Solicitante y potencial Firmante/Suscriptor de la existencia de un clausulado predispuesto así como de la Declaración de Prácticas y Políticas de Certificación, debiendo además hacerle entrega gratuita de un ejemplar de los mismos, o en su caso, ponerlos a disposición para su consulta por medios electrónicos normalmente en la dirección URL del PSC. La redacción de la oferta deberá cumplir con los requisitos de transparencia, claridad, concreción y sencillez que con carácter general exige el art. 5.5. LCGC.

ii) Medidas de seguridad.-

El PSC también debe informar al Solicitante de las obligaciones que asumirá como Firmante/Suscriptor en función del contrato de certificación reconocida que celebrará, particularmente respecto de las medidas de seguridad que debe adoptar, como la obligación de custodia de la clave privada y el modo en que debe proceder para efectuar dicha custodia (art. 18.b.1.LFE).

Dichas medidas de seguridad pueden consistir en el empleo de un número de identificación personal (PIN o password) a objeto de acceder a la clave privada, también

pueden consistir en la utilización de técnicas más seguras y complejas, como la biometría a efectos de autenticación del usuario de la clave.⁴⁰⁸

Asimismo, se debe comunicar el procedimiento que se debe seguir para comunicar la pérdida o posible utilización indebida tanto de la clave privada, como de los dispositivos de creación y de verificación de firma que permitan la utilización de los datos de firma y el certificado expedido. Esta información resulta particularmente importante, toda vez que únicamente a partir de la cancelación del certificado queda exonerado el Firmante/Suscriptor de todo tipo de responsabilidad.⁴⁰⁹

En segundo lugar, el PSC debe poner en conocimiento del Solicitante respecto de los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo (art.18.b.2. LFE); es decir, no se refiere a actuaciones del Firmante/Suscriptor durante el ciclo vital del certificado sino a actuaciones posteriores relativas a la conservación fiable de un documento firmado electrónicamente, respecto de las que debe ser informado el Firmante/Suscriptor.

iii) Método empleado para comprobar la identidad.-

Por otra parte, se informará el método empleado por el PSC a momento de comprobar tanto la identidad del futuro Firmante/Suscriptor u otro tipo de datos que figuren en el certificado (art.18.b.3. LFE),⁴¹⁰ que para el caso de certificados reconocidos consiste en la personación física del Solicitante para comprobar su identidad. Si se trata de personas jurídicas, comprobar los datos relativos a la constitución y personalidad jurídica así como la

⁴⁰⁸ En todo caso el futuro Firmante/Suscriptor debe actuar con la diligencia debida exigible a un profesional, pues como empresario mercantil que es (individual o colectivo), hace uso de ella y del certificado con fines profesionales.

⁴⁰⁹ Al respecto la LMFE en su art. 9.1.d. (inciso v) establece que el PSC tiene el deber de proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera: “v) *si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1) del artículo 8 de la presente Ley.*”

⁴¹⁰ Con relación a este punto la LMFE en su art. 9.1.d. (inciso i) establece que el PSC tiene el deber de proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera: “i) *el método utilizado para comprobar la identidad del firmante.*”

extensión y vigencia de las facultades de representación del Solicitante, mediante los documentos públicos que sirvan para acreditar los extremos citados (art. 13 LFE).⁴¹¹

iv) Condiciones y límites de empleo del certificado.-

Asimismo, las condiciones precisas de utilización del certificado y sus posibles límites de uso deben ser obligatoriamente informadas (art. 18.b.4. LFE), pues no olvidemos que aunque en principio un certificado es válido para uso general, el PSC puede limitar cuantitativa o cualitativamente su empleo, ya sea a iniciativa propia (con la intención de limitar su posible responsabilidad) o a petición del Solicitante (v.gr. cuando se emiten certificados transaccionales que sirven para una o varias operaciones en concreto).

Nótese que de estos extremos debe estar informado no sólo el Solicitante (en el caso de límites establecidos unilateralmente por el PSC) sino también a su debido momento el Usuario del certificado, pues el PSC se exonera de responsabilidad por el empleo distinto al previsto y/o que vayan más allá de los límites establecidos. Por esta razón y por su importancia para el Usuario del certificado es que dichos límites forman parte del contenido mínimo obligatorio de un certificado reconocido, conforme lo establecido en el art. 11.2.h. LFE.⁴¹²

En ese sentido también es posible *inferir* este deber (si bien no es una obligación conforme se plasma en el texto) del art. 10.d. LMFE, la cual señala que para establecer la fiabilidad de los servicios que presta el PSC podrá tenerse en cuenta “*la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste*”.

⁴¹¹ Esta información reviste particular valor sobre todo para los Usuarios del certificado, pues permite establecer el nivel de seguridad del certificado a momento de autenticar la identidad del Firmante/Suscriptor; de manera que resulta de importancia que no únicamente el Firmante/Suscriptor sino también el Usuario del certificado conozcan esta situación, a objeto de evaluar la fiabilidad del certificado.

⁴¹² Con relación a este punto la LMFE en su art. 9.1.d. (inciso ii) establece que el PSC tiene el deber de proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera: “*ii) cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado.*”

v) Garantías.-

A las mencionadas se añade la obligación de informar respecto a la forma en que el PSC garantiza su responsabilidad patrimonial, que en el caso de PSC que emiten certificados reconocidos consiste en una garantía obligatoria de al menos 3.000.000 de euros (art. 20.2. LFE); información que evidentemente resulta relevante para que los Solicitantes y en su momento los Usuarios del certificado establezcan la solvencia del PSC, frente al riesgo de responsabilidad por daños y perjuicios que podrían ocasionarse por el uso de los certificados que expiden.

vi) Certificaciones técnicas obtenidas.-

Por otra parte resultará particularmente importante que el Solicitante se encuentre informado a momento de tomar una decisión para contratar, sobre las certificaciones técnicas que haya obtenido el PSC de conformidad con las disposiciones del art. 26 LFE, o incluso, respecto de las certificaciones que poseen los dispositivos seguros de creación de firma electrónica con los que el PSC opera, de conformidad con lo establecido en el art. 27 LFE.⁴¹³

También es posible *inferir* este deber (si bien no es una obligación conforme se plasma en el texto) del art. 10.f. LMFE, la cual señala que para establecer la fiabilidad de los servicios que presta el PSC podrá tenerse en cuenta “*la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden*”. De modo que si el PSC cuenta con una certificación debe informarlo a sus potenciales clientes.

vii) Procedimientos para resolución extrajudicial de conflictos.-

Asimismo, el Solicitante debe conocer los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir durante la prestación del servicio de certificación (art.18.b.5. LFE). En ese sentido, la realidad del tráfico nos

⁴¹³ En este sentido la Exposición de Motivos de la LFE al explicar los beneficios del nuevo sistema de certificación (acreditación) de los PSC enfatiza que “*El nuevo régimen nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica...*”

demuestra que por lo general los PSC prefieren optar por incorporar una cláusula arbitral en el contrato de certificación, de manera que ante el surgimiento de una desavenencia entre las partes como consecuencia de la ejecución del contrato, el litigio se somete a decisión de un árbitro cuyo laudo deviene en vinculante para las partes. De hecho, la Disposición adicional undécima LFE establece que los usuarios y prestadores de servicios de certificación podrán someter los conflictos que se susciten en sus relaciones al arbitraje.

Esta previsión se encuentra también contenida en el art. 32 de la LSSI, el cual dispone que el prestador y el destinatario de servicios de la SI se encuentran facultados para someter sus divergencias a los arbitrajes previstos en la legislación de arbitraje, así como a los procedimientos de resolución extrajudicial de conflictos que se instauren por medio de códigos de conducta u otros instrumentos de autorregulación (art. 32.1. LSSI); en estos casos, la Ley faculta el empleo de medios electrónicos en los términos que establezca la normativa específica (art.32.2. LSSI).

viii) Información sobre precios.-

Otra información que resulta importante que el PSC proporcione es la referida a los precios o tarifas que cobra por sus servicios, debiendo comunicar qué tipo de servicios son cobrados y cuáles no; los PSC suelen cobrar fundamentalmente por la emisión del certificado, en tanto que los restantes servicios vinculados como servicios de suspensión o revocación de certificados, servicios de directorio y/o consulta sobre vigencia de certificados, etc. normalmente no se encuentran sujetos a precio alguno.

En el caso de los que sí se hallan sujetos a un precio debe informarse respecto de los montos exactos exigidos, siendo desde nuestro punto de vista de utilidad en ese sentido el art. 10.1.f. LSSI que obliga al prestador a brindar: *“información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables...”*.

Cabe analizar la incidencia que la LCGC posee sobre el precio. Conforme se estudió previamente la referida norma establece una regulación sobre las condiciones generales de los contratos y sus límites, conteniendo un régimen legal al efecto, de aplicación en todas las ocasiones e independientemente de la naturaleza del sujeto que contrata, a cualquier relación contractual donde exista una o varias condiciones generales.

Ello nos lleva a cuestionarnos si es posible entender como condición general una imposición previa a la relación contractual - por parte del PSC al Solicitante - de que el precio de los servicios que está a punto de contratar va a ser establecido de una concreta forma. Y si ello fuera así, las incidencias que los límites introducidos en el texto legal pudieran tener en la materia.

Actualmente la LCGC en cuanto a la protección que contiene hacia el sujeto que contrata bajo condiciones generales, se extiende a cualquier persona, física o jurídica. Por ello, y a priori, podemos afirmar que el ámbito de aplicación incluye todas las relaciones de prestación de servicios profesionales como la que estamos estudiando, siempre que exista en ellas condiciones generales. La imposición del precio por parte del PSC, bien directamente, bien por remisión a baremos profesionales o por cualquier otra forma o criterio de determinarlo a posteriori, es o puede aparecer, como una condición general de la contratación siempre y cuando presente los caracteres que la ley exige para ellos.

Como sabemos la LCGC define las condiciones generales no por su contenido sino por su forma de presentarse (son cláusulas pre-redactadas), y por dos datos objetivos fácilmente constatables: son impuestas por una de las partes (es decir, no negociadas) y tienen la finalidad de ser incorporadas a la generalidad de contratos que lleve a cabo el profesional. El contenido de las mismas (es decir si se refiere a elementos esenciales, accidentales, accesorios) es un tema que al legislador, en principio, le parece irrelevante para calificar una determinada cláusula como condición general o no.

Así, señala la norma que ni la autoría material del clausulado, ni la apariencia externa, ni la extensión, ni “*cualesquiera otra circunstancia*” (art. 1.1. LCGC) son cuestiones que afecten al concepto de condiciones generales. Solamente es tenido en cuenta el contenido del contrato - en cuanto a la materia o rama del Derecho que afecte - en el art. 4 LCGC, relativo a los contratos excluidos del ámbito de aplicación de la ley. Por último, el artículo 5.1 LCGC establece que cuando se acepten, las condiciones generales pasarán a formar parte del contrato, y, por tanto, gozarán del efecto obligatorio propio de todo contrato.

Por consiguiente entendemos que nada impide poder considerar la imposición del precio por parte del profesional, utilizando para ello la fórmula de pre-redactarlo, como una condición general del contrato de prestación de servicios.⁴¹⁴ Partiendo de esta afirmación razonaremos a continuación sobre las consecuencias jurídicas que se derivan de ella.

En primer lugar, el PSC debe informar sobre la existencia de la condición general relativa al precio facilitando al Solicitante y futuro Firmante/Suscriptor el conocimiento de la misma. Así, en el caso de que el precio se impusiera con relación a los precios usuales que rigen en el mercado de certificados electrónicos, el PSC deberá facilitar éstos, e incluso, explicar su contenido si fuese de difícil entendimiento para el cliente debido a su desconocimiento del lenguaje técnico-jurídico. No olvidemos que las condiciones generales “*deberán ajustarse a los criterios de transparencia, claridad, concreción y sencillez*” (art. 5.4 de LCGC).

En segundo lugar, y para el supuesto que los requisitos enunciados no se cumplieren, la nulidad de la *cláusula precio* presentada bajo la forma de condición general ilegal, arrastraría la nulidad del contrato en su integridad según lo dispuesto en el art. 9 LCGC, dado que el precio es un elemento esencial del contrato.

⁴¹⁴ En este sentido se pronuncia la autora Cervilla, quien sostiene que no existe impedimento legal alguno para admitir la posibilidad de que el profesional oferte sus servicios al cliente, imponiéndole el precio de éstos, lo que desde su punto de vista, configura una auténtica condición general de la contratación (M. Cervilla, 2001: 212 y ss.).

ix) Otras informaciones.-

No obstante todo lo señalado hasta el momento, cabe reparar en el hecho que la formación del consentimiento contractual no está ordenada únicamente mediante las normas a las que se ha hecho referencia, sino que también es posible analizar otras disposiciones que rigen la conducta del PSC que actúa profesionalmente en el mercado de la certificación.

En ese entendido consideramos que resultan siendo igualmente aplicables, en tanto que el PSC es un auténtico Prestador de Servicios de la Sociedad de la Información,⁴¹⁵ las normas generales contenidas en la LSSI, particularmente el art. 10 que se corresponden con las obligaciones de información exigidas por el art. 5 de la DCE.

Entre estas disposiciones cabe resaltar que de conformidad con el art. 10 LSSI, el PSC está obligado a proporcionar los medios que permitan a los destinatarios del servicio acceder por medios electrónicos de forma permanente, fácil, directa y gratuita a un mínimo de información (art.10.1 LSSI), obligación que se tendrá por cumplida si el prestador incluye dicha información en su página o sitio de Internet (art. 10.2 LSSI).

La información que mínimamente debe proporcionar consiste en: i) su nombre o denominación social; ii) su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; iii) su dirección de correo electrónico y cualquier

⁴¹⁵ Al respecto consideramos importante hacer una observación (y aclaración), en sentido que resulta llamativo al estudiar las obras de los diferentes autores españoles que se ocupan de la temática del comercio y las firmas electrónicas, éstos denotan prácticamente de modo generalizado una marcada tendencia a efectuar un análisis por separado del contenido de la normativa que los regula, sin que medie un esfuerzo integrador de las disposiciones que hacen a ambas materias, particularmente cuando se ocupan de abordar el estudio de las obligaciones y responsabilidades de los Prestadores de Servicios de Certificación (PSC), a quienes para su análisis los encasillan en las disposiciones españolas y comunitarias sobre firma electrónica y, pareciera que se olvidan, que como Prestadores de Servicios de la Sociedad de la Información (SI) que son, también les resultan de aplicación las normas españolas y comunitarias que regulan los servicios de la SI, de manera que el lector iniciado en el tema tiene la impresión que respecto de los certificadores sólo resultan de aplicación las Leyes y Directivas de firma electrónica, quedando reservadas para los que proporcionan un servicio de intermediación (*tales como operadores de redes de telecomunicaciones y proveedores de acceso, los que realizan copia temporal de los datos solicitados por los usuarios, los que efectúan alojamiento o almacenamiento de datos o los que facilitan enlaces a contenidos o instrumentos de búsqueda*) las disposiciones que hacen a los servicios de la SI, olvidándose desde nuestro punto de vista, que los PSC constituyen verdaderos prestadores de servicios precisamente de esa SI, con lo cual, les resultarán también de aplicación en cuanto corresponda las disposiciones generales de la Ley 34/2002 (LSSI) y la Directiva 2000/31/CE (DCE). Según Llanea, tanto la relación de servicios incluidos como la de los excluidos en la LSSI “no es exhaustiva y no excluyente: son todos los que están, pero no están todos los que son.” P. Llanea González, “LSSI: día cero”, *Noticias Jurídicas*, Madrid, Bosch, oct.-nov./2002, p. 34.

La excepción a la regla la encontramos -sin que ello quiera decir que son los únicos- al consultar los siguientes trabajos: M. Jesús Moro Almaraz, “Servicios de la sociedad de la información y sujetos intervinientes”, en M. Jesús Moro Almaraz, comp., *Autores, consumidores y comercio electrónico*, Madrid, Colex, 2004, pp. 120-122; quien identifica tres clases de prestadores de servicios de la SI, a saber: i) proveedores de contenidos y servicios, ii) proveedores de servicios de certificación, y iii) proveedores de servicios de intermediación propiamente; además cita a autores como Aparicio, quien considera que los PSC constituyen un “especial tipo de proveedor de servicios en línea”, o Illescas, que los califica de “especial prestador de servicios de intermediación”, razón por la cual Moro concluye en sentido que si bien la regulación específica de los certificadores corresponde a la LFE, les resultan también aplicables las normas de carácter general de la LSSI. En idéntico sentido se pronuncia Apol-Lònia Martínez Nadal, quien entiende que dentro del concepto genérico de prestador de servicios de la SI “tiene cabida, como especie, el prestador de servicios de certificación” (A. Martínez, 2004: 281-282).

otro dato que permita establecer con él una comunicación directa y efectiva; iv) los datos de su inscripción en el Registro Mercantil; v) el número de identificación fiscal que le corresponda; vi) los códigos de conducta a los que en su caso esté adherido y la manera de consultarlos electrónicamente.

Sinopsis.-

Conforme venimos sosteniendo con relación a la información que el PSC se encuentra obligado a ofrecer al interesado en adquirir un certificado reconocido, ésta debe extenderse a todos los extremos del contrato y que se encuentran incorporados en modelos estandarizados, y desde luego debe poner a disposición la Declaración de Prácticas de Certificación así como las Políticas de Certificación asociadas al certificado reconocido.

Además comprendemos que una conducta leal del PSC en los tratos preliminares, demanda que dicha información sea puesta a disposición de los potenciales clientes sin que éstos se la requieran o la soliciten expresamente, independientemente que constituya una obligación *ex lege* (art. 18.b) LFE), ya que su actuación debe derivar de la buena fe (art. 57 C.com. y 1.258 C.c.).

El deber de información que recae sobre el PSC en la fase previa al contrato, como amplificación del principio-deber de la buena fe, es de trascendental importancia. Primero, porque ayuda al Solicitante y futuro Firmante/Suscriptor a tener un adecuado conocimiento de: las condiciones en que se presta el servicio, sus derechos y obligaciones, las medidas de seguridad que debe adoptar, etc., cuyo conocimiento cabal podría desencadenar finalmente la no prestación del consentimiento por su parte.

Segundo, porque en la medida que el Solicitante tenga toda la información clara y comprenda perfectamente las implicancias de la prestación del servicio, podrá comparar los servicios que se ofrecen en el mercado, los precios, ventajas y desventajas a objeto de tomar

una mejor dedición respecto a que PSC le conviene, así como formará su voluntad de modo consciente y con conocimiento de causa.

2.2.4. Oferta vinculante.-

Consideramos asimismo, que tras determinadas comprobaciones que denotan por parte del Solicitante y potencial Firmante/Suscriptor su intención sería de estar dispuesto a contratar, como por ejemplo el envío de su pre-solicitud de certificado a la dirección de Internet del PSC, determina que este último quede obligado, debiendo considerarse que existe una oferta vinculante e irrevocable de contrato.

Así, debe considerarse que la oferta tendrá un plazo de validez indeterminado, excepto cuando que medien circunstancias extraordinarias o no imputables al PSC, teniendo éste la carga de la prueba de la concurrencia de tales circunstancias; en tanto que las consecuencias de la revocación improcedente serán, en el orden comercial: el mantenimiento de la oferta por el tiempo que restaba; en el orden civil: la reparación de los daños y perjuicios que la conducta del PSC haya provocado en el cliente.

Precisamente sobre este particular debemos reparar que la LFE presenta un vacío normativo, toda vez que no establece el régimen jurídico aplicable a la oferta en la contratación del servicio de certificación. Ante esta evidencia existen dos posibilidades para llenar dicho vacío, acudir a las normas generales del derecho privado (C.c. y C.com.) o apoyarnos en normas que tengan relación con la materia, en procura de orientación y certeza. Desde nuestro punto de vista, en ambos casos además podemos hacer uso supletorio de los principios generales del derecho de obligaciones y contratos.

Al respecto, si decidimos acudir a las normas generales del derecho privado nos encontramos con que el C.com. omite toda referencia; en tanto que el C.c. hace una parca

mención en su art. 1.262 que resulta a todas luces insuficiente para resolver la problemática planteada.⁴¹⁶

Consideramos que lo adecuado y oportuno es acudir a la LSSI, que constituye una norma específica que hace a la materia y por consiguiente de preferente aplicación a las normas generales. Así, en su art. 27.3. especifica que sin menoscabo de las normas establecidas en la legislación específica, “*las ofertas o propuestas de contratación realizadas por vía electrónica serán válidas durante el período que fije el oferente o, en su defecto, durante todo el tiempo que permanezcan accesibles a los destinatarios del servicio*”.

Si bien es evidente que la disposición comentada se encuentra contenida dentro del Título IV de la LSSI, donde se regula específicamente la contratación por vía electrónica, consideramos que las normas del citado art. 27 resultan aplicables por extensión al contrato de certificación reconocida, toda vez que aunque la contratación no siempre se perfecciona por medios electrónicos - como se tiene apuntado - es innegable que existen fases del *iter* contractual, concretamente en el periodo de formación del contrato que se producen en línea, siendo una de ellas precisamente la referida a la oferta contractual que está contenida en el sitio de Internet o URL del PSC, constituyendo por consiguiente desde nuestro punto de vista una verdadera oferta realizada por medios electrónicos.⁴¹⁷

Por ello razonamos que resultan también aplicables - salvando las distancias que corresponden y de manera auxiliar - las obligaciones previstas en el art. 27.1., particularmente los incisos a) y c) de la LSSI, por las cuales el prestador de servicios debe informar al destinatario de manera clara, comprensible e inequívoca y antes de iniciar el

⁴¹⁶ Así lo reconoce Díez-Picazo cuando señala “*El art. 1.262 CC es un precepto insuficiente. Se limita a hablar, en general, de oferta y de aceptación sin definir ninguno de estos términos, ni puntualizarlos y, sobre todo, sin aludir para nada su régimen jurídico, lo que obliga a integrar las insuficiencias del Código con materiales traídos de otras partes. La materia relativa a la llamada “formación del contrato”, que ha determinado una amplia producción estudios en el Derecho anglosajón, tal vez por influencia de una muy extendida jurisprudencia, ha sido objeto de especial al tratamiento en algunos campos de Derecho uniforme, cuya utilidad para la integración de nuestro Código en esta materia está, a nuestro juicio, fuera de duda.*” (L. Díez-Picazo, 1996: 281).

⁴¹⁷ La temática de la oferta contractual por medios electrónicos es analizada en el artículo de Antonio José Santander Rengifo, “La Oferta al Público por Internet: Una visión desde la Doctrina del Derecho Civil”, en *REDI: Revista Electrónica de Derecho Informático*, No. 79, Perú, Alfa-Redi, febrero/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=977> // En igual sentido el trabajo de Lisette Hernández Fernández, “La oferta y la aceptación. Especial referencia a los contratos celebrados por medios electrónicos”, en *REDI: Revista Electrónica de Derecho Informático*, No. 76, Cuba, Alfa-Redi, noviembre/2004, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1037>

procedimiento de contratación, sobre los siguientes aspectos: a) los distintos trámites que deben seguirse para celebrar el contrato; y c) los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos. Disposiciones que se corresponden con las contempladas en el art. 10 incisos a) y c) de la DCE.

Con relación a este último requisito, no olvidemos que en el proceso de solicitud de un certificado el interesado accede al sitio web del PSC a través de su dirección URL, donde se le requiere introducir ciertos datos como su DNI, NIF, NIE o CIF (caso de personas jurídicas) en el punto de recogida de datos dispuesto para ello. Posteriormente se generarán las claves Pública y Privada (*en Tarjeta criptográfica o en el navegador*) que serán vinculadas al Certificado, al mismo tiempo que se asigna al interesado un código de solicitud, procedimiento eminentemente complejo que requiere de la debida información por parte del PSC.

Igualmente aplicable consideramos que resulta el art. 27.4. LSSI que se corresponde con el art. 10.3. DCE, por los cuales se dispone que de manera previa al inicio del procedimiento de contratación, el prestador de servicios se encuentra en la obligación de poner a disposición del destinatario las condiciones generales a las que se encuentra sujeto el contrato, de tal forma que las mismas puedan ser almacenadas y reproducidas por el destinatario; en el caso concreto de la certificación reconocida, dichas condiciones generales de la contratación deben ser ubicadas por el Firmante/Suscriptor en la Declaración de Prácticas y Políticas de Certificación del PSC, quien tiene el deber de hacerlas accesibles, al menos por vía electrónica y de modo gratuito (art. 19 LFE).

También reflexionamos que si se hace un análisis cuidadoso, en realidad, los problemas derivados de la fase formativa del contrato de certificación reconocida no difieren sustancialmente de los que se suscitan, en general, en la contratación mercantil internacional.

Para la solución de esas cuestiones que se pueden plantear durante la fase de formación del contrato, el Derecho uniforme del comercio internacional cuenta con dos instrumentos de uniformación, por un lado, la Convención de Viena sobre Compraventa Internacional de Mercaderías de 1980 (CVCIM)⁴¹⁸ y, por otro, los ya mencionados Principios UNIDROIT⁴¹⁹ cuyas soluciones en materia de formación del contrato pueden aplicarse a los contratos de certificación reconocida, máxime si se tiene en consideración que la CVCIM ha sido objeto de un instrumento de adhesión del Estado español en 17 de julio de 1990 y su texto, como parte integrante en el Derecho español, fue publicado en el BOE el 30 de enero de 1991.

Los principios que pueden inducirse de la Norma vienesa en su Capítulo II - que regula la formación del contrato - pueden extenderse analógicamente para solventar los problemas que plantean ciertas estipulaciones que de manera sistemática incorporan los clausulados contractuales de las compañías certificadoras. Tampoco puede olvidarse que el contrato de certificación reconocida se celebra sobre la base de clausulados contractuales que vienen a configurar al detalle la disciplina de la relación contractual.

En concreto, los arts. 14 al 24 CVCIM norman de modo bastante preciso la formación del contrato de venta internacional de mercaderías. Aunque en la CVCIM estas normas tienen

⁴¹⁸ La temática de los problemas que hacen a la formación del contrato tuvo gran evolución, especialmente en el Derecho norteamericano, que se concretó finalmente en el Código de comercio unificado. Asimismo, la intención de generar normas uniformes en el Derecho de la compraventa internacional de mercaderías, dio lugar a una serie de trabajos que, bajo la conducción de la CNUDMI o en inglés UNCITRAL, culminó en un texto definitivo que se sometió a una conferencia internacional celebrada en Viena en 1980 y fue aprobada como Convenio de las Naciones Unidas, el cual se conoce como Convenio de Viena. Al respecto consultar (L. Díez Picazo, 1996: 281).

⁴¹⁹ Los Principios de UNIDROIT se ocupan con algún detalle del régimen jurídico de los clausulados contractuales. Sobre el particular, el primer precepto que los “Principios” destinan a la regulación de los clausulados contractuales es el artículo 2.19, donde su primer apartado dispone la aplicación de las reglas generales sobre formación del contrato cuando se incorporan al mismo clausulados contractuales, en tanto que el apartado segundo de la norma define los denominados *standard terms*. La consecuencia de la aplicación de las reglas generales sobre formación del contrato contenidas en los “Principios” -arts. 2.1 a 2.22- plantea el tema de la aceptación del clausulado contractual por la parte adherente. La alusión a las normas sobre formación del contrato en el artículo 2.19 (1) quiere significar la necesidad de la aceptación del adherente, bien sea ésta explícita o implícita. Ahora bien, la aceptación implícita del adherente resulta admitida de forma restrictiva. En este sentido, se considera que la incorporación implícita de las condiciones generales al contrato sólo se produce, de un lado, si obedece a una práctica negocial de las partes -*course of dealing*- o, de otro lado, si la contratación mediante clausulados contractuales representa un uso difundido y regularmente observado por las partes en el sector económico concernido -v. arts. 1.8 y 4.3 - La versión inglesa de los “Principios” define en su artículo 2.19 (2) a los clausulados contractuales como “... *provisions which are prepared in advance for general and repeated use by one party and which are actually used without negotiation with the other party*”. Se trata de un concepto que recoge los elementos característicos desde un punto de vista objetivo de las definiciones de condiciones generales más usuales en el Derecho comparado: la contractualidad, la predisposición y la imposición (Sobre estos elementos objetivos de la noción de condiciones generales de la contratación y sobre la función que desempeña la definición legal de las mismas, ver J. Alfaro Aguilera-Real, *Las condiciones generales de la contratación*, Madrid, Civitas, 1991, pp. 112 y ss. // También, M. Ruiz Muñoz, *La nulidad parcial del contrato y la defensa de los consumidores*, Valladolid, Lex Nova, 1993, pp. 267-270). Tal concepto abarca, por su propia ubicación sistemática en los “Principios” - Capítulo II, sobre la formación del contrato - también a las cláusulas referentes a la celebración del contrato, destinadas a producir efectos antes o en la celebración del mismo.

por objeto la formación de contratos de venta internacional, conforme defiende Díez-Picazo “*nada impide, y, lejos de ello, todo aconseja, que sus normas sean tenidas en cuenta para integrar la parvedad del art. 1.262 CC y resolver de este modo los problemas generales de formación del contrato mediante oferta y aceptación cualquiera que sea la naturaleza del contrato en cuestión*”.⁴²⁰ Resultan igualmente informativos los arts. 11 a 24 del Código Europeo de Contratos (CEC) y los arts. 2.201 a 2.211 de los PELC.

En consecuencia, tomaremos en cuenta el contenido y los principios de los referidos documentos para procurar construir el régimen de la oferta en los contratos de certificación reconocida.

En primer lugar y llegados a este punto, es preciso señalar que resulta fundamental distinguir las verdaderas ofertas de las simples invitaciones a ofertar.⁴²¹ Podemos indicar que una declaración dirigida a la celebración de un contrato de certificación reconocida tendrá valor de oferta, si contiene todos los requisitos del contrato a realizar o las indicaciones suficientes en cuanto a la posibilidad de determinar el contenido, de manera que pueda ser objeto de una aceptación pura y simple, y si además expresa - al menos implícitamente - la voluntad del PSC (autor de la oferta) de considerarse como obligado en caso de aceptación por parte del Firmante/Suscriptor (arts. 13.1. CEC; 14.1 CVCIM; 2.1.2. PUNIDROIT; 2.201. PELC).

Por consecuencia, la declaración del PSC que no se encuentre conforme a las condiciones señaladas o que, dirigida a personas indeterminadas presente el carácter de

⁴²⁰ (L. Díez-Picazo, 1996: 280 y ss.).

⁴²¹ Como bien hace notar Miranda la CVCIM se decanta por entender que la oferta, para ser tal, ha de ir dirigida a una o varias personas determinadas, sentando la regla presuntiva de que las propuestas destinadas al público en general no pueden categorizarse jurídicamente como verdaderas ofertas negociales, sino como simples invitaciones a ofrecer, señalando al respecto que “*El asunto, lejos de tener un mero interés teórico o dogmático, reviste trascendencia práctica, toda vez que en el moderno tráfico comercial no es infrecuente que los empresarios dirijan sus propuestas comerciales al público en general, siendo relevante en tales casos dilucidar si tales propuestas constituyen meras invitaciones a ofrecer o se trata, en cambio, de genuinas ofertas negociales. A nadie se ocultan las muy diversas consecuencias jurídicas que se derivan de una y otra solución. Si se consideran meras invitaciones a ofrecer, los empresarios proponentes siempre tienen manos libres para decidir su vinculación negocial una vez se emitan declaraciones de voluntad conformes con sus propuestas. En cambio, si reciben la consideración de genuinas ofertas de contrato, quedan vinculados contractualmente con quienes acepten sus propuestas negociales.*” Luis María Miranda Serrano, *La aplicación en el derecho español no uniforme de la noción de oferta de contrato de la Convención de las Naciones Unidas sobre la Compra Venta Internacional de Mercaderías: en torno a las ofertas a personas indeterminadas*, Proyecto de Investigación Veinticinco años de Derecho de los consumidores: análisis legal y propuestas de modernización (referencia DER 2010-16204), financiado por el Ministerio de Ciencia e Innovación (IP: Prof. Dr. Luis María Miranda Serrano), Madrid, 2010, p.3 // Sobre este temática también consultar (L. Díez-Picazo, 1996: 282).

mensaje publicitario, no constituye una oferta y no es susceptible por tanto de ser aceptada por el Firmante/Suscriptor. En todo caso constituirá una invitación para ofertar (art. 13.2. CEC; 14.2 CVCIM).

Desde este punto de vista y toda vez que la oferta del PSC se encuentra en un medio abierto como lo es Internet, por consecuencia dirigida a un número indeterminado de potenciales clientes, debemos asumir que se configura como una oferta pública que es eficaz mientras no sea revocada, rechazada o se extinga (art. 14.2 CEC; 2.1.3. PUNIDROIT). En todo caso, la oferta únicamente puede revocarse mientras el destinatario no haya expedido la aceptación (arts.15.1. CEC; 16.1. CVCIM; 2.1.4. PUNIDROIT; 2.202.1. PELC). Por contramano, la oferta es ineficaz mientras no llegue a su destinatario y puede hasta entonces ser retirada por su autor, incluso frente a quien no la ha conocido (arts. 14.1 y 22 CEC; 15.2. CVCIM).

Finalmente en función de la disposición del art. 27.3. LSSI, que hace referencia al periodo de validez de la oferta, consideramos que la misma se torna irrevocable cuando el PSC se obliga expresamente a mantenerla durante un cierto periodo de tiempo, o si, sobre la base de negocios precedentes realizados entre las partes, de tratos preliminares, del contenido de cláusulas o de la costumbre, se puede razonablemente reputar como tal (arts. 17 CEC; 16.2 CVCIM; 2.1.4. (2) PUNIDROIT; 2.202. (3) PELC).

2.2.5. Deberes de información y conducta del Solicitante.-

Así como surgen una serie de obligaciones pre-contractuales para el PSC, se manifiestan para el Solicitante también una serie de deberes de información y conducta pre-contractuales. El principio-deber de *Buena fe* trae aparejado consigo el deber de información cierta, de manera que el Solicitante se encuentra obligado a proporcionar toda la información requerida por el PSC, misma que debe ser veraz y entregada dentro de los términos fijados para ello.

Tanto en ocasión de digitar sus datos en la presolicitud *on line* como a momento de aproximarse ante la ER, debe suministrar la información necesaria para realizar una correcta y plena identificación (art. 23.1.a. LFE), garantizando la exactitud y veracidad de la información proporcionada.

En el caso de certificados que se emiten a nombre de personas jurídicas, el Solicitante se encuentra obligado a responsabilizarse de la custodia de la clave privada asociada a dicho certificado. Por otra parte, recae sobre el Solicitante la carga de notificar cualquier cambio en los datos aportados para la creación del certificado.

De igual modo debe actuar con la intencionalidad tal, que denote su auténtico interés por obtener un certificado reconocido y en consecuencia por perfeccionar un contrato de certificación, no cabiendo un comportamiento *animus jocandi*,⁴²² es decir, con propósito de burla, jocosidad o broma sino que debe mediar una intención seria y formal de perfeccionar el contrato.

Por último, el Solicitante deberá acudir personalmente ante la ER a objeto de: acreditar y confirmar su identidad, efectuar conjuntamente la Solicitud del certificado reconocido que requiere y cumplimentar el contrato de certificación reconocida.

2.2.6. Responsabilidad pre-contractual.-

En nuestra investigación no nos detendremos a analizar la responsabilidad pre-contractual, por cuanto consideramos que únicamente sería responsable el PSC en el hipotético caso que se originaran daños a la contraparte, ya sea por la no celebración del contrato de certificación reconocida o se rompan brusca e injustificadamente los tratos preliminares, violando con ello la confianza.

Adscribiéndonos al razonamiento sostenido por la autora Pérez, este tipo de responsabilidad no es frecuente en el ámbito de actividad del PSC como tampoco - en general - en la órbita del Derecho español, concluyendo en sentido que si se llegase a plantear, se

⁴²² (C. Morales, 1994: 602 y ss.)

solucionaría en todo caso aplicando las normas generales sobre responsabilidad precontractual, toda vez que no existe especialidad alguna para el PSC.⁴²³

III. Perfeccionamiento y ejecución del contrato.-

3.1. (Etapa IV) Adhesión a cláusulas generales y Registro.-

El Solicitante debe personarse ante el PSC o la ER delegada a objeto de formalizar la solicitud de certificado reconocido y cumplimentar propiamente el *Contrato de Prestación de Servicios de Certificación Reconocida*,⁴²⁴ procediendo de esta forma la adhesión del Solicitante al contrato y condiciones generales pre-formulado por el PSC, lo que conlleva además su implícita adhesión a la Declaración de Prácticas de Certificación y las Políticas de Certificación asociadas al certificado reconocido solicitado (*procedimiento off line*).⁴²⁵

De forma paralela y simultánea el PSC o la ER delegada procederán a identificar al Solicitante, quien deberá aportar los datos que se le requieran y acreditará su identidad personal, en caso de tratarse de persona física. En el caso de certificados reconocidos de personas jurídicas y los que reflejan una relación de representación voluntaria, se comprobará los datos relativos a la constitución y, en su caso, personalidad jurídica así como a la extensión y vigencia de las facultades de representación del Solicitante, ya sea directamente mediante los documentos públicos que sirvan para ello o a través de tercero, acudiendo para ello al Registro Mercantil en el caso de sociedades mercantiles o cualquier otro registro público correspondiente.⁴²⁶

⁴²³ (M. Pérez, 2009: 207).

⁴²⁴ Conforme sostiene Devoto “*El primer y único contacto cara a cara de la autoridad de certificación con el titular del par de claves se verifica antes del proceso de emisión del certificado, cuando el interesado suscribe la solicitud, siempre que este requisito conste en la política de emisión de certificados. De allí en más su función es pasiva, sin relación directa con su cliente y con los documentos que éste suscribe.*” Mauricio Devoto, *Comercio electrónico y firma digital. La regulación del ciberespacio y las estrategias globales*, Buenos Aires, La Ley, 2001, p. 213.

⁴²⁵ La personación del Solicitante no será indispensable si la firma en la solicitud de expedición de un Certificado ha sido legitimada en presencia notarial (sin perjuicio de la necesidad de acreditar suficientemente la extensión y vigencia de sus facultades de representación, en el caso de personas jurídicas), o cuando la identidad u otras circunstancias permanentes de los solicitantes y/o firmantes constaran previamente al PSC, de conformidad con lo dispuesto en el art. 13.4. inc. a) y b) LFE.

⁴²⁶ El art. 13 LFE en los numerales 2 y 3 respectivamente, establece que la citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los mencionados datos, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

En cualquiera de los casos, el encargado de acreditación verificará que los documentos aportados cumplen todos los requisitos para confirmar la identidad del Solicitante (y de la entidad que éste representa en caso de certificados emitidos para personas jurídicas), procediendo a registrarlo en lo que se configura como un “Servicio de registro”.

Es a partir de esta etapa que el Solicitante (o la entidad que éste representa en caso de certificados emitidos para personas jurídicas) pasa a denominarse propiamente “Firmante/Suscriptor”, o en términos del art. 6.2. de la LFE “*Firmante*”.

3.2. (Etapa V) Envío de información al PSC.-

La ER procederá a validar los datos y a enviarlos junto con el código de solicitud obtenido en su momento por el Solicitante en la fase de presolicitud. Esta transmisión de información al PSC debe efectuarse mediante comunicaciones seguras establecidas para tal fin entre la ER y el PSC (*procedimiento on line*).

3.3. (Etapa VI) Emisión del certificado.-

Una vez recibidos por el PSC los datos personales del Firmante/Suscriptor así como el código de solicitud obtenido en la fase de presolicitud, se procederá a la emisión del certificado reconocido, lo que supone la generación de documentos electrónicos que confirman la identidad del Solicitante y Firmante/Suscriptor, así como su correspondencia con la clave pública asociada (*procedimiento off line*).

Acto seguido, el PSC por medio de su propia firma electrónica reconocida autentica el certificado debiendo emplear mecanismos criptográficos que doten de autenticidad e integridad al certificado, con el fin de evitar la manipulación de la información contenida en el mismo (*procedimiento off line*).

3.4. (Etapa VII) Composición del nombre distintivo (DN) del Firmante/Suscriptor.-

Con los datos personales del Solicitante recogidos durante el proceso de solicitud del certificado, se procede a componer el nombre distintivo (DN) del Firmante/Suscriptor

conforme al estándar X.500, asegurando que dicho nombre tenga sentido y no dé lugar a ambigüedades. Normalmente no se contempla el uso de seudónimos como forma de identificación del Firmante/Suscriptor, aunque la misma está permitida por el art. 11.e) LFE cuando se trata de personas físicas.

Una vez compuesto el nombre distintivo (DN) que identificará al Firmante/Suscriptor, se crea la correspondiente entrada en el directorio, asegurando como se tiene dicho que el nombre distintivo sea único en toda la ICP del PSC (*procedimiento off line*).

3.5. (Etapa VIII) Publicación del certificado.-

Una vez generado el certificado por parte del PSC se publicará en el directorio y/o servicio de consulta-verificación sobre vigencia de certificados (art. 18. incs. c) y d) LFE), concretamente en la entrada correspondiente al nombre distintivo (DN) del Firmante/Suscriptor. Si en el proceso de solicitud el Solicitante proporcionó una dirección de correo electrónico, normalmente se le enviará una comunicación de la disposición de su certificado para su descarga (*procedimientos on line*).

3.6. (Etapa IX) Descarga e instalación del certificado.-

Transcurrido el tiempo establecido desde que el Solicitante se apersona en la ER (o ante el propio PSC) para acreditar su identidad, y una vez que el certificado haya sido generado, se pone a disposición del Firmante/Suscriptor un mecanismo de descarga de certificado en la dirección URL del PSC accediendo a la opción “*Descarga del Certificado*” (*procedimiento on line*).

En este proceso guiado se le pedirá al Firmante/Suscriptor que introduzca el número identificativo con el que realizó el proceso de presolicitud (DNI, NIF, CIF, etc.), así como el código de solicitud devuelto por el sistema al finalizar dicho proceso. Si el certificado no ha sido aún generado por cualquier motivo, se le indicará este hecho en el momento que intente su descarga.

Si el certificado ya ha sido puesto a disposición del Firmante/Suscriptor, éste será introducido en el soporte en el que se generaron las claves durante el proceso de presolicitud (*Tarjeta criptográfica del PSC o soporte convencional de almacenamiento de software a través del navegador*).

3.7. (Etapa X) Aceptación o rechazo del certificado.-

Aceptación expresa.- El Firmante/Suscriptor debe comprobar todos los datos contenidos en el certificado. Si no tiene observaciones procederá a aceptar el certificado haciéndolo saber al PSC, caso contrario, lo rechazará y el PSC deberá revocar el certificado para emitir uno nuevo (*procedimiento on line*).

Aceptación tácita.- Si el Firmante/Suscriptor empieza a hacer uso del certificado se considera que media una aceptación tácita del contenido del mismo (*procedimiento on line*).

3.8. (Etapa XI) Empleo del certificado.-

Con el certificado reconocido aceptado por el Firmante/Suscriptor (de modo expreso o tácito), éste puede empezar a emplearlo para efectuar actos de comercio electrónico y/o contratación electrónica (*procedimiento on line*).

3.9. (Etapa XII) Comprobación del estado del certificado.-

Tanto el Firmante/Suscriptor del certificado reconocido como los terceros Usuarios del certificado podrán a partir de este momento realizar la comprobación del estado de un certificado en la forma y condiciones que se expresan en las Prácticas de Certificación del PSC (*procedimiento on line*). Las posibilidades para dicho fin consisten fundamentalmente en alguna de las siguientes: generación y publicación de las Listas de Revocación de Certificados (LRC); los servicios de consulta y validación de Certificados mediante OCSP.

3.10. Ciclo vital del certificado.-

Como es sabido a cada certificado electrónico o digital se le asigna un periodo de validez contractualmente, el cual no puede ser superior al dispuesto por la LFE y debe ser

adecuado a las características y tecnología empleada para generar los datos de creación de firma; en todo caso, cuando se trata de certificados reconocidos dicho período no puede ser superior a cuatro (4) años (art. 8.2. LFE).

Este periodo marca el tiempo durante el cual se espera que el certificado sea válido, pero la legislación prevé una serie de circunstancias que determinan la suspensión (art. 9 LFE)⁴²⁷, revocación a solicitud del titular (art. 8.1.b. LFE)⁴²⁸ y extinción (art. 8 LFE)⁴²⁹ del certificado.

Con relación al momento a partir del cual la extinción de la vigencia de un certificado electrónico surte efectos respecto de terceros, la legislación española dispone que en los supuestos de expiración del período de validez del certificado, la extinción opera desde el instante en que se produce esta circunstancia y, con relación a los demás casos, desde el momento que la indicación de la referida extinción se publique en el servicio de consulta sobre vigencia de certificados, el cual debe ser puesto a disposición de los usuarios por parte del PSC (art. 8.3. LFE), servicio que como se tiene referido es ofrecido en línea a través de la LRC o el servicio OCSP.

⁴²⁷ El art. 9.1. LFE dispone en el numeral 1) que los PSC suspenderán la vigencia de los certificados electrónicos expedidos, cuando se verifique alguna de las siguientes causales: a) solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica; b) resolución judicial o administrativa que lo ordene; c) la existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c) y g) del artículo 8.1; y d) cualquier otra causa lícita prevista en la declaración de prácticas de certificación. El art. 8.1 señala: c) Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero; g) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad. De otra parte, el numeral 2) de la disposición analizada, con relación al momento a partir del cual surte plenos efectos la suspensión de un certificado, establece que el mismo se produce desde el instante en que la suspensión es incluida por el PSC en el servicio de consulta sobre la vigencia de certificados.

⁴²⁸ El art. 8.1.b. LFE establece que la revocación debe ser formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

⁴²⁹ El art. 8.1. LFE establece como causas de extinción de la vigencia de un certificado electrónico, incluidos obviamente los certificados reconocidos: a) la expiración del período de validez que figura en el certificado; b) revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica; c) violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del PSC o utilización indebida de dichos datos por un tercero; d) resolución judicial o administrativa que lo ordene; 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, terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica; f) cese en la actividad del PSC, salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro PSC; g) alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad; y finalmente h) cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

Para concluir con el análisis de la normativa española, adelantamos en señalar que el art. 10 LFE establece una serie de disposiciones comunes a la extinción y suspensión de la vigencia de certificados electrónicos, que se constituyen en deberes que recaen sobre el certificador, las cuales serán analizadas con detenimiento a momento de estudiar las obligaciones del PSC.

IV. Contenido del contrato de certificación reconocida.-

Destinaremos el presente acápite inicialmente al análisis del contenido del contrato de certificación reconocida, del que devienen una serie de obligaciones (y en consecuencia derechos) contractuales tanto para el PSC como para el Firmante/Suscriptor.

Posteriormente nos ocuparemos del estudio de las obligaciones que atingen al Usuario del certificado, las cuales si bien no tienen su origen en el contrato de certificación reconocida, resultan de imprescindible consideración a objeto de integrarlas en la comprensión a cabalidad del contrato objeto de estudio.

En todo caso es necesario reparar previamente sobre los siguientes aspectos: la LFE no se ocupa de regular explícitamente los deberes del Firmante/Suscriptor así como tampoco los del Usuario del certificado, a diferencia de lo que ocurre con el PSC, para quien dedica de forma más o menos meticulosa varios artículos que señalan sus obligaciones y específicamente dos artículos para abordar la temática de la responsabilidad (art.22 LFE) y los límites a la responsabilidad (art. 23 LFE) del PSC (sin agotar no obstante la materia), articulado del cual se pueden inferir ciertas obligaciones que recaen sobre el Firmante/Suscriptor y el Usuario del certificado.

No obstante y en todo caso habrá que recurrir a efectuar una interpretación integral del texto normativo, para que a partir de esta operación coliguemos en qué consisten dichos deberes, pues conforme hace notar Martínez a momento de analizar específicamente el contenido del art. 23 LFE:

“...aun cuando no sea su finalidad principal, es posible hallar, una enumeración de obligaciones y deberes de los firmantes y terceros usuarios, siquiera de forma indirecta, a efectos de establecer los supuestos de exoneración de responsabilidad de los prestadores de servicios de certificación (que van vinculados al incumplimiento de tales obligaciones y deberes por parte de firmantes y terceros usuarios).”⁴³⁰

En todos los casos, la incorporación a un contrato de dichas prerrogativas y prestaciones así como de otras no mencionadas en la LFE, tendrá como consecuencia que se configuren en derechos y obligaciones contractuales, siendo el contrato ley entre las partes. Pero si alguna o algunas de éstas no fueran incorporadas expresamente en un contrato, entonces se configuran en verdaderos derechos y obligaciones legales, siendo de imprescindible observancia por todos los sujetos intervinientes por constituir la LFE una norma de naturaleza imperativa.

4.1. Parámetro de la obligación y diligencia profesional.-

La obligación fundamental del PSC es la de proceder con la debida diligencia profesional que demanda su actividad certificadora.⁴³¹ Es decir, debe conducirse de conformidad con la *lex artis* (leyes del arte) que hacen a su oficio.

A objeto de comprender a cabalidad que significado encierra el concepto de diligencia acudiremos al auxilio de la doctrina, así, conforme apunta Díez-Picazo “*En un sentido vulgar o usual diligencia significa esfuerzo, cuidado y eficacia en la ejecución de alguna actividad...Sin embargo, con el tiempo...pasa a significar la compleja actividad que una persona debe o tiene que desplegar en una situación jurídica dada. F. De Castro señaló que*

⁴³⁰ (A. Martínez, 2004: 335, 383).

⁴³¹ Con relación al grado de diligencia exigible a los PSC, Martínez señala que ni el Real Decreto-ley 14/1999 (que hablaba simplemente de «la debida diligencia») ni la directiva comunitaria (que se refiere meramente a la no negligencia) contienen previsión expresa respecto de esta cuestión, no obstante -sostiene- debía considerarse que la debida diligencia exigible a un prestador de servicios de certificación no es simplemente la diligencia media sino de un nivel superior, dado su condición de profesional (A. Martínez, 2004: 349). En el mismo sentido Apol-Lònia Martínez Nadal, *La ley de firma electrónica*, Madrid, Civitas, 2000, pp.284-288 // Igualmente se pronuncia Rodríguez, quien afirma que el grado de diligencia que ha de exigirse al PSC debe ser la que corresponde con la conducta del profesional, artífice o perito, y no la simple diligencia del buen padre de familia contemplada en el art. 1.104 Cc. (M. Huerta y D. Rodríguez, 2001: 132).

*se trata de un “modelo de conducta”, al que los usos sociales dotan de contenido efectivo”.*⁴³²

A su turno, el art. 1.104 C.c. dispone que *“La culpa o negligencia del deudor consiste en la omisión de aquella diligencia que exija la naturaleza de la obligación y corresponda a las circunstancias de las personas, del tiempo y del lugar. Cuando la obligación no exprese la diligencia que ha de prestarse en su cumplimiento, se exigirá la que correspondería a un buen padre de familia.”*

Ahora bien, cuando el deudor del *facere* es un profesional en la materia la diligencia exigida se eleva, es decir, no es idéntica a la que se exigiría a un sujeto no perito en el cumplimiento de la actividad (*la de un buen padre de familia*). Cuando el prestador es profesional dichas circunstancias influyen en el contenido de la obligación, de tal manera que la diligencia requerida para que la prestación se entienda cumplida, no es la misma de ser cualquier otro sujeto el deudor de dicha actividad.

De este modo se exigirá al profesional la diligencia media: i) según la naturaleza de la obligación (*la obligación será fundamentalmente una prestación de hacer derivada de un contrato de servicios, en el supuesto que nos ocupa*); ii) sus circunstancias personales (*el PSC es un profesional en la materia cuyos servicios ofrece, y por ese motivo ha sido contratado para ello*); y iii) las concretas circunstancias de tiempo y lugar en que la obligación hayan de cumplirse exijan. Y esta diligencia-tipo es la diligencia media que un buen profesional, en atención a los conocimientos (técnicos o científicos) que emplea en el cumplimiento del concreto *facere* y según los condicionamientos externos en que la actividad se desarrolla.

El PSC que concierta con el Firmante/Suscriptor un contrato de certificación reconocida, en base al cual se obliga con su acreedor a suministrarle unos medios (sus conocimientos y prácticas de la profesión en cuestión), incumplirá dicha obligación si los medios puestos a disposición del cliente no son acordes con las reglas que el mercado de la

⁴³² (L. Díez-Picazo, 1996: 95).

certificación exige.

Para determinar si la obligación ha sido o no cumplida, será necesario establecer si el *facere* se ha llevado a cabo con la diligencia media consistente en adecuarlo a las reglas empresariales que debe dominar y conocer un certificador medio (*lex artis*) situadas en un contexto temporal y espacial determinado (*ad hoc*).

Así, la seguridad y fiabilidad (*lex artis*) como criterio valorativo de la diligencia exigible al PSC, opera a lo largo de todo el ciclo vital del certificado reconocido (contexto temporal) en el mercado interior europeo (contexto espacial) desde su emisión, pasando por una posible suspensión, su revocación o extinción (*ad hoc*).

En este sentido siguiendo a Cervilla podemos definir la *lex artis* por las siguientes notas: i) es una regla de medición o valoración de una conducta; ii) en base a criterios objetivos; iii) de naturaleza técnica; iv) cuyo contenido se establecerá en función del acto concreto de la actividad profesional cuya diligencia se trata de calibrar, así como de las concretas circunstancias de la empresa-profesional, y de tiempo y lugar en las que el *facere* se lleva a cabo.⁴³³

No implica la infalibilidad del PSC sino simplemente la adecuación de su actividad a la diligencia patrón del buen padre de familia, que en este caso podría denominarse del buen profesional, y que se establece según las reglas de su concreto oficio, adaptadas a las concretas circunstancias que rodean al cumplimiento de la obligación.

En ese sentido, el art. 22.1. pfo. segundo LFE establece de manera expresa esta previsión cuando señala: “*La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.*” (las negrillas y subrayado son nuestros).

⁴³³ (M. Cervilla, 2001: 135).

De esa manera en los supuestos de responsabilidad por culpa, el PSC responde a no ser que pruebe su diligencia profesional. Por esta razón Rodríguez hace notar la importancia que para el PSC posee el registro y la documentación de sus actividades.⁴³⁴

La LMFE contempla esta carga en su art. 9.1.b. al señalar que es deber del PSC “actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales”.

En conclusión podemos afirmar que al PSC - como prestador de un servicio que reviste notoria complejidad técnica - se le exige una diligencia profesional, tanto para determinar el cumplimiento de la obligación como para posteriormente imputar o no un posible incumplimiento (es decir como criterio para establecer si sobrevinieron los sucesos de imprevisibilidad e inevitabilidad, básicos para apreciar caso fortuito o fuerza mayor liberatoria), y que se valorará según las reglas concretas de su profesión adaptadas a las circunstancias específicas que concurren en el cumplimiento de la obligación.⁴³⁵

En todo caso, el Firmante/Suscriptor tiene derecho a recibir por parte del PSC un servicio que esté acorde con los más fiables niveles de seguridad y los estándares de calidad debidos. No nos olvidemos que la certificación es una actividad que se sujeta a las reglas de la libre oferta y demanda del mercado, por lo que la competencia entre los distintos PSC obliga a que estos fidelicen a sus clientes, y ello únicamente se puede conseguir brindando servicios de óptimas características.

Con las consideraciones introductorias anotadas, pasemos al análisis en detalle.

⁴³⁴ Conforme sostiene Rodríguez, toda la información y documentación relativa a un certificado deberá ser registrada durante un período de 15 años, al objeto de que se pueda utilizar como medio de prueba de la certificación en el ámbito de una reclamación o procedimiento judicial; prosigue señalando que en el ámbito material, los documentos relacionados con el certificado abarcan desde la solicitud de su emisión, hasta los datos identificativos del solicitante y los documentos que haya aportado para acreditar su identidad, y los propios datos del contenido del certificado (M. Huerta y D. Rodríguez, 2001: 125-126). En idéntico sentido (M. Pérez, 2002: 948).

⁴³⁵ Al respecto Cervilla precisa que “La concreción de la existencia o no de diligencia en una concreta actuación, a fin de apreciar o no la existencia de culpa, con las consecuencias que ello lleva consigo, es una labor jurisprudencial, por lo que, en esta materia, la labor de los Tribunales ha sido la que ha ido perfilando el concepto de *lex artis ad hoc*, elaborado a partir del art. 1104 del CC.” (M. Cervilla, 2001: 136-137).

4.2. Obligaciones del PSC.-

4.2.1. Obligaciones principales.-

El PSC posee dos prestaciones absolutamente necesarias o fundamentales, las cuales pasamos a estudiar a continuación:

i) Emisión y entrega del certificado reconocido.-

Una de las obligaciones principales del PSC sin duda alguna consiste en generar y poner a disposición del Firmante/Suscriptor el certificado reconocido, debiendo observar los siguientes aspectos:

A momento de generar el certificado reconocido:

El PSC debe cumplir todas las formalidades debidas y seguir los procedimientos técnicos y de seguridad necesarios, asegurándose que el certificado se encuentre debidamente consignado con toda la información correctamente registrada, estipulando con claridad y certeza los datos y otras circunstancias del Firmante/Suscriptor, particularmente deben estar consignados en el certificado todos los elementos necesarios que hacen a un certificado reconocido.

El PSC en ningún caso debe incluir en el certificado información distinta de la acordada, ni circunstancias, atributos específicos del Firmante/Suscriptor o límites económicos y/o de empleo del certificado diferentes a los pactados.

La emisión del certificado supone la generación de documentos electrónicos que confirman la identidad del Solicitante y Firmante/Suscriptor, así como su correspondencia con la clave pública asociada, razón por la cual, dicha emisión de certificados únicamente puede realizarla el certificador en su calidad de Prestador de Servicios de Certificación, no existiendo ninguna otra entidad u organismo con capacidad de emisión de dichos documentos. En ese entendido debe quedar claro que las ER delegadas no emiten bajo

ninguna circunstancia certificados, solo coadyuvan con el PSC en la administración de los mismos.

A tiempo de generarlo, el PSC debe además autenticar el certificado por medio de su propia firma electrónica reconocida. Por otro lado y con el fin de evitar la manipulación de la información contenida en el mismo, el PSC debe emplear robustos mecanismos criptográficos que doten de autenticidad e integridad al certificado.

En cualquier caso el PSC debe actuar diligentemente para: no ignorar hechos notorios que puedan afectar a la fiabilidad del certificado; asegurarse que el nombre distintivo (DN) asignado en el certificado sea único en toda la ICP del PSC.

A momento de entregar el certificado reconocido al Firmante/Suscriptor:

El PSC tiene el deber de poner a disposición del Firmante/Suscriptor el certificado reconocido por medio de canales tecnológicos absolutamente fiables y seguros, conforme los procedimientos que se han explicado previamente (apartado 2.1.2.).

Con todo, cáigase en cuenta que tan sólo el certificado no satisface el servicio útil, el propósito global e integral del contrato de certificación reconocida, a lo sumo, satisface la *auto-identificación* del Firmante/Suscriptor, pero evidentemente sin ninguna utilidad práctica.

Evidentemente, recordemos que el fin último buscado con el contrato, que es la identificación cierta y segura Firmante/Suscriptor en una red de comunicación abierta, no se logra únicamente con la emisión y entrega del certificado sino que éste debe ser publicado por el PSC en un directorio de consulta por parte de terceros, a objeto que accedan a la clave pública asociada al certificado, con la cual llevaran a cabo la validación de la clave privada del Firmante/Suscriptor, lo cual únicamente se consigue con la prestación de un servicio ulterior de consulta sobre vigencia o verificación de certificados.

En otras palabras, la utilidad del servicio no se traslada al Firmante/Suscriptor únicamente con la emisión y puesta a disposición del certificado por parte del PSC, por tanto,

la prestación principal del PSC no se limita simplemente a emitir y entregar el certificado sino que se encuentra consustancialmente vinculada con otra prestación principal, la cual pasamos a estudiar.⁴³⁶

ii) Mantener un directorio y garantizar un servicio de consulta de certificados.-

Conforme hemos venido argumentando, la segunda prestación principal del PSC indisolublemente ligada con la anterior, consiste en mantener un directorio actualizado de certificados en el que deben figurar los certificados que efectivamente han sido emitidos, con la indicación respecto a si se encuentran vigentes o si han sido objeto de una suspensión o extinción (art. 18.c. LFE), garantizando paralelamente el acceso a un servicio expedito de consulta sobre la vigencia o verificación de los certificados (art. 18. d. LFE). En ambos casos, tanto la integridad del directorio como la seguridad del servicio de consulta, deben resguardarse por medio del empleo de óptimos mecanismos tecnológicos de seguridad.

El modo en el que normalmente el PSC cumple con las obligaciones que nos ocupan en este apartado, consiste en proporcionar las siguientes aplicaciones:

ii.1.) Generación y publicación de las Listas de Revocación de Certificados (LRC).-

El PSC procede a habilitar listas de los certificados revocados (LRC)⁴³⁷, por un plazo equivalente al de validez teórica del certificado en el momento de su emisión.

La LRC es un fichero firmado digitalmente por un PSC según el estándar RFC 5280,⁴³⁸ en los que incluye la lista de certificados emitidos que por algún motivo han dejado

⁴³⁶ Con relación a la noción de servicio útil, traemos a colación el análisis de Villanueva, quien sostiene "...el acreedor de una obligación de puro hacer encuentra la utilidad en el servicio que recibe. Es decir, la obligación de hacer se resuelve en algo más que la actividad en sí misma considerada: es servicio útil prestado de acuerdo con la diligencia debida en cada supuesto." (C.Villanueva, *El servicio...*,2009:294). Más adelante continúa razonando la referida autora en sentido que "El *facere* en los servicios está orientado hacia la consecución de un resultado útil para el acreedor. Por lo mismo, el servicio debe resultar para el acreedor y el deudor algo más que actividad en sí misma considerada. Así, en concreto, el servicio se considera como actividad en sí misma útil y productora de beneficios y ayudas para el acreedor o destinatario de la prestación...no tiene sentido una obligación en la cual no sea debido un comportamiento productor de una utilidad destinada al acreedor. Si en la obligación disociamos dos elementos relacionados funcionalmente como el medio y la finalidad, el primero de estos elementos, el medio, estará representado por el comportamiento debido, que constituye el contenido de la obligación; el segundo elemento, la finalidad o resultado, que representa una utilidad para el acreedor, será el objeto o el contenido del derecho de crédito. La satisfacción del interés del acreedor se logra sobre la consecución o el cumplimiento de ese derecho de crédito. En definitiva, el bien debido es lo que satisface el interés de la prestación, y no la prestación como comportamiento. Esto es, el objeto de la prestación está configurado por la conducta o comportamiento debido por el deudor, pero la satisfacción del interés del acreedor y el cumplimiento de la obligación por el deudor se concitan sobre el bien debido." (C. Villanueva, *El servicio...*,2009: 322-323).

⁴³⁷ En el idioma inglés de las conoce como CRL "Certificate Revocation List".

⁴³⁸ Para validar una firma electrónica o un certificado digital es necesario seguir los procedimientos descritos en el estándar RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

de ser válidos de manera previa a la expiración de su periodo de validez original. La forma de publicar este fichero depende de cada PSC y debe estar descrita en su DPC.⁴³⁹

Al expirar el período originario de validez de un certificado éste deja de estar listado en las LRC. Normalmente se publican con una periodicidad máxima de veinticuatro (24) horas, y tienen una validez asimismo de veinticuatro (24) horas.⁴⁴⁰

Para saber si un certificado es de confianza, se debe proceder a comprobar si el Número de Serie del mismo está incluido en la LRC publicada por la autoridad de certificación emisora. Si es así, el certificado ha sido revocado y no es de confianza.

ii.2.) Servicio de consulta y validación de Certificados mediante OCSP.-

Por otra parte, el PSC facilita la consulta de certificados a través de un servicio de consulta y validación de certificados mediante OCSP (*Online Certificate Status Protocol - Protocolo de Estado de Certificado en Línea*),⁴⁴¹ el cual proporciona a los usuarios y las aplicaciones, un método ágil y rápido para conocer la validez de un determinado certificado digital en un momento dado, realizando una consulta *online* a un servidor OCSP y evitando de esa forma tener que descargar la Lista de Certificados Revocados (LRC).

El interesado realiza una petición de validación según la norma RFC 2560⁴⁴² a la URL del PSC, obteniendo como respuesta una evidencia digital firmada por el propio PSC sobre la validez de un certificado, lo que permite obtener una evidencia electrónica sobre la respuesta generada.

De modo resumido el servicio funciona de la siguiente manera: el servidor OCSP verifica la firma de la petición OCSP efectuada por un interesado y comprueba el estado de los certificados, emitiendo a continuación una respuesta de OCSP informando acerca del

⁴³⁹ Procedimiento de consulta del estado de los Certificados.- Si el interesado no posee acceso a las LRC, dispone de una aplicación en la dirección URL de Internet del PSC a través de la cual y previa autenticación con sus datos de creación de firma (clave privada), se le informará acerca del estado de su certificado.

⁴⁴⁰ El perfil de estas listas normalmente sigue los estándares de la Recomendación UTI-T X.509 versión 2.

⁴⁴¹ El Protocolo OCSP constituye un protocolo de comunicaciones estándar que permite realizar una consulta sobre el estado de un certificado concreto y obtener una respuesta por parte de una Entidad de Validación.

⁴⁴² RFC 2560 "*Online Certificate Status Protocol – OCSP*".

estado en el que se encuentran en ese momento los certificados incluidos en la petición (vigente, suspendido o extinguido).⁴⁴³ El PSC habitualmente no almacenará copias de las peticiones de validación a menos que se contrate previamente un *Servicio de custodia de peticiones de validación*.

Además, resulta oportuno añadir que los PSC suelen ofrecer adicionalmente un *Servicio de búsqueda y descarga de certificados* desde su página Web. La búsqueda de certificados puede realizarse por el E-mail o por el Número de Serie del certificado. Como resultado se obtendrán los certificados que coincidan con el criterio de búsqueda, mostrando su estado actual (vigente, suspendido o extinguido). La utilización de este servicio es pública y normalmente gratuita, destinada a facilitar a los usuarios la obtención de los certificados de otros usuarios con los que desean comunicarse de manera segura.

Con relación al tema, Martínez subraya que desde el punto de vista material parecen articularse dos instrumentos distintos: un directorio de certificados y un servicio de consulta sobre la vigencia de los mismos; aun cuando en algún momento parece que el legislador español confunde ambos elementos o les da un tratamiento unitario, de forma que no queda claro - argumenta - si son dos instrumentos distintos, como parece deducirse de su previsión en dos apartados diferentes o bien si existe un instrumentos único, el directorio, siendo el que el servicio de consulta simplemente una forma de acceso al mismo.⁴⁴⁴

En todo caso e independientemente de la interpretación que se haga de las disposiciones señaladas, lo importante es que el servicio de consulta cumple un papel de especial trascendencia, toda vez que a efectos de extinción o suspensión de la vigencia de certificados, la LFE vincula su eficacia anticipada frente a terceros, no a la inclusión en el directorio sino precisamente en el servicio de consulta, es decir, cuando es posible su

⁴⁴³ En las DPC normalmente se refieren a la entidad que presta este servicio como Autoridad de Validación (VA), que es un Prestador de Servicios de Certificación que proporciona certeza sobre la validez de los certificados digitales y sobre los documentos firmados electrónicamente en un momento dado.

⁴⁴⁴ (A. Martínez, 2004: 284).

conocimiento efectivo por parte de terceros, de conformidad con las disposiciones del art. 8.3. LFE (en el caso de extinción, mas no en el caso de expiración del periodo de validez del certificado, que opera desde que se produce dicha circunstancia) y el art. 9.2. LFE (para el caso de suspensión de certificados) respectivamente, debiendo el PSC hacer constar cualquiera de estas situaciones de modo indubitado en el servicio de consulta sobre vigencia de certificados (art. 10.1. LFE).

En ese sentido, entendemos que la disposición del art. 18.c. LFE de mantener un directorio de certificados hace referencia a la obligación de crear y mantener un registro de certificados, es decir, una base de datos de certificados que debe ser accesible por medios telemáticos a través del servicio de consulta dispuesto por el art. 18.d. LFE, disposiciones que encuentran su paralelo en el inc. b) Anexo II de la DFE.

Como práctica comercial habitual, el PSC debe hacer públicamente accesible la información sobre el estado y vigencia de los certificados que ha emitido, así como de las listas de certificados que se encuentran revocados. El fin de este registro es, en principio, colocar los certificados a disposición de los Usuarios de los mismos a objeto de ser empleados para la verificación de la firma digital del Firmante/Suscriptor, de modo que se constituyen en un mecanismo eficiente para la distribución de certificados, los cuales pueden ser consultados en línea “*on line*”;

De igual forma, la publicación de la fecha de revocación tiene por objetivo hacer de conocimiento del Usuario de clave pública, que no puede confiarse en los certificados afectados. Nótese en consecuencia, que el registro resulta siendo el elemento fundamental para la adecuada operatividad de una Infraestructura de Clave Pública (ICP) en una comunidad abierta, puesto que es el punto central de información para todas las aplicaciones de la entidad certificadora.

Igualmente, de la revisión de la LMFE podemos encontrar que las obligaciones del PSC anteriormente referidas están previstas en el art. 9.1. incisos c) y d).⁴⁴⁵

Por otra parte, conforme afirma Martínez no hay acuerdo sobre si la publicación de certificados debería ser obligatoria o simplemente voluntaria, tomando en cuenta que un registro de certificados constituye un archivo de datos privados, ya que el certificado a más de contener una secuencia numérica (la clave pública del titular), usualmente también incluye información personal del Firmante/Suscriptor, caso de los certificados de atributos, razón por la que su inclusión en un directorio de acuerdo con la legislación española y comunitaria sobre protección de datos, debería ser autorizada por su tenedor (v.gr. a momento de efectuar la solicitud); toda vez que es posible que el Firmante/Suscriptor no desee la publicación de sus datos privados.⁴⁴⁶

En ese sentido, el RDL 14/1999 derogado contenía una previsión expresa al igual que la DFE (apartado I., inciso tercero, del Anexo II)⁴⁴⁷, al establecer en su art. 11.e. que al registro de certificados “*podrá accederse por medios telemáticos y su contenido estará a disposición de las personas que lo soliciten, cuando así lo autorice el signatario*”. Tal previsión ha desaparecido en la actual LFE, introduciendo el legislador español la creación del denominado servicio de consulta respecto del que no existe exigencia alguna de consentimiento. En todo caso consideramos que resulta de aplicación a la actividad del PSC la normativa de protección de datos personales, tal como se establece en el art. 17 LFE.

⁴⁴⁵ El art. 9.1. de la LMFE señala la obligación del PSC de:

c) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) proporcionar... (información respecto de)

iii) si los datos de creación de la firma son válidos y no están en entredicho;

⁴⁴⁶ (A. Martínez, 2004: 287). En el mismo sentido se pronuncia Rodríguez afirmando que “...es preciso destacar que la disponibilidad para terceros del registro sólo operará cuando lo autorice el signatario...y que encuentra su apoyo en que se está ante una modalidad de protección de datos personales.” (M. Huerta y D. Rodríguez, 2001: 116) // Igualmente (M. Pérez, 2002: 948).

⁴⁴⁷ El inc. 3ro., apartado I), Anexo II de la DFE señala que los PSC debe utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que: los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado.

También debemos considerar que de la interpretación integral de la LFE y más concretamente del art. 20.1.g., el cual señala que el PSC debe utilizar sistemas fiables para almacenar certificados reconocidos que “...*restringan su accesibilidad en los supuestos o a las personas que el firmante haya indicado...*” podemos concluir que en el derecho español la publicación de certificados debe hacerse previo consentimiento del Firmante/Suscriptor, aunque evidentemente no es una previsión general, por lo menos debemos entender que el Firmante/Suscriptor se reserva el derecho a restringir el acceso al certificado en los casos o a los sujetos que considere convenientes.

4.2.2. Obligaciones específicas.-

El PSC que emite certificados reconocidos, al margen de cumplir las obligaciones generales que se establecen para todo certificador (expidan o no certificados reconocidos), se encuentra obligado a cumplir una serie de obligaciones específicas, las cuales podemos clasificar en dos sub-categorías: i) obligaciones previas a la emisión del certificado reconocido, básicamente reflejadas en los arts. 12 y 13 LFE; y ii) obligaciones a tiempo de emitir un certificado reconocido, contenidas en el art. 20 LFE. De ellas precisamente nos ocuparemos en los dos acápites subsiguientes.

4.2.2.1. Previas a la emisión del certificado reconocido.-

El PSC que emite certificados digitales reconocidos, se encuentra obligado a cumplir básicamente cuatro obligaciones previas a la emisión efectiva del certificado. A continuación explicaremos en qué consisten efectuando las matizaciones pertinentes.

i) Comprobación de identidad de los solicitantes.-

El primerísimo y más importante de los deberes de todo PSC que expide certificados reconocidos con carácter previo a su efectiva emisión, consiste en comprobar y asegurarse la identidad y otras circunstancias personales de los solicitantes de certificados reconocidos (art.

12.a. LFE; inc. d) Anexo II DFE) de conformidad con el procedimiento y disposiciones previstas por Ley (art. 13 LFE).

El PSC puede efectuar los procedimientos y acciones de comprobación de identidad por sí mismo o por medio de otras personas físicas o jurídicas, públicas o privadas (art. 13.5. LFE), constituyendo la segunda posibilidad la regla cuando el PSC actúa prestando sus servicios en comunidades geográficamente dispersas, ocasión en la que entran en juego las Entidades de Registro (ER), con las que normalmente el PSC suscribe un contrato o mantiene un acuerdo (o finalmente es una entidad que forma parte de la estructura empresarial del propio PSC), para que éstas a nombre, por cuenta y en representación del PSC procedan a efectuar determinadas labores que hacen a las actividades de certificación, siendo una de ellas precisamente la comprobación en la identidad y otras circunstancias de los solicitantes. En todo caso y a todos los efectos el PSC asume responsabilidad por las actividades llevadas a cabo por la ER delegada.

Sostenemos que la identificación indubitada de los solicitantes constituye la obligación de mayor importancia y trascendencia del PSC, ya que, repárese en el hecho que todo el sistema de seguridad y confianza que gira en torno a una Infraestructura de Clave Pública (ICP), descansa finalmente en que los distintos sujetos implicados puedan tener la certeza absoluta respecto de la identidad de la persona que ha firmado electrónicamente un documento y que respalda su firma electrónica con un certificado reconocido, el cual contiene su clave pública, en base al cual el receptor del mensaje procederá a validar la correspondiente clave privada, con lo que, de complementarse el juego de claves se produce la autenticación de la identidad del emisor, lo que finalmente deviene en la generación de la debida certeza, seguridad y confianza entre las partes.

Por consiguiente, el momento vital de todo el ciclo que hace a la vida de un certificado reconocido, reside precisamente en la ocasión en que el PSC comprueba y se

cerciora de la identidad y otras circunstancias del solicitante del certificado reconocido, pues una indebida identificación o un error en el proceso trae aparejado como consecuencia, el derrumbamiento de todo tipo de seguridad y confianza en el sistema tecnológico, amén de las responsabilidades que surgen como consecuencia de ello.

Por las razones expuestas el PSC debe asegurarse por todos los medios razonables y a su alcance, de que quien solicita un certificado reconocido es efectivamente quien dice ser. Ahora bien, efectivamente puede darse el caso que un solicitante se presente portando documentos identificativos y/o acreditativos de representación falsificados, situación que nos coloca ante el análisis de quién asume la responsabilidad en caso que el certificado sea no obstante emitido y con su empleo fraudulento se ocasionen daños a terceros.

Al respecto, debemos señalar que el PSC se encuentra obligado a comprobar los datos identificativos que le proporcionan los solicitantes con la debida diligencia, que como se tiene dicho, no es una diligencia media sino una verdadera diligencia profesional, debiendo acudir a todas las instancias a su alcance para verificar la identidad del solicitante, incluyendo el caso de personas jurídicas, para lo cual debe recabar información de los registros públicos donde éstas se hallen inscritas (v.gr. Registro Mercantil en caso de Sociedades Mercantiles).

Con lo cual, si el PSC demuestra que empleó la diligencia que se espera de él - dada la condición profesional en que ejerce su labor - y no obstante se emitió el certificado, entonces se exonera de la responsabilidad por los posibles daños que puede traer aparejado el uso fraudulento del certificado; pero caso contrario, es decir, cuando no procedió con la debida diligencia en la comprobación de los datos identificativos de un solicitante, debe asumir las consecuencias del daño que el empleo fraudulento del certificado pueda ocasionar a terceros, entre ellos, la persona suplantada en su identidad y la persona que confió en el certificado (por la apariencia creada que lo llevó a actuar en consecuencia).

En ese sentido, salvo que la firma en la solicitud de expedición de un certificado reconocido haya sido legitimada en presencia notarial - situación en la que puede prescindirse de la personación - en todos los demás casos la identificación de la persona física que solicite un certificado reconocido demanda que ésta se presente ante el PSC o la ER delegada, quienes deben proceder a verificar la identidad del solicitante. Este último está obligado a acreditarla mediante su documento nacional de identidad (DNI), pasaporte u otros medios admitidos en derecho (art. 13.1. LFE); excepto en dos circunstancias concretas, a saber:

- En los casos que el solicitante que efectúa la petición de un certificado lo hace empleando a dicho efecto otro certificado vigente, en el cual - a momento de su emisión - se procedió a identificar al Firmante/Suscriptor de conformidad con las previsiones del art. 13 LFE. Para que esta forma de solicitud prospere se requiere además, que el PSC tenga la certeza que el período de tiempo transcurrido desde la identificación es menor de cinco años (art. 13.4.b. LFE);
- En los casos que en virtud de una relación preexistente, en la que a objeto de identificación del interesado se utilizaron los procedimientos contemplados en el art. 13 LFE, la identidad u otras circunstancias permanentes de los solicitantes de los certificados son de conocimiento efectivo por parte del PSC. Para que esta forma de solicitud prospere se requiere además, que el período de tiempo transcurrido desde la identificación sea menor a cinco años (art. 13.4.a. LFE).

Cuando el solicitante manifieste su intención de incluir dentro la información del certificado otras circunstancias personales o una serie de atributos suyos, como podría ser su titulación profesional, la condición de titular de un cargo público, su pertenencia a determinado colegio profesional, etc., éstas deben ser objeto de comprobación por parte del PSC acudiendo a dicho fin a la consulta de los documentos oficiales que las acrediten, de conformidad con su normativa específica (art. 13.3. párrafo segundo LFE).

Cuando la emisión del certificado será a favor de personas jurídicas, el PSC se encuentra en la obligación de comprobar, además de los datos identificativos de la persona física solicitante, los datos relativos tanto a la constitución y personalidad jurídica así como a la extensión y vigencia de las facultades de representación orgánica del solicitante, operación que puede efectuar acudiendo ya sea, a la consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, o, cuando aquellos no sean de inscripción obligatoria, a través de la consulta de los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente (art. 13.2. LFE).⁴⁴⁸

Para aquellos otros casos en los que no existe una representación orgánica sino que el certificado reconocido reflejará una representación voluntaria, el PSC debe proceder a verificar la información referente a la personalidad jurídica de la entidad representada, así como la que demuestra la extensión y vigencia del poder y facultades del representante. En estos casos, al igual que en el supuesto anterior, el PSC puede acudir a dicho objeto a la consulta en el registro público en el que estén inscritos los documentos de constitución y de apoderamiento, o, cuando aquellos no sean de inscripción obligatoria, a través de la consulta de los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente (art. 13.3. párrafo primero LFE).

Finalmente, en todos aquellos casos en los que los certificados reconocidos incluirán otros supuestos de representación, el PSC tiene la obligación de exigir al Solicitante la acreditación fehaciente de las circunstancias en las que se fundamenten, conforme las previsiones descritas precedentemente (art. 13.3. párrafo segundo LFE).

⁴⁴⁸ La Exposición de motivos de la LFE resalta sobre este particular que el Ordenamiento español "...permite que los prestadores de servicios de certificación podrán, con el objetivo de mejorar la confianza en sus servicios, establecer mecanismos de coordinación con los datos que preceptivamente deban obrar en los Registros públicos, en particular, mediante conexiones telemáticas, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de éstos. Dichos mecanismos de coordinación también podrán contemplar la notificación telemática por parte de los registros a los prestadores de servicios de certificación de las variaciones registrales posteriores."

ii) Asegurar exactitud de la información.-

Otra de las obligaciones que recae sobre el PSC, es que con carácter previo a la emisión del certificado reconocido debe asegurarse en sentido que la información contenida en el certificado es precisa y exacta (art. 12.b. LFE), es decir, que los datos incluidos en el documento no sufren de errores u omisiones. Así, deberá constatar que se indique expresamente que el certificado es emitido como reconocido; que se incluye correctamente el código identificativo único del certificado; que consta la identificación del PSC que expide el certificado y su domicilio correctamente asentado.

En el supuesto de personas físicas verificar que el nombre, apellidos y número de DNI o, en su caso, el seudónimo están correctamente registrados; en el caso de personas jurídicas debe verificar que la denominación o razón social y su código de identificación fiscal se incluyen sin errores.

En caso que reflejen cualquier otra circunstancia o atributo específico del Firmante/Suscriptor, debe asegurar su adecuado reflejo en el certificado; si el certificado admite una relación de representación, la indicación del documento público que acredite las facultades del firmante y los datos registrales de la persona que representa deben igualmente encontrarse correctamente consignados; que tanto el comienzo como el fin del período de validez del certificado está debidamente asignado; que tanto los límites de uso del certificado como los límites del valor de las transacciones para las que puede utilizarse el certificado - si se establecen - figuran correctamente registrados.

Del mismo modo el PSC debe asegurarse que el certificado incluye todos los elementos establecidos para un certificado reconocido, lo cual incluye, además de la señalada previamente: la firma electrónica avanzada del PSC así como la clave pública (datos de verificación de firma) que se corresponde con la clave privada (datos de creación de firma) que se encuentren bajo el control del firmante.

iii) Cerciorarse la efectiva posesión del Firmante/Suscriptor del par de claves.-

Conforme se tiene analizado, el interesado en obtener una firma electrónica basada en cifrado asimétrico, es decir una firma digital, tiene dos posibilidades: generar el par de claves (datos de creación y verificación de firma) en un entorno propio, o, generarlos en un sistema central, en este último caso puede ser el propio PSC que le preste ese servicio o incluso un tercero ajeno al entorno del PSC.

En cualquiera de los supuestos, sea que el interesado genere el juego de claves de firma en su entorno o que recabe los mismos de un tercero (el PSC u otro), a momento de solicitar el certificado reconocido con el cual respaldará dicha firma electrónica, el PSC se encuentra en la obligación de asegurarse que el Solicitante y futuro Firmante/Suscriptor se encuentra en posesión efectiva de la clave privada (datos de creación de firma) que debe corresponderse con la clave pública asociada (datos de verificación de firma) que constan en el certificado (art. 12.c. LFE).

De todas formas, la realidad del tráfico nos demuestra que por lo general el interesado en efectuar transacciones de comercio electrónico a momento de hacerse de una firma electrónica, acude directamente a un PSC de reconocido prestigio para que sea éste quien genere el juego de claves (es decir los datos de creación y verificación de firma) y paralelamente le emita el certificado reconocido con el cual avalará su firma en la red.

Simultáneamente, lo normal es que los PSC recomienden a sus clientes el empleo de los recursos tecnológicos que ellos mismos ofrecen, es decir el software y los dispositivos seguros de creación y verificación de firma, o incluso que restrinjan la prestación de sus servicios a los elementos tecnológicos por ellos proporcionados, lo cual reviste de cierta lógica, pues el PSC debe asegurarse de que dichos elementos reúnan mínimas condiciones de seguridad; fiabilidad que el PSC no posee en el caso que el Solicitante acuda con su propio juego de claves, pues desconoce el nivel de seguridad con las que fueron generadas y

obviamente no estará dispuesto a correr riesgos, máxime si el PSC está sujeto a responsabilidades por daños que su puedan ocasionar por el empleo de claves de dudosa procedencia.

iv) Garantizar complementariedad del juego de claves.-

Por último cuando es el propio PSC quien genera el juego de claves, se encuentra lógicamente obligado a garantizar la complementariedad de los datos de creación y verificación de firma (art. 12.d. LFE).

4.2.2.2. A tiempo de emitir el certificado reconocido.-

Del mismo modo, el PSC que emite certificados digitales reconocidos se encuentra obligado a cumplir una serie de obligaciones concretas a momento de emitir el certificado. A continuación explicaremos en qué consisten efectuando las matizaciones pertinentes.

i) Constituir un seguro

En tanto la utilización de la firma electrónica puede eventualmente originar daños no sólo a los Firmante/Suscriptores sino también a los Usuarios de certificados, u otros terceros que actúen de buena fe, estas entidades asumen la responsabilidad (contractual y/o extracontractual) por los mismos, haciendo notar que no obstante que la temática sobre responsabilidad se regula específicamente en los arts. 22 y 23 de la LFE, ello no impide que con pleno respeto a tales previsiones pueda ser acotada contractualmente (frente a los Firmante/Suscriptores e incluso los Usuarios del certificado) y a través de su declaración de Prácticas y Políticas de certificación (frente a terceros).

Pero aún con todas las previsiones que pueda adoptar el PSC, ya sea limitando sus responsabilidad contractualmente o por medio de sus Prácticas de Certificación, y a pesar del empleo de toda la diligencia debida en el ejercicio de sus actividades, es de prever que acontecerán hechos que generen daños imputables al PSC, con la consiguiente responsabilidad contractual o extracontractual que de ello deviene, razón por la cual y frente

a estos imprevistos, el PSC que expide certificados reconocidos debe proceder a constituir un seguro de responsabilidad civil por un monto que alcance por lo menos la suma de 3.000.000 de euros, a objeto precisamente de hacer frente al riesgo de la responsabilidad por los daños y perjuicios que pueda eventualmente ocasionar el uso de los certificados que expida (art. 20.2. párrafo primero LFE; inc. h) Anexo II DFE).⁴⁴⁹

ii) Demostrar fiabilidad técnica

Al mismo tiempo el PSC que vaya a emitir certificados reconocidos debe garantizar y demostrar la fiabilidad necesaria para prestar servicios de certificación reconocida (art. 20.1.a. LFE; inc. a) Anexo II DFE). Esta exigencia consiste - de manera general - en el empleo de tecnología y sistemas seguros que garanticen de manera óptima el ejercicio de sus actividades, previsión también contenida en los arts. 9.1.f. y 10 LMFE.

Por ejemplo, a momento de proceder con la emisión, suspensión o revocación de un certificado reconocido, el PSC debe emplear recursos tecnológicos garantizados que permitan brindar los niveles de seguridad adecuados a la administración del sistema de certificados.⁴⁵⁰ De la misma forma, cuando procede a publicar la emisión, suspensión o revocación del certificado, o a momento de generar o resguardar su propia clave privada, debe establecer procedimientos adecuados y fiables.⁴⁵¹

Precisamente para la adecuada gestión de una infraestructura de clave pública resulta bastante útil la implementación de auditorías periódicas, cuyo objetivo es poner a prueba la fiabilidad del prestador y en caso de detectarse fallas en los diversos procedimientos, se

⁴⁴⁹ El PSC puede sustituir total o parcialmente dicha garantía, por una garantía mediante aval bancario o seguro de caución, de forma tal que la sumatoria de las cantidades aseguradas lleguen por lo menos a la suma de 3.000.000 de euros (art. 20.2. párrafo segundo LFE).

⁴⁵⁰ En ese entendido, el art. 10.b LMFE señala que para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes: “*b) la calidad de los sistemas de equipo y programas informáticos.*”

⁴⁵¹ En idéntico sentido que el anterior, el art. 10.c LMFE señala que podrán tenerse en cuenta: “*c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros.*”

puedan implementar las correcciones necesarias que tiendan a asegurar el desarrollo seguro y fiable de sus tareas.⁴⁵²

De hecho varios PSC prevén en su DPC la ejecución temporal de dichas auditorías, que si bien normalmente son internas (pues no se encuentran sometidas a un control de organismo autónomo y sirven para la auto-regulación de la propia entidad de certificación, sin control externo ni verificación objetiva e independiente), no es menos cierto que contribuyen efectivamente en procura de mejorar las condiciones de seguridad.⁴⁵³

Conjuntamente varios PSC desarrollan en su DPC planes de contingencias y de recuperación frente a desastres que tienden a hacer frente a situaciones imprevistas, debido a las perjudiciales consecuencias que se podrían derivar de una paralización del funcionamiento de los sistemas de una entidad de certificación.

iii) Garantizar precisión temporal

De igual manera el PSC tiene la obligación de garantizar que pueda determinarse con absoluta precisión la hora y la fecha en las que se expidió, suspendió o extinguió la vigencia de un certificado reconocido (art. 20.1.b. LFE; inc. c) Anexo II DFE).

Esta obligación resulta en la práctica de trascendental importancia, debido a que un documento firmado electrónicamente a través de una clave privada únicamente contribuye a la identificación de su emisor,⁴⁵⁴ pero tómesese en cuenta que la firma electrónica, por sí sola, no contribuye a probar el momento temporal de creación o envío del mensaje.

En el ámbito del comercio electrónico (en sentido amplio o estricto) como sabemos, la prueba del tiempo exacto en que una determinada acción se produce, por ejemplo, la

⁴⁵² Sobre este punto y siguiendo el mismo sentido que los dos anteriores, el art. 10.e LMFE señala que podrán tenerse en cuenta: “e) la periodicidad y el alcance de la auditoría realizada por un órgano independiente.”

⁴⁵³ Al respecto, Martínez propone como una alternativa a esta problemática la autorregulación del sector y el otorgamiento de sellos de calidad a aquellos PSC que, entre otras evaluaciones, superen aquellas relativas a la fiabilidad de sus servicios; cuya fiabilidad - sostiene - dependerá de su objetividad y representatividad de los distintos intereses en juego, y no sólo los del propio sector (A. Martínez, 2004: 299). A nosotros se nos ocurre en ese sentido, que es también factible la elaboración por parte de los PSC de códigos de conducta, de conformidad a las previsiones del art. 18 LSSI.

⁴⁵⁴ La identificación del emisor de un mensaje de datos se efectuará en base a la clave pública asociada y contenida en el correspondiente certificado reconocido, de manera que se relaciona de modo efectivo al emisor con el mensaje electrónico enviado por éste.

transmisión, creación o recepción de un documento, o tiempo en que se realiza una declaración de voluntad, es de vital importancia.

De tal manera que la prueba del tiempo resulta a todas luces necesaria, particularmente: a momento de verificar una firma digital (saber el tiempo o la fecha en la firma fue creada permite determinar si se empleó durante el tiempo de vigencia del certificado que la respalda, de lo contrario no se debe confiar en ella); en caso de revocación de un certificado (es necesario determinar el momento exacto de revocación del certificado para deslindar responsabilidades por los documentos firmados con posterioridad a dicho evento); o por ejemplo cuando existen distintas versiones de las Declaraciones de Prácticas y Políticas de Certificación (se torna imprescindible precisar el momento en que el PSC publica cada versión de dichos documentos, para poder establecer la que resulta aplicable a un certificado en concreto).

La solución a la ausencia de prueba temporal que recae sobre el empleo de la firma digital por sí sola, vino de la mano de los denominados “*Servicios de sellado temporal digital*”, también conocidos como “*Servicios de datación electrónica*” o en inglés *time stamping*, por medio de los cuales se introduce una marca temporal en el documento electrónico combinando la firma digital con un sello temporal digital, lo que permite confirmar el momento exacto de determinadas acciones (v.gr. fecha y hora en que se produjo la suspensión de un certificado, o en la que se firmó un documento electrónico, por ejemplo, un contrato).⁴⁵⁵

De esa manera, la utilidad del sello temporal estriba en que permite al receptor de un mensaje de datos y verificador de la autenticidad de la firma digital con la que aquél se encuentra rubricado, determinar con exactitud y certeza si una firma digital fue creada, o no, durante el periodo operativo establecido en el certificado reconocido y actuar en

⁴⁵⁵ (M. Pérez, 2009: 44-45).

consecuencia, ya sea confiando en el certificado que la respalda, ya sea descartando dicha confianza.⁴⁵⁶

En otras palabras, se trata de un servicio cuya finalidad es proporcionar al destinatario la seguridad de que el documento electrónico existía con anterioridad al momento en que es realizado el fechado digital, garantizando además que dicho documento no ha sido modificado tras la inserción de la fecha y hora. De ese modo se permite al receptor del mensaje de datos cerciorarse si la firma electrónica se incorporó, o no, dentro del periodo de vigencia del certificado.

Los servicios de sellado temporal pueden ser proporcionados por el propio PSC o también por otra entidad de confianza diversa, ya sea dependiente del PSC o inclusive puede darse el caso que constituya una entidad que presta sus servicios de manera completamente independiente al PSC; son conocidas como Entidades de Fechado Digital. De todas maneras, el valor probatorio del sello temporal obedecerá al hecho que el mismo sea proporcionado por un sistema seguro y fiable, asumiendo el PSC la obligación de garantizar que pueda determinarse con absoluta precisión la hora y la fecha en las que se expidió, suspendió o extinguió la vigencia de un certificado reconocido, ya sea cuando es él mismo quien presta el servicio de sellado temporal, ya sea que se trate de un tercero relacionado o independiente.

La realidad española demuestra que en la generalidad de los casos los PSC han optado por ser ellos mismos quienes proporcionen este servicio.

⁴⁵⁶ Al respecto consultar (A. Martínez, 2004: 300-308) // En idéntico sentido (A. Martínez, 2001: 78-85). Conforme apunta Ramos, las Entidades de Fechado Digital (EFD) - TSA o *Time Stamping Authorities*, en lengua inglesa - que vinculan un instante de tiempo a un documento electrónico avalando con su firma la existencia del documento en el instante referenciado, resolverían el problema de la exactitud temporal de los documentos electrónicos. Fernando Ramos Suárez, "La firma digital", en *REDI: Revista Electrónica de Derecho Informático*, No. 9, España, Alfa-Redi, abril/1999, ubicado en <http://www.alfa-redi.org/rdi-articulo.shtml?x=252> // El mismo autor señala además, que la EFD puede ser individual, es decir prestar exclusivamente estos servicios o puede ser parte de una gama de servicios relacionados con los PSC; proporcionan una prueba de existencia de una cierta información en un momento dado. El mecanismo de fechado digital proporciona una semántica del tipo "antes de": corrobora la evidencia de que el documento existía antes del instante de sellado, y garantiza que no se ha modificado con posterioridad. Por tanto, permiten al verificador determinar fehacientemente si la firma digital fue ejecutada dentro del periodo de validez del certificado, previenen fechados fraudulentos antes o después de la fecha consignada e impiden alterar el contenido del documento posteriormente al instante de firma. Fernando Ramos Suárez, "Como Aplicar la Nueva Normativa sobre Firma Electrónica", en *REDI: Revista Electrónica de Derecho Informático*, No. 19, España, Alfa-Redi, febrero/2000, ubicado en <http://www.alfa-redi.org/rdi-articulo.shtml?x=421>

iv) Emplear personal cualificado

Prosiguiendo con el estudio de las obligaciones que recaen sobre el PSC que emite certificados reconocidos, debemos señalar que éste debe emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos (art. 20.1.c. LFE; inc. e) Anexo II DFE; art. 9.1.f. LMFE).

De manera que el PSC debe asegurarse de contar con personal que tenga la debida preparación y competencia, tanto desde el punto de vista de la técnica como de la confianza, puesto que gestionar un sistema de certificados y la ICP demandan gente proba en su oficio, con los conocimientos especializados, la experiencia suficiente y las cualificaciones necesarias correspondientes para el nivel de los servicios prestados, particularmente se requiere de personas que posean niveles óptimos de competencia en materia de gestión, así como conocimientos técnicos en el ámbito de la firma electrónica y suficiente familiaridad con los procedimientos de seguridad digital.⁴⁵⁷

Debido a que determinados trámites en la gestión de certificados demandan la comprobación y examen de documentación, como por ejemplo, a momento de la solicitud se deben verificar los documentos identificativos de los solicitantes, así como los poderes en caso de mediar una representación y las escrituras constitutivas y registros correspondientes de las personas jurídicas, que implican no únicamente su examen formal sino también una valoración de la validez y vigencia de dichos documentos, es deseable que los PSC incluyan dentro de su personal y en las ER delegadas - que son en definitiva quienes mantienen el contacto directo con los solicitantes - a profesionales abogados que puedan cumplir con la debida suficiencia dichas tareas.⁴⁵⁸

⁴⁵⁷ En ese entendido, el art. 10.f. LMFE señala que el PSC debe “utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.”

⁴⁵⁸ Rodríguez indica, que como a los PSC se les debe exigir -en el cumplimiento de sus obligaciones- una diligencia profesional, comprensiva de ésta se puede entender la obligación de acudir a expertos en aquellos casos en los que la identidad del sujeto plantee dudas, de modo que “Por este camino se vendría a completar la intervención de los prestadores con la de los profesionales del Derecho...” (M. Huerta y D. Rodríguez, 2001: 128). En el mismo sentido (A. Martínez, 2004: 309).

v) Emplear procedimientos adecuados

Aparejada con la obligación anterior se encuentra el deber del PSC de poner en práctica los procedimientos administrativos y de gestión adecuados, conformes a normas reconocidas; así como los procedimientos de seguridad apropiados al ámbito de la firma electrónica (art. 20.1.c. LFE; inc. e) Anexo II DFE; art. 9.1.f. LMFE). Como se notará, esta obligación esta también directamente relacionada con el deber de garantizar y demostrar la fiabilidad necesaria para prestar servicios de certificación reconocida, por lo cual nos remitimos a lo señalado en su momento.

vi) Utilizar recursos fiables

El empleo de sistemas y productos de firma electrónica fiables es otra de las obligaciones del PSC, los cuales deben estar protegidos contra toda alteración y garantizar la seguridad tanto técnica y, en su caso criptográfica, de los procesos de certificación a los que sirven de soporte (art. 20.1.d. LFE; inc. f) Anexo II DFE; art. 10 LMFE).

En esa dirección, el art. 28.1. LFE - cuyo contenido hace referencia al reconocimiento de la conformidad con la normativa aplicable a los productos de firma electrónica - establece la presunción que los productos de firma electrónica mencionados en la propia LFE, concretamente en el párrafo d), apartado 1, del art. 20 (que estudiamos en esta parte) y en el apartado 3, art. 24 *“son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el Diario Oficial de la Unión Europea”*.

Con relación a lo anotado precedentemente, el art. 3.5. DFE dispone que 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”.

vii) Prevenir falsificaciones

La adopción de medidas contra la falsificación de certificados constituye otra de las obligaciones concretas del PSC (art. 20.1.e. LFE; inc. g) Anexo II DFE). Sobre este punto cabe anotar, que si bien la falsificación de un certificado reconocido resulta una tarea bastante compleja desde el punto de vista técnico, ya que la firma electrónica avanzada del PSC protege su integridad, no obstante, no es un hecho completamente descartable, ya que podría darse el caso que ante la pérdida de la clave privada del PSC o el compromiso de su seguridad, un tercero que tenga acceso a la misma emita de modo fraudulento certificados firmándolos con la clave privada del PSC, acarreando graves perjuicios.

En este caso nos encontraríamos ante un tipo delictivo de falsedad documental, consistente, conforme al art. 390.1 del Código Penal (C.p.) español, en la alteración de un documento en algunos de sus requisitos o elementos esenciales, es decir, añadir, suprimir o modificar alguna de las partes de un documento. Ya sea que se trate de falsedad ideológica o material, la persona que emite el certificado fraudulento comete el delito de falsificación de documento privado (art. 395 C.p.). Igualmente cometería dicho delito el titular del certificado falso que lo utilizara a sabiendas de su falsedad en perjuicio del tercero Usuario, de acuerdo con el art. 396 C.p., mismos que para su comisión requieren la actuación dolosa del sujeto activo.⁴⁵⁹

viii) Asegurar confidencialidad de la clave privada

Cuando el propio PSC es quien genera la clave privada (datos de creación de firma), debe garantizar su confidencialidad tanto a momento de proceder a la generación, como a

⁴⁵⁹ Al respecto consultar (A. Martínez, 2004: 311 y ss.) // Para ahondar en la materia de ilícitos cometidos a través de Internet (ilicitud civil y penal), recomendamos consultar: (H. Fernández, 2000: 149-170) // Sobre el mismo tema Ricardo Mata Martín, “Algunos aspectos de la delincuencia patrimonial en el comercio electrónico”, en Joseba A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001, pp.441-462.

tiempo de su entrega a través de un procedimiento seguro al Firmante/Suscriptor (art. 20.1.e. LFE; inc. g) Anexo II DFE).

En otras palabras, conforme ya se tiene ampliamente referido, cuando el PSC asume la labor de generar la clave privada recaen sobre él de modo simultáneo dos obligaciones básicas e intrínsecamente relacionadas, por un lado, el deber de forjar la clave privada empleando óptimos procedimientos de seguridad y recursos técnicos fiables, pero además, el PSC debe garantizar que la entrega de la clave privada al Firmante/Suscriptor se lleve a cabo mediante procedimientos igualmente seguros y confiables, de modo que en ningún momento se comprometa la fiabilidad de la clave privada, desde su creación hasta su efectiva entrega y recepción por parte del Firmante/Suscriptor.

De esa manera se asegura y consigue la confidencialidad de la clave privada, no únicamente en el momento inicial sino también en el momento crítico de entrega de la clave a su titular, en el que podría perderse o comprometerse la misma.⁴⁶⁰

ix) Conservar información

La penúltima de las obligaciones concretas del PSC consiste en la conservación de toda la información y documentación relativa a un certificado reconocido, así como de las Declaraciones de Prácticas y Políticas de certificación vigentes en cada momento, empleando para ello cualquier medio que garantice la seguridad debida (art. 20.1. f. LFE; inc. i) Anexo II DFE).

Entre la información que el PSC está llamado a precautelar podemos señalar: la documentación referida a la solicitud de los certificados; la información de cada certificado emitido, incluyendo los datos de creación, emisión, uso y suspensión, revocación, expiración

⁴⁶⁰ En ese entendido, Pérez sustenta que la función básica del certificado digital, de la que deriva su aptitud para depositar la confianza en la entidad de certificación, será la de vincular de forma fiable un elemento de verificación de la firma (ligado inescindiblemente al de creación de ésta que se confiere al signatario) con una persona o entidad determinada; pero la fiabilidad del certificado radicará, además, en el hecho que el elemento de creación de firma - asociado al certificado - sea transmitido al titular del mismo dentro de un entorno de comunicación absolutamente seguro (J. Pérez, 2001: 254) // En idéntico sentido (A. Martínez, 2004: 313). Por otro lado, Rodríguez manifiesta que las claves deben ofrecer varias posibilidades, por una parte, señala que es más seguro la generación de las claves en el entorno del Firmante que en el del PSC. Por otra parte indica la necesidad de que las claves se puedan almacenar y transmitir de forma segura, para así mantener la seguridad de la ICP. Daniel Rodríguez Ruiz de Villa, “*Dos aspectos de los prestadores de servicios de certificación electrónica: concepto y acceso*”, disponible en <http://www.ieid.org/congreso/ponencias/Rodriguez%20Ruiz.%20Daniel.pdf>

y renovación del certificado. En idéntica manera se deberá preservar la información relevante concerniente al nombre del sujeto solicitante, copia de los documentos acreditativos presentados para comprobar su identidad, así como documentación de todos los pasos que se hayan seguido para establecer esa identidad; en el caso de personas jurídicas deberán constar los datos de constitución y registro correspondientes, junto con los poderes que acrediten la representación legítima de quien actuó por cuenta de aquella y otros elementos importantes incluidos en el certificado, de forma segura y fiable.

En cuanto a la forma de llevar este registro la LFE determina que el archivo de información podrá realizarse por cualquier medio seguro, de modo que a nuestro entender, el registro puede constar en soportes electrónicos (que de hecho es la previsión de la DFE) como no electrónicos o tradicionales (v.gr. el papel), pero con la condición indispensable que el PSC garantice la exigencia de seguridad en la preservación de dicha información.

El plazo mínimo fijado para conservar la mencionada información es de quince (15) años, los cuales se computan desde el momento en que se expide el certificado reconocido, término de tiempo que coincide con el plazo de prescripción de las obligaciones personales de conformidad con el art. 1.964 C.c.

Entendemos que el propósito objetivo y práctico de esta obligación de registro y conservación de la información, reside en hacer posible la verificación de las firmas efectuadas - en base al certificado reconocido en que se respaldan - en cualquier momento posterior, por ejemplo, a efectos de su empleo como medio de prueba de la certificación en la eventualidad de un procedimiento judicial (inc. i) Anexo II DFE).

x) Almacenar certificados de modo seguro

Finalmente sobre el PSC recae la exigencia de utilizar sistemas fiables para almacenar certificados reconocidos, los cuales deben permitir: i) comprobar su autenticidad e impedir que personas no autorizadas alteren los datos; ii) restrinjan su accesibilidad en los supuestos o

a las personas que el firmante haya indicado; y iii) permitan detectar cualquier cambio que afecte a estas condiciones de seguridad (art. 20.1.g. LFE; inc. 1) Anexo II DFE).⁴⁶¹

En otras palabras, el PSC a tiempo de utilizar sistemas fiables para conservar certificados reconocidos que garanticen su verificación, debe asegurar que únicamente personas autorizadas puedan acceder a efectuar anotaciones y modificaciones en el contenido del certificado, que lógicamente sea factible comprobar la autenticidad de la información, así como también debe asegurar que los certificados se encuentren disponibles a los Usuarios de certificados para que efectúen las correspondientes consultas, limitando el acceso a los mismos en aquellos casos o a las personas que el Firmante/Suscriptor haya solicitado.

Por último, los sistemas fiables para conservar certificados reconocidos deben garantizar que se pueda detectar todos los cambios técnicos que coloquen en desconfianza a los requisitos de seguridad mencionados.

Respecto a la utilidad que en la práctica reviste este archivo, desde la perspectiva del Firmante/Suscriptor su provecho estriba en la factibilidad de solicitar una copia en el caso que haya perdido el certificado que le fuera remitido inicialmente; en tanto que para el PSC, el beneficio radica en la posibilidad de conocer en todo momento lo que ha sido firmado por éste y, en caso de que el certificado emitido se traspase a un directorio, de igual modo facilita al PSC controlar que no se emitan dos certificados con las mismas claves.⁴⁶²

4.2.3. Obligaciones adicionales.-

El PSC se encuentra reatado además al cumplimiento de las siguientes obligaciones adicionales:

⁴⁶¹ Respecto de esta obligación Martínez apunta lo siguiente: "...el apartado g) del art. 20 LFE parece referirse a un archivo de certificados distinto del simple registro o directorio de certificados del art. 18.c) y probablemente del servicio de consulta del art. 18.d)" cuestión que desde su punto de vista -y compartimos nosotros- "...plantea la duda de si debe ser un archivo diferenciados del registro y del servicio de consulta o si sería suficiente que el directorio general y su servicio de consulta del prestador cumplieran estas exigencias del art. 20.1.g) LFE para los certificados reconocidos." (A. Martínez, 2004: 316).

⁴⁶² Al respecto (M. Huerta y D. Rodríguez, 2001: 31-32) // (M. Huerta y D. Rodríguez, 2001: 115-116) // En idéntico sentido (A. Martínez, 2004: 316-317).

i) Actuar de buena fe

Conforme se tiene ampliamente analizado, en virtud de lo dispuesto en el art. 57 C.com. y el art. 1.258 C.c., el PSC tanto a momento de efectuar los tratos preliminares como durante la ejecución propiamente del contrato, debe actuar conforme al principio-deber de *Buena fe*. Además está obligado lógicamente a cumplir de manera general con lo dispuesto por la normativa sobre firma electrónica vigente.

ii) Administrar el ciclo vital del certificado reconocido

El PSC lógicamente tiene la obligación de administrar todo el ciclo vital del certificado reconocido, el cual abarca desde el momento de la emisión del mismo, su entrega por medio de canales seguros de distribución al Firmante/Suscriptor, pasando por eventuales casos de suspensión de su vigencia, continuando con la posible revocación que pueda solicitar expresamente en determinado momento el Firmante/Suscriptor (lo que determina la extinción de su vigencia), hasta la extinción de vigencia del certificado, ya sea debido a una invalidez anticipada por causas no previstas o por finalización del plazo de vigencia que figura en el certificado.

También puede darse el caso que el Firmante/Suscriptor solicite actualizar los datos contenidos en el certificado (v.gr. cambio de representante legal con el consiguiente cambio de poderes), lo que obliga al PSC a brindar un “Servicio de actualización o modificación de datos del certificado”.

De acuerdo con el análisis realizado en su momento, el art. 9.1. LFE establece las causales de suspensión de la vigencia de los certificados electrónicos, es decir pérdida de vigencia temporal, disponiendo con relación al momento a partir del cual surte plenos efectos la suspensión de un certificado, que éste se produce desde el instante en que la suspensión es incluida por el PSC en el servicio de consulta sobre la vigencia de certificados (art.9.2 LFE)

De otra mano, el art. 8 LFE se ocupa de regular los casos de extinción de la vigencia de los certificados electrónicos, es decir, la pérdida de vigencia definitiva. Con relación a la eficacia de la extinción de los certificados, el art. 8.3. LFE dispone que la misma se hará efectiva frente a terceros desde el momento que acontezca la expiración del plazo de validez del certificado (eficacia inmediata) y, en los restantes casos, desde que la información referente a la extinción se incluya por el PSC en el servicio de consulta sobre vigencia de certificados (eficacia diferida).

Previsiones con relación al posible entredicho de los datos de creación de firma y su comunicación oportuna por parte del Firmante /Suscriptor, así como respecto de los servicios de revocación de certificados, también se hallan contenidas en el art. 9.1.e. de la LMFE.⁴⁶³

Tanto las situaciones de suspensión como de extinción de vigencia del certificado electrónico revisten de mucha importancia, debido a que los terceros deben dejar de confiar en un certificado extinguido o suspendido, para lo cual se hace necesario que éstos puedan conocer dicha información, la cual debe ser incluida por el PSC en el servicio de consulta sobre vigencia de certificados.

Del mismo modo, las disposiciones que hacen a la extinción y suspensión de vigencia de los certificados, sirven también para delimitar eventuales responsabilidades entre las distintas partes implicadas en caso de litigio provocado en torno a un certificado suspendido o extinguido, las cuales analizaremos con mayor detenimiento a momento de tratar el régimen de responsabilidades que surgen del contrato de certificación reconocida, tanto para el PSC, el Firmante/Suscriptor e incluso para terceros.

Precisamente con relación a los casos de suspensión y extinción de vigencia de los certificados, surge la obligación del PSC de dar publicidad respecto al acaecimiento de las

⁴⁶³ Señala el referido artículo que el PSC tiene el deber de proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera: “e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), (alude a los servicios para que el firmante de aviso de la puesta en peligro de los datos de creación de firma) proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1) del artículo 8 de la presente Ley y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), (alude a los servicios de revocación de certificados) cerciorarse de que existe un servicio para revocar oportunamente el certificado.” (art. 9.1.e. LMFE).

mismas (art. 10 LFE). Tómese en cuenta que la referida publicación constituye un elemento de fundamental trascendencia, toda vez que a partir de ese momento la suspensión o extinción del certificado va a ser conocida por terceros; y, en concreto, representa el momento preciso a efectos de distribución o imputación de responsabilidades entre los diversos sujetos implicados (PSC, Firmante/Suscriptor y Usuario del certificado).⁴⁶⁴

En ese entendido la normativa española contiene una serie de disposiciones comunes a la extinción y suspensión de la vigencia de certificados electrónicos, contenidas en el art. 10 de la LFE que comentamos. Inicia el referido articulado estableciendo la obligación que posee el PSC de hacer constar de manera inmediata, clara e indubitada, la extinción o suspensión de la vigencia de los certificados electrónicos en el servicio de consulta sobre vigencia de certificados, tan pronto como tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia (art. 10.1. LFE).

Del mismo modo, la norma dispone que el PSC se encuentra en la obligación de informar al signatario y titular del certificado respecto de esta circunstancia, ya sea con carácter previo o simultáneo a la extinción o suspensión de la vigencia del certificado electrónico, debiendo aclarar las razones así como la fecha y hora en que el certificado va a quedar sin vigencia.

Para los casos de suspensión, el PSC debe además, aclarar la duración máxima de dicha suspensión. Pero si transcurrido dicho plazo no se hubiera levantado la suspensión, el efecto previsto en todo caso es la extinción de la vigencia del certificado (art. 10.2. LFE). La norma de modo categórico decreta igualmente que la extinción o suspensión de la vigencia de un certificado electrónico, en ningún caso puede tener efectos con carácter retroactivo (art. 10.3. LFE).

⁴⁶⁴ Así por ejemplo, el art. 23.2 LFE exonera de responsabilidad al PSC cuando el Usuario del certificado y destinatario de los documentos firmados electrónicamente por el Firmante/Suscriptor, actúe de forma negligente por no tener “*en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados*”.

Finalmente, con relación al plazo que la información sobre la extinción o suspensión de vigencia de un certificado electrónico debe ser mantenida accesible en el servicio de consulta sobre vigencia de certificados, la legislación comentada ordena que éste deba ser al menos hasta la fecha en que hubiera finalizado el período de validez inicialmente previsto en el certificado (art. 10.4. LFE).

iii) Proporcionar información actualizada (DPC)

Igualmente constituye un deber del PSC comunicar al Firmante/Suscriptor, a los Usuarios del certificado (y eventualmente otros terceros interesados), sobre los cambios que podrían existir en las Prácticas y Políticas de Certificación, así como proporcionar cualquier otro tipo de información relevante, cuyo desconocimiento podría ocasionar eventuales perjuicios o daños.

iv) Protección de datos personales

El PSC a momento de emitir el certificado reconocido únicamente puede recabar datos personales con el consentimiento expreso del Solicitante - Firmante/Suscriptor y directamente de éste, debiendo ser los exclusivamente necesarios para la expedición y el mantenimiento del certificado y la prestación de otros servicios que brinde relacionados con la firma electrónica; de manera que el PSC no puede hacer uso de dichos datos con otra finalidad, a no ser que cuente con el consentimiento expreso del Firmante/Suscriptor (art. 17.2. LFE).⁴⁶⁵

El manejo de los datos recabados deben adecuarse a las disposiciones de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LPDPC) y en sus normas de desarrollo (art. 17.1. LFE), no debiendo incluir en el certificado reconocido en todo caso, los datos a los que se refiere el art. 7 de la mencionada Ley (art.

⁴⁶⁵ Un análisis detallado sobre la afectación de la intimidad en Internet así como respecto de la protección de datos personales, puede ser encontrado en María Paz García Rubio, "Bases de datos y confidencialidad en Internet", en Joseba A. Echebarria Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001, pp.463-489 // De igual modo Pedro Canut, "El Secreto Profesional del Abogado ante la Ley Orgánica de Protección de Datos de Carácter Personal", en *REDI: Revista Electrónica de Derecho Informático*, No. 90, España, Alfa-Redi, enero/2006, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=4226> // Sobre el mismo tema examinar el aporte de (H. Fernández, 2000: 207-241).

17.4. LFE), es decir, aquellos datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias, los que hagan referencia al origen racial, a la salud y a la vida sexual o aquellos relativos a la comisión de infracciones penales o administrativas.⁴⁶⁶

Si el PSC consigna un seudónimo en el certificado reconocido por solicitud del Solicitante-Firmante/Suscriptor, se debe asegurar de confirmar la verdadera identidad de éste, conservando la documentación que la acredite; en todo caso, el PSC ante la solicitud de un organismo competente en el ejercicio de sus funciones y en los demás supuestos previstos en el art. 11.2. de la LPDCP, se encuentra obligado a revelar la identidad del Firmante/Suscriptor sin consentimiento previo de éste, cuando así se lo requieran (art. 17.3. LFE).

Esta previsión se halla contenida también en el art. 11.2.e) LFE, relativo al contenido de los certificados reconocidos, cuando señala: *“La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos ... o a través de un seudónimo que conste como tal de manera inequívoca...”*, y en el art. 25.3.d) LFE, que exige que los dispositivos de verificación de firma electrónica garanticen, siempre que sea *técnicamente* posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos: *“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”*; exigencia que por otra parte se encuentra contenida en el apartado f) Anexo IV DFE, la cual como se tiene dicho, establece una serie de recomendaciones para la verificación de la firma.⁴⁶⁷

⁴⁶⁶ Estas disposiciones se encuentran también previstas en el art. 8 DFE, el cual establece de modo genérico, que los estados miembros deben asegurar que los PSC cumplan los requisitos establecidos en la Directiva 95/46/EC y 97/66/CE del Parlamento y del Consejo, 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 (art. 8.1.DFE). Más específicamente el art. 8.2. DFE señala: *“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 ó tratarse con fines distintos sin el consentimiento de su titular.”* Asimismo, en su parte considerativa señala expresamente que *“Para incrementar la confianza de los usuarios en la comunicación y el comercio electrónicos, los proveedores de servicios de certificación deben observar la normativa sobre protección de datos y el respeto de la intimidad.”*

⁴⁶⁷ La DFE con relación al empleo de seudónimos en el certificado, señala en su parte considerativa que *“Las disposiciones relativas al uso de seudónimos en los certificados no deben impedir a los Estados miembros exigir la identificación de las personas de conformidad con el Derecho comunitario o nacional.”*

v) No almacenar ni copiar los datos de creación de firma del Firmante/Suscriptor

Como se tiene analizado previamente, el interesado en obtener una firma electrónica basada en cifrado asimétrico, es decir, una firma digital (tecnológicamente hablando), tiene dos opciones: i) generar el par de claves en el sistema o entorno propio; ii) generarlas en un sistema central de otra entidad, que puede ser el propio PSC o incluso una tercera persona que preste el servicio de generación de claves.

Cuando el par de claves es generado en el sistema del titular del certificado, muy probablemente en el mismo hardware o software en el que la clave privada (datos de creación de firma) será almacenada y usada, no existe el problema de asegurar la transferencia segura de la misma, dado que en ningún momento la clave privada abandona su entorno de origen.⁴⁶⁸

En cambio cuando el par de claves es generado en el sistema central del PSC, la clave privada debe ser transportada de forma segura al sistema del titular, debiendo el PSC proceder a la destrucción de toda la información referente a la creación del par de claves, y en especial, la propia clave privada de firma.⁴⁶⁹ Es decir, existe una prohibición expresa en sentido que el PSC no puede copiar ni almacenar los datos de creación de firma, que en un sistema criptográfico asimétrico se corresponden con el de la clave privada (art. 18.a. LFE).

De manera que si bien en el derecho español se regula el sistema de generación de claves por el propio PSC, con la ventaja de seguridad y fiabilidad que ello trae aparejado *“debido a que con mucha probabilidad la entidad poseerá sistemas más seguros que los que*

⁴⁶⁸ Conforme hace notar Martínez, este sistema tiene la ventaja de que genera mayor confianza en torno a las claves privadas puesto que ninguna otra parte distinta del titular ha tenido acceso a las mismas; sin embargo -sostiene- su problema reside en la fiabilidad del «hardware» o el «software» de generación de claves utilizados por los solicitantes de un certificado; porque si estos mecanismos no reúnen las suficientes garantías podría ocurrir que se planteara el problema de generación de claves no fiables (A. Martínez, 2004: 269).

⁴⁶⁹ Respecto de este sistema, Rodríguez afirma que la admisión de la generación de claves por parte del propio PSC es elogiada por la doctrina especializada, al suponerse que el certificador dispondrá de sistemas más seguros que los que podría utilizar el firmante (M. Huerta y D. Rodríguez, 2001: 90) // En el mismo sentido se manifiesta Martínez, quien alega como argumento favorable la ventaja de que el PSC posee mayores recursos y controles más fuertes y, por ello, es capaz de crear un juego de claves de más alta calidad, es decir, menos predecibles o susceptibles de ruptura computacional. No obstante -resalta- su inconveniente estriba en el hecho que deben existir garantías de que los datos de firma no son objeto de maniobras fraudulentas (en especial, de que la clave privada es objeto de destrucción); y garantías de que la clave privada llega efectivamente a manos del titular de forma segura; una manera puede ser la entrega en mano, o a través de un correo certificado, de una tarjeta inteligente que contenga la clave privada, donde se puede incluir o descargar una copia del certificado con la clave pública, así como la clave pública de la entidad de certificación (A. Martínez, 2004: 269-270). La otra forma, es que el certificado sea remitido por medio telemáticos al Firmante/Suscriptor, quien lo descargará en su sistema o en la tarjeta inteligente previamente suministrada por el PSC. // Un análisis sobre las ventajas e inconvenientes de estos sistemas también es efectuado por Josep Lluís Ferrer Gomila, “Aspectos científicos de la firma digital”, en Susana García Santa Cecilia, comp., *Firma Electrónica*, Madrid, 2000; en Estudios Jurídicos. Secretarías Judiciales, IV-2000, Madrid, Solana e Hijos A.G., S.A., 2000, pp.317-318.

podría acceder el titular de las claves”⁴⁷⁰, no es menos cierto que el inconveniente radica en el hecho que no es posible tener cien por ciento de certeza de que el PSC no almacene ni copie y destruya efectivamente la clave privada una vez que es entregada al Firmante/Suscriptor, con lo que podría ser objeto de empleo ilegítimo.

La situación descrita conduciría al Firmante/Suscriptor a asumir responsabilidad frente a terceros, debido a la apariencia creada por la firma de documentos electrónicos con una clave privada de firma - en principio atribuida al Firmante y titular del certificado de forma exclusiva - que ha podido ser utilizada maliciosamente por un sujeto (el propio PSC o un tercero) que dispone de una copia de la misma.⁴⁷¹ Por ello Martínez sugiere la conveniencia de auditorías periódicas que, entre otras cuestiones, revisen y controlen este punto.⁴⁷²

La obligación que venimos estudiando se encuentra también prevista en el Anexo II DFE, que en el apartado j) dispone el deber de los PSC que expiden certificados reconocidos de *“no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves”*, no previendo excepción alguna, por tanto, ha de considerarse como una prohibición absoluta.⁴⁷³

De todas formas debe quedar claro que con independencia del soporte empleado para almacenar el certificado reconocido (convencional o Tarjeta criptográfica), el Firmante/Suscriptor tiene el derecho absoluto a la confidencialidad de su clave privada (datos de creación de firma) la cual estará siempre bajo su exclusivo control, no archivándose copia de ellos por el PSC, quien en el caso de haber efectuado la generación de la clave privada debe proceder a su destrucción, deviniendo éstas en verdaderas obligaciones del certificador,

⁴⁷⁰ (A. Martínez, 2004: 272).

⁴⁷¹ Así lo advierte Rodríguez cuando señala que la generación de claves por el propio PSC *“...genera el peligro de que el proveedor pueda no destruir la clave privada, una vez que es entregada al suscriptor, de modo que pueda ser empleada ilegítimamente por un tercero...”* (M. Huerta y D. Rodríguez, 2001: 90).

⁴⁷² (A. Martínez, 2004: 272). En el mismo sentido (M. Huerta y D. Rodríguez, 2001: 119).

⁴⁷³ Asimismo, la DFE resalta en su parte considerativa que: *“El almacenamiento y la copia de los datos de creación de la firma pueden poner en peligro la validez jurídica de la firma electrónica.”*

en tanto que la custodia de la clave privada, conforme analizaremos en su momento, constituye el más fundamental deber del Firmante/Suscriptor.

vi) Comunicación del cese de actividades

Cuando acontecen las circunstancias en que el PSC cesará en el ejercicio de sus actividades como certificador, ya sea por razones voluntarias (v.gr. disolución de la empresa por acuerdo de los socios) o incluso involuntarias (v.gr. quiebre de la empresa), el art. 21 LFE establece una doble obligación de comunicación del cese de actividad: por una parte, a los Firmante/Suscriptores (que prevista en el contrato constituye una obligación contractual) y, por otra, al Ministerio de Ciencia y Tecnología (la cual reviste la categoría de obligación legal)⁴⁷⁴, de forma respectiva. Al respecto se hace notar que la DFE no establece exigencia alguna para el PSC en caso de que deje de ofrecer sus servicios en el mercado.

La razón de esta obligación radica en el hecho que ante la suspensión de los servicios por parte del PSC, se ocasione el menor impacto negativo posible tanto para los Firmante/Suscriptores como para los Usuarios del certificado. Por este motivo el PSC que ha tomado la decisión de cesar en sus actividades, tiene la obligación de informarla a sus clientes con una anticipación de por lo menos dos (2) meses a la suspensión efectiva de sus servicios; tanto a los Firmante/Suscriptores que emplean los certificados electrónicos que fueron emitidos, como a los solicitantes de certificados que fueron emitidos a nombre de personas jurídicas.

No obstante, el PSC se encuentra facultado a transferir la gestión de los certificados que aún sigan vigentes a momento del cese a otro PSC que los asuma o, en caso contrario, extinguir su vigencia. En el primer supuesto se requiere del consentimiento expreso del

⁴⁷⁴ Respecto de esta obligación la LFE dispone que el PSC que expide certificados electrónicos al público, está en la obligación de informar al Ministerio de Ciencia y Tecnología, con dos meses de anticipación al cese efectivo de actividades, respecto de esta situación así como el destino que dará a los certificados, aclarando si va a transferir la gestión de los mismos, caso en el que debe especificar además la entidad que se hará cargo a partir de ese momento de los certificados, o, en todo caso, si extinguirá su vigencia (art. 21.2. LFE). Asimismo, el PSC con carácter previo al cese definitivo, debe remitir al indicado Ministerio toda la información referente a los certificados electrónicos que haya emitido y cuya vigencia haya sido extinguida, a objeto que éste órgano del Poder Ejecutivo se haga cargo de su custodia, a efectos de lo previsto en el artículo 20.1.f) -el cual dispone la obligación de conservar por al menos 15 años, toda la información relativa a un certificado reconocido- para que puedan verificarse las firmas efectuadas con el referido certificado, debiendo el Ministerio mantener 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 (art. 21.3. LFE).

Firmante/Suscriptor para que se viabilice el traspaso, situación que amerita la obligación adicional del PSC de informar respecto a las características del certificador al que se propone la transferencia de la gestión de los certificados; pero si el Firmante/Suscriptor se niega a aceptar la asunción en la gestión de sus certificados por otro PSC, no queda otra opción más que la extinción de su vigencia (art. 21.1. LFE).⁴⁷⁵

4.2.4. Obligaciones accesorias.-

Dentro de las obligaciones accesorias del PSC figuran otras prestaciones que eventualmente se pueden contratar. De hecho el art. 2. LFE define al PSC como “*la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica*”⁴⁷⁶ (las negrillas son nuestras).

El PSC en consecuencia puede prestar diferentes servicios, aunque lógicamente su función básica es la emisión de certificados. Sobre el particular resulta pertinente tomar muy en cuenta los preceptos de la DFE, la cual señala en su parte considerativa lo siguiente:

⁴⁷⁵ A título informativo en esta parte, mencionar que sobre el PSC recaen además otras obligaciones de origen administrativo y no contractual. Entre ellas se encuentra la obligación de facilitar al Ministerio de Ciencia y Tecnología toda la información y colaboración precisas para el ejercicio de las funciones que dicha entidad del Poder Ejecutivo tiene encomendadas por Ley, particularmente las contempladas en el art. 29 LFE, por el que se regula las facultades de supervisión y control que posee el referido Ministerio, mismas que fueron asumidas por el Ministerio de Industria, Turismo y Comercio en virtud del Real Decreto 553/2004, de 7 de abril, respecto del cumplimiento por parte de los PSC que expidan al público certificados electrónicos de las obligaciones establecidas en la LFE. Asimismo, es competente para supervisar el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma electrónica, pudiendo efectuar las inspecciones que considere necesarias para el cumplimiento de sus funciones; en todo caso, está autorizado a delegar en entidades independientes y técnicamente cualificadas la asistencia en el cumplimiento de estas tareas de control y supervisión. El PSC especialmente deberá facilitar el acceso a sus instalaciones de los agentes y el personal inspector de la referida entidad, permitiendo la consulta de cualquier documentación relevante para la inspección de que se trate (art. 30.1. LFE). Asimismo y en todos los casos, el PSC debe comunicar al mencionado Ministerio el inicio de sus actividades, los datos de identificación fiscal y su inscripción en el Registro Mercantil, los datos para contactar al PSC (v.gr. dirección, teléfonos, fax, etc.), incluidos el nombre de dominio de Internet, así como los datos de atención al público, las características de los servicios que presta, las certificaciones obtenidas para prestar sus servicios y las certificaciones de los dispositivos que utilice, información que debe ser actualizada por el PSC en caso de sufrir modificaciones y constará publicada en la dirección de Internet del citado Ministerio, a objeto de que se asegure la adecuada difusión y conocimiento por parte de los interesados (art. 30.2. LFE). Nótese que estas exigencias de información revisten bastante similitud a las exigencias contenidas en los arts. 9 y 10 de la LSSI. En todo caso no deben entenderse como una forma de autorización previa, pues como se indicó, en el mercado de la certificación rige el principio (tanto comunitario como español) de libertad de acceso a la actividad, el cual se efectúa en régimen de libre competencia; de manera que estas informaciones exigidas al PSC, deben entenderse simplemente como obligaciones administrativas que tienden a que el Estado pueda tener cabal conocimiento de los certificadores que operan en el mercado y a través de su sitio Internet difunda a la población del modo más eficiente la información relativa a los mismos, a objeto de generar niveles óptimos de seguridad y confianza respecto de la actividad de éstos, pero en ningún caso, como dijimos, constituyen autorizaciones previas. Y así se establece precisamente en la exposición de motivos de la LFE cuando señala en el acápite III: “...es de destacar de manera particular, la eliminación del registro de prestadores de servicios de certificación, que ha dado paso al establecimiento de un mero servicio de difusión de información sobre los prestadores que operan en el mercado, las certificaciones de calidad y las características de los productos y servicios con que cuentan para el desarrollo de su actividad.”

⁴⁷⁶ La DFE lo define en el art. 2.11 “proveedor de servicios de certificación: la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica”. En tanto que la LMFE establece en su art. 2.e. “Por prestador de servicios de certificación se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas”.

“La comunicación y el comercio electrónicos requieren firmas electrónicas y **servicios conexos** de autenticación de datos.”⁴⁷⁷

“La firma electrónica se utilizará en muy diversas circunstancias y aplicaciones, dando lugar a una gran variedad de nuevos servicios y productos relacionados con ella o que la utilicen. La definición de dichos productos y servicios **no debe limitarse a la expedición y gestión de certificados, sino incluir también cualesquiera otros servicios o productos que utilicen firmas electrónicas o se sirvan de ellas**, como los servicios de registro, los servicios de estampación de fecha y hora, los servicios de guías de usuarios, los de cálculo o asesoría relacionados con la firma electrónica”⁴⁷⁸ (en ambos casos las negrillas y subrayado son nuestros).

Entre los servicios accesorios a los que hacemos referencia, se encuentran los servicios de certificación especiales: la certificación de sitios web, firma de códigos y los visados electrónicos, sobre cuyo contenido nos remitimos a lo ya mencionado en nuestro primer Capítulo, al momento de abordar la temática relativa a la diferenciación de la certificación reconocida respecto de estos otros contratos de certificación especiales.

Además de los enumerados precedentemente también contamos, entre otros, fundamentalmente con los servicios de: acuse de recibo; homologación de certificados y provisión del dispositivo criptográfico junto con el software correspondiente, de los que nos ocuparemos a continuación.⁴⁷⁹

i) Provisión del dispositivo criptográfico y el software correspondiente

Cuando el Firmante/Suscriptor lo ha solicitado, el PSC tiene la obligación de proporcionar el dispositivo criptográfico (Tarjeta inteligente, token USB u otros) y el

⁴⁷⁷ Considerando 4 DFE.

⁴⁷⁸ Considerando 9 DFE.

⁴⁷⁹ Los servicios accesorios relacionados con la firma electrónica que pueden brindar los PSC, abarcan en realidad un espectro más amplio, así por ejemplo, contamos con los servicios por los que un PSC (X) valida los certificados emitidos por otro PSC (Y); también se encuentran los servicios de custodia de peticiones de validación; los de búsqueda y descarga de certificados, etc. Por ello dejamos constancia que no se efectúa en esta parte un análisis exhaustivo y acabado de los mismos, aclarando que para nuestro estudio nos hemos abocado a las prestaciones accesorias más relevantes.

software de generación o importación de los datos de creación y de verificación de firma en la Tarjeta.⁴⁸⁰

ii) Servicio de acuse de recibo.-

Si bien la firma digital conforme explica Ortega, solventa la identificación de las partes, la autenticidad y la integridad del mensaje de datos, así como su no repudio y confidencialidad, lo evidente es que, por sí sola, no consigue una prueba absoluta acerca de la existencia y del contenido de un documento electrónico, por ejemplo un contrato.⁴⁸¹

En el ámbito de la contratación electrónica, la LCE dispone que el oferente está obligado a confirmar la recepción de la aceptación al que la hizo, entre otros, mediante el envío de un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro (24) horas siguientes a la recepción de la aceptación (art. 28.1.a. LCE).

Precisamente para obtener prueba tanto de envío como de recepción del documento electrónico, las partes deben acudir a un servicio de acuse de recibo. El acuse de recibo es un documento firmado digitalmente, que el receptor de un mensaje envía al emisor del mismo para hacerle saber que lo ha recibido correctamente; mediante esta solución se obtiene prueba de envío y recepción del mensaje, así como copia firmada por las partes, es decir, prueba plena de la existencia y contenido del contrato electrónico, con la intervención de un tercero cuya actuación garantice y avale dicha situación.⁴⁸²

Al igual que en el caso del servicio de datación electrónica, el servicio de acuse de recibo puede ser proporcionado por el propio PSC o contratado con un sujeto independiente que se encargue de ello.

⁴⁸⁰ En realidad, la provisión del dispositivo criptográfico y el software correspondiente se identifica más propiamente con la distribución de productos que con la prestación de servicios, y así lo hace notar Umaña cuando señala “*No cabe duda de que las entidades de certificación digital distribuyen productos dentro del giro ordinario de negocios...actúa usualmente como intermediaria en la venta de aparatos (la tarjeta inteligente y/o los token criptográficos), toda vez que no los produce. Es en ese sentido que se afirma que distribuye productos.*” (A.F. Umaña, 2003: 441).

⁴⁸¹ (J. F. Ortega, 2008:153-164).

⁴⁸² (J. F. Ortega, 2008:153-164). Un análisis sobre el servicio de acuse de recibo es igualmente efectuado por Juan Ignacio Alcaraz Carsi, “Breve comentario sobre la notificación del acuse de recibo del prestador de servicios de la Sociedad de la Información”, en *REDI: Revista Electrónica de Derecho Informático*, No. 21, España, Alfa-Redi, abril/2000, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=448>

iii) Servicio de homologación de certificados.-

De conformidad con el art. 14 LFE que hace referencia a la equivalencia internacional de certificados reconocidos, los certificados electrónicos que se emiten al público como reconocidos por los PSC que se encuentran establecidos en un Estado que no sea miembro del Espacio Económico Europeo (EEE) - conforme a la normativa aplicable en dicho Estado - serán equivalentes a los emitidos por los PSC establecidos en territorio español, siempre que se cumpla alguna de las condiciones especificadas en los incs. a), b) o c) de dicho artículo, las cuales se corresponden en el ordenamiento comunitario con los incs. a), b) o c) del art. 7 de la DFE.⁴⁸³

La condición contemplada en el art. 14, inc. b) LFE (correspondiente con el art. 7.1.b. DFE) impone como condición dos aspectos: i) el hecho que el certificado esté garantizado por un PSC establecido en el EEE, y ii) que el PSC observe los requisitos establecidos en la DFE para la emisión de certificados reconocidos. De ese modo se configura la prestación del *servicio de homologación* de certificado reconocido, el cual es brindado por un PSC situado en el EEE que cumple las normas comunitarias de firma electrónica.

La homologación consecuentemente puede ser efectuada por un PSC establecido en España, que como se tiene dicho constituye un servicio por el cual, el PSC radicado en territorio español y previo acatamiento a las disposiciones comunitarias (y españolas consideramos) avala la calidad de los certificados emitidos con carácter de reconocidos por un PSC extranjero, igualando sus efectos a los certificados emitidos por los PSC establecidos en España y, por consiguiente, a los radicados dentro del EEE.⁴⁸⁴

⁴⁸³ De igual manera en la LMFE es posible encontrar en el art. 12.2. una referencia respecto del reconocimiento de certificados extranjeros: “2. Todo certificado expedido fuera [del Estado promulgante] producirá los mismos efectos jurídicos en [el Estado promulgante] que todo certificado expedido en [el Estado promulgante] si presenta un grado de fiabilidad sustancialmente equivalente.”

⁴⁸⁴ “...si no existe una ICP internacional, pueden surgir una serie de problemas con respecto al reconocimiento de certificados por parte de entidades certificadoras de países extranjeros. El reconocimiento de certificados extranjeros se realiza generalmente mediante un método denominado “certificación cruzada”. En tales casos es necesario que entidades certificadoras sustancialmente equivalentes (o entidades certificadoras dispuestas a asumir ciertos riesgos con respecto a los certificados emitidos por otras entidades certificadoras) reconozcan mutuamente los servicios prestados, de forma que los respectivos usuarios puedan comunicarse entre ellos de manera más eficaz y con mayor confianza en la fiabilidad de los certificados que se emitan.” (ONU, 2002: 33-34).

Cabe aclarar que el servicio de homologación contrariamente a lo que podría pensarse, no es prestado a los Firmantes/Suscriptores de los certificados emitidos, sino que son los terceros Usuarios que confían en los certificados emitidos por el PSC extranjero y que han sido homologados por el PSC domiciliado en España, los verdaderos destinatarios de este servicio. En suma, lo que se pretende con la homologación es extender la validez de los certificados de firma electrónica avanzada emitidos como reconocidos por PSC extranjeros.

4.2.5. Obligaciones de la Entidad de Registro (ER).-

Como se ha venido estudiando, la Entidad de Registro (ER) constituye una entidad que actúa, ya sea en relación de dependencia del PSC (forma parte de la estructura empresarial del certificador, a modo de unidad encomendada), ya sea mediante contrato o acuerdo suscrito con el PSC (sujeto independiente); en cualquiera de los dos casos, modulando sus actividades de conformidad a lo estipulado en la Declaración de Prácticas (DPC) y Políticas de Certificación (PC) emitidos por el PSC.

Por consiguiente las ER son entidades encargadas de efectuar determinadas tareas que hacen a las labores de certificación, siendo en todo caso el PSC el responsable directo de los servicios que ésta proporciona, debiendo responder por los ocasionales daños que la negligencia de la ER pueda originar frente al Firmante/Suscriptor, los Usuarios de certificados u otros terceros afectados.

Con las consideraciones anotadas pasemos a efectuar un repaso a los deberes de la ER, que como se tiene dicho, en realidad no son otra cosa que las obligaciones propias del PSC delegadas en otro sujeto, los cuales pueden variar (siendo más amplias o restringidas) en función de la DPC y las PC de cada certificador en concreto.

- En primer lugar, la ER se encuentra obligada a respetar lo dispuesto en la DPC y las PC correspondientes al PSC.

- Por otra parte debe proteger la seguridad de sus claves privadas, las cuales emplea entre otras cosas precisamente para comunicarse de forma segura con el PSC, por ejemplo para remitirle las solicitudes de certificados efectuadas junto con toda la información relacionada al Solicitante.
- Sin duda alguna que su deber y responsabilidad más importante consiste en comprobar debidamente la identidad de los Solicitantes y Firmantes/Suscriptores de los certificados reconocidos que emitirá el PSC (art.13.5. LFE).
- Directamente vinculada con la anterior, está la obligación de verificar la exactitud y autenticidad de toda la demás información suministrada por el Solicitante, como por ejemplo: sus datos personales, dirección, teléfono, fax, dirección de correo electrónico, poderes de representación, documentos que autentiquen en caso de personas jurídicas los datos de constitución y registro correspondientes, así como verificar cualquier otra circunstancia o atributos del Solicitante que sean necesarios para emitir el certificado reconocido.
- De la misma forma la ER debe proceder al archivo y custodia por el periodo dispuesto en la legislación vigente (quince años), de los documentos suministrados por el solicitante o Firmante/Suscriptor.
- Por otra parte la ER debe dar curso a las solicitudes de suspensión, renovación o revocación de un certificado reconocido.
- También figuran entre sus responsabilidades, cuando el PSC no lo hace de modo directo, el hecho de comunicar al Firmante/Suscriptor la suspensión o revocación del certificado reconocido por medio de e-mail, un sistema *on line*, teléfono, fax, correo ordinario o cualquier otra forma adecuada al supuesto concreto.

- Igualmente importante es el deber de la ER de respetar y observar las reglas de conducta que emanan del contrato de certificación reconocida celebrado entre el PSC y el Firmante/Suscriptor.
- Finalmente, la ER se obliga a informar al PSC de las causas de suspensión, revocación y/o extinción del certificado reconocido, siempre y cuando tome conocimiento de ello

4.3. Obligaciones del Firmante/Suscriptor.-

Examinadas las obligaciones del PSC, distinguiremos a continuación las obligaciones que asume el Firmante/Suscriptor de un certificado reconocido en virtud del contrato celebrado. Conforme se argumentó en su momento, la obligación principal consiste en pagar el precio establecido por el certificado contratado así como por los demás servicios adicionales que haya solicitado; además, el Firmante/Suscriptor asume ciertos deberes de conducta que surgen de la buena fe contractual y el contenido adicional del contrato.

Con las consideraciones previamente enunciadas, pasemos al estudio de las obligaciones que asume el Firmante/Suscriptor de un certificado reconocido.

4.3.1. Obligación principal.-

- Pago del precio como contraprestación por el servicio⁴⁸⁵

La básica y fundamental obligación del Firmante/Suscriptor consiste en el pago del precio como contraprestación por los servicios recibidos. En la mayoría de las ocasiones el precio consistirá en la entrega de una suma de dinero, configurándose por tanto una obligación pecuniaria.

Sobre el particular es necesario efectuar algunas precisiones. El artículo 1.544 C.c. define el contrato de arrendamiento de obras o servicios como un contrato oneroso, al establecer como requisito del mismo “*el precio cierto*” en calidad de contraprestación o pago

⁴⁸⁵ Para la construcción del presente apartado, por lo orientador y claro, nos hemos basado sobre todo en el trabajo de María Dolores Cervilla (M. Cervilla, 2001: 161 y ss.). De igual modo han servido de guía los siguientes documentos: Convención de Viena sobre Compraventa Internacional de Mercaderías (1980); los Principios de Derecho Europeo. Contratos de Servicios (PEL-SC); y los Principios UNIDROIT sobre contratos comerciales internacionales

por la obra ejecutada o el servicio prestado por el deudor. Nótese que ante tal ambigüedad o parquedad han sido muchos los problemas planteados sobre la interpretación del requisito del precio cierto.

Con carácter general, la doctrina aboga por una interpretación amplia del requisito de la certeza exigido en el C.c. español en relación a la remuneración debida por el receptor de los servicios prestados. Interpretación extensa que permite entender cumplido el requisito, cuando se pactó el precio sin estipular cuantía y refiriéndose a unas tarifas profesionales, o bien, cuando nada se pactó al respecto pero los usos o costumbres establecen la obligación de retribuir tal o cual prestación.⁴⁸⁶ No nos olvidemos que el art. 2 del C.com. señala que los actos de comercio se regirán por las disposiciones contenidas en él; en su defecto, por los usos del comercio observados generalmente en cada plaza; y a falta de ambas reglas, por las del Derecho común.

Las relaciones jurídicas objeto de nuestro estudio son relaciones caracterizadas por su onerosidad, que vienen determinadas por la profesionalidad del sujeto prestador del servicio. Onerosidad y profesionalidad son conceptos que van íntimamente relacionados con una justificación con base económica y empresarial evidente: el PSC, cuando lleva a cabo la actividad propia de su oficio lo hace guiado por un motivo no altruista, tal cual es el *animus lucrandi*. Pero la profesionalidad no es motivo que justifique la onerosidad de la relación profesional-cliente en la actualidad, ya que al regularse estas relaciones bajo el esquema normativo del arrendamiento de servicios estas son onerosas, no porque el sujeto prestador sea profesional, sino porque el arrendamiento de obras o servicios es un contrato esencialmente oneroso.⁴⁸⁷

⁴⁸⁶ (M. Cervilla, 2001: 81).

⁴⁸⁷ (M. Cervilla, 2001: 161).

Sentada la onerosidad con los apuntes antes mencionados de la relación jurídica PSC-Firmante/Suscriptor, ingresaremos a continuación a analizar otras cuestiones en torno al precio que se plantean cuando el sujeto de esta relación jurídica es un empresario profesional.

Conforme se tiene adelantado, el artículo 1.544 C.c. al definir el contrato de arrendamiento de servicios como contrato oneroso, lo hace exigiendo como objeto del mismo la existencia de “*precio cierto*”. Por ello, el precio cierto se configura como objeto del contrato de arrendamiento de servicios y como tal su existencia condiciona la validez del contrato.

El artículo 1.261 C.c. al igual que el artículo 1.544 C.c. exigen que el objeto del contrato sea cierto, lo que nos invita a concretar el significado del término “cierto”. Así el objeto del contrato, en este caso el precio, será cierto cuando sea determinado o determinable según las reglas generales, tal y como lo establece el artículo 1.273 C.c..

No presenta por consiguiente problema alguno, cuando el precio de los servicios está determinado por acuerdo expreso o tácito de las partes con anterioridad a la contratación de los servicios. Con toda lógica y dentro el ámbito de la autonomía de la voluntad, las partes pueden acordar el precio que deseen sobre el servicio contratado, precio cuya cuantía puede ser superior o inferior al que normalmente se establezca en el mercado. En este supuesto, el precio de la relación jurídica establecida entre profesional-cliente será cierto por estar determinado con anterioridad a concertarse la relación.

El problema sobreviene cuando el precio no se encuentra determinado a momento de perfeccionarse el contrato. Al respecto, consideramos que pueden ser de ayuda - obviamente salvando las distancias correspondientes - las normas de la CVCIM y los PUNIDROIT, las cuales pasaremos a estudiar sintéticamente y a título informativo, en procura de guía y orientación en la problemática planteada.

El carácter oneroso de la relación jurídica de certificación supone que para la empresa certificadora el objeto fundamental del contrato estriba en la obtención de un precio. El sinalagma del contrato de certificación queda por consiguiente completo mediante la estipulación de la retribución a percibir por el PSC. Pero cuando el precio no ha sido fijado de antemano por las partes interesa mencionar a este respecto, que, por analogía con lo dispuesto en la CVCIM (art. 14) el contrato de certificación debe ser considerado como perfectamente válido, porque *“una propuesta es suficientemente precisa si indica las mercaderías y, expresa o tácitamente, señala la cantidad o el precio o prevé un medio para determinarlos”*, conforme afirma la mencionada norma de la CVCIM.

Y posteriormente, tanto la CVCIM como los PUNIDROIT van más lejos y regulan la posibilidad de la existencia de los denominados *open price contracts*.⁴⁸⁸ Así el art. 55 de la CVCIM ordena *“Cuando el contrato haya sido válidamente celebrado pero en él ni expresa ni tácitamente se haya señalado el precio o estipulado un medio para determinarlo, se considerará, salvo indicación en contrario, que las partes han hecho referencia implícita al precio generalmente cobrado en el momento de la celebración del contrato por tales mercaderías, vendidas en circunstancias semejantes, en el tráfico mercantil de que se trate”*.

Resulta también orientador el criterio seguido por los PECL-SC, que en su art. 1:102(2) establece: *“Where the contract does not fix the price or the method of determining it, the price is the market price generally charged at the time of the conclusion of the contract.”*

Los PUNIDROIT dan un paso ulterior y precisan que si no puede determinarse el precio con arreglo al tráfico mercantil de que se trate, se acuda al criterio del precio *razonable* (art. 5.1.7.1). El criterio del precio razonable se utiliza repetidamente en el precepto analizado de los PUNIDROIT, así, cuando el precio debe fijarse por una de las partes y su

⁴⁸⁸ Para una discusión detallada del problema del precio en la CVCIM de 1980 y también en los PUNIDROIT que resuelve la aparente contradicción entre los artículos 14 y 55 del Texto vienés, consultar P. Perales Viscasillas, *La formación del contrato de compraventa internacional de mercaderías*, Valencia, Tirant Lo Blanch, 1996, p. 315 y ss..

determinación es manifiestamente no razonable, el precio razonable sustituye a aquél, incluso si existe estipulación en contrario en el contrato (art. 5.1.7.2); del mismo modo, si es un tercero el que debe establecer el precio y no puede o no lo precisa, el precio del contrato debe ser un precio razonable (art. 5.1.7.3).⁴⁸⁹

Por lo tanto, en nuestra opinión el contrato de certificación reconocida debe considerarse válidamente celebrado si existe una estipulación sobre el precio, si sólo se establecen criterios de determinación del precio e incluso si no existe pacto *ad hoc*. En este último caso, el tráfico mercantil de que se trata en el momento de la conclusión del contrato puede facilitar el correspondiente precio.

4.3.2. Obligaciones accesorias.-

i) Actuar de Buena fe

De acuerdo a lo que se tiene ampliamente analizado, en virtud de lo dispuesto en el art. 57 C.com. y el art. 1.258 C.c., el Firmante/Suscriptor tanto a momento de efectuar los tratos preliminares como durante la ejecución propiamente del contrato, debe actuar conforme al principio-deber de *Buena fe*. Además está obligado lógicamente a cumplir de manera general con lo dispuesto por la normativa sobre firma electrónica vigente.

ii) Conservar diligentemente su clave privada

La conservación diligente de su clave privada (datos de creación de firma) sin duda alguna se configura como uno de los deberes fundamentales del Firmante/Suscriptor, toda vez que junto con la generación y entrega de la misma empleando medios fiables (obligación del PSC), de la custodia segura de la clave privada depende completamente toda la certeza y confiabilidad de un sistema de certificados digitales (art.23.1.c. LFE; art. 8.1.a. LMFE).

El más mínimo resquebrajamiento en la tenencia confidencial de la clave privada, puede devenir en consecuencias desastrosas, pues un tercero que haya tenido acceso a la

⁴⁸⁹ El artículo 5.1.7.4 de los PUNIDROIT establece un ulterior método de fijación del precio: “Si el precio tiene que determinarse por referencia a factores que no existen o han dejado de existir o de ser accesibles, el factor equivalente más cercano se considerará como sustituto”.

misma podría hacer uso ilegítimo y fraudulento de ella, procediendo a firmar documentos electrónicos a nombre y por cuenta del titular de firma electrónica, quien puede verse gravemente perjudicado por los daños subsecuentes que se ocasionarían a los Usuarios del certificado u otros terceros afectados (en el último caso debe responder extracontractualmente), quienes creyendo estar efectuando transacciones de comercio electrónico en sentido estricto con el Firmante/Suscriptor, dejándose llevar por la apariencia creada y la confianza depositada en el certificado reconocido que contiene la clave pública relacionada con la privada (con la que precisamente procederán a autenticar la firma electrónica adjunta al mensaje de datos emitido por el emisor suplantador) se verían engañados.

Precisamente por las razones apuntadas, el Firmante/Suscriptor debe asegurarse de conservar por todos los medios y haciendo uso de todos los procedimientos de seguridad recomendados, la reserva y confidencialidad de su clave privada, omisión que genera una limitación en la responsabilidad del PSC y la asunción de toda ella por el Firmante/Suscriptor.⁴⁹⁰

Esta obligación se extiende no únicamente al resguardo efectivo y seguro de la clave privada sino también a la guarda igualmente segura de los códigos de acceso, números PIN o *passwords* que facultan el acceso del Firmante/Suscriptor al dispositivo tecnológico en el que se halla contenida la clave privada (y normalmente también se encuentra depositado el certificado reconocido).

iii) Comunicar la puesta en peligro o pérdida de su clave privada

Directamente relacionada con la anterior, el Firmante/Suscriptor posee la obligación de comunicar al PSC los casos en los que su clave privada se ha puesto en peligro, ha sido extraviada o de cualquier otra manera se ve comprometida (art. 23.1.d. LFE; 8.1.b. LMFE).⁴⁹¹

⁴⁹⁰ El art. 8.1.a. de la LMFE contiene esta previsión señalando que es deber del firmante “actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma.”

⁴⁹¹ El art. 8.1.b. de la LMFE dispone que constituye deber del firmante “sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme al artículo 9 de la presente Ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar

Así por ejemplo, cuando tiene conocimiento de ataques externos a su sistema por los denominados *hackers* o piratas informáticos, que son programadores expertos que logran romper la secuencia matemática de la clave privada y descifrarla (lo cual si bien es poco probable, no es descartable).

De otra, cuando accidentalmente ha perdido la clave o cuando de cualquier otra forma tiene severas sospechas de que la integridad o fiabilidad de su clave privada se encuentra en entredicho, entonces su deber es advertir de esta situación al PSC, quien por razones de seguridad estricta y ante el advenimiento de tales hechos que colocan en vilo la certeza y confiabilidad del sistema de certificados, deberá proceder a revocar el certificado reconocido publicando dicha circunstancia en el directorio correspondiente, a efectos que los Usuarios del certificado tomen conocimiento y retiren su confianza a los mensajes firmados con posterioridad a la extinción del certificado.

iv) Respetar las condiciones de empleo del certificado conforme la DPC

Lógicamente que actuar dentro del marco general proporcionado por la Declaración de Prácticas de Certificación (DPC) constituye un ineludible deber del Firmante/Suscriptor, quien además se encuentra llamado a observar y respetar las Políticas de Certificación (PC) asociadas al certificado reconocido que solicita, ya sea que se trate de un certificado emitido a favor de una persona física, bien cuando se trate de un certificado generado para una persona jurídica (art. 23.1.f. LFE).

En ese entendido, la DPC y las PC vinculadas al certificado acotan las reglas en base a las cuales el Firmante/Suscriptor debe emplear el certificado reconocido, debiendo respetarlas y no encontrándose facultado para dar al certificado un uso distinto del previsto en dichos documentos.

servicios que la apoyen si: i) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho.”

De manera que el empleo de los certificados que consiste en la ejecución de operaciones no autorizadas según la DPC y las PC aplicables en concreto al certificado reconocido solicitado, tendrán el carácter de usos indebidos o prohibidos a los efectos legales correspondientes, eximiéndose en consecuencia el PCS en función de la legislación aplicable, de cualquier responsabilidad por el uso indebido de los certificados por parte del Firmante/Suscriptor.

En la práctica comercial se prohíbe el empleo del certificado reconocido para:

- Firmar otro certificado.
- Firmar software o componentes.
- Generar sellos de tiempo para procedimientos de *Fechado electrónico*.
- Prestar servicios a título gratuito u oneroso, como por ejemplo: prestar servicios de OCSP; generar Listas de Revocación; prestar servicios de notificación, u otros.

v) Respetar los límites de uso del certificado

El Firmante/Suscriptor de igual modo tiene la obligación de respetar las restricciones que figuren en el certificado electrónico en cuanto a los posibles usos de las transacciones que puedan realizarse con él (art. 23.1.f. LFE). Estas restricciones se denominan también limitaciones *cualitativas* del certificado.

Las restricciones pueden provenir del PSC, quien las hace conocer a través de la DPC y las PC asociadas al certificado reconocido que solicita el Firmante/Suscriptor, o también pueden haber sido solicitadas por el propio Firmante/Suscriptor al momento de la solicitud de emisión del certificado.

Así, cuando un certificado ha sido emitido para que sea empleado en el ámbito mercantil, es decir, para que el Firmante/Suscriptor se relacione electrónicamente con otras entidades a fines estrictamente comerciales, resulta evidente que éste precisamente constituye el límite de uso de dicho certificado, no pudiendo efectuar otro tipo de operaciones con su

respaldo, de modo que no podrá emplearse el certificado por ejemplo para el ámbito de relaciones con las Administraciones Públicas (v.gr. la Administración Tributaria).

vi) Respetar los límites de los importes que figuran en el certificado

El Firmante/Suscriptor de igual forma tiene la obligación de respetar las restricciones que figuren en el certificado electrónico en cuanto al importe individualizado de las transacciones que puedan realizarse con él (art. 23.1.f. LFE). Estas restricciones se denominan también limitaciones *cuantitativas* del certificado.

A semejanza del caso anterior, las restricciones pueden provenir el PSC, quien las hace conocer a través de la DPC y las PC asociadas el certificado reconocido que solicita el Firmante/Suscriptor, o también su inclusión puede haber sido solicitada por el propio Firmante/Suscriptor al momento de la solicitud de emisión del certificado. Este tipo de certificados se conocen como *Certificados transaccionales*.⁴⁹²

Así por ejemplo, cuando un certificado ha sido emitido con un límite de hasta 50.000 euros, resulta evidente que éste precisamente constituye el límite del importe de dicho certificado, no pudiendo efectuarse transacciones comerciales que superen dicho monto con su respaldo.

vii) Comunicar los cambios de la información reflejada en el certificado.

En las ocasiones que la información inicialmente proporcionada por el Solicitante para confeccionar el certificado reconocido sufra cambios posteriores, ésta debe ser inmediatamente comunicada al PSC; es decir, el Firmante/Suscriptor debe notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez (art.23.1.b. LFE; 8.1.c. LMFE).⁴⁹³

⁴⁹² Sobre los certificados transaccionales: (J.F. Ortega, 2008: 370-374).

⁴⁹³ El art. 8.1.c. de la LMFE dispone que constituye deber del firmante “cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.”

Esto ocurrirá normalmente en el caso de los denominados certificados de atributos, reconocidos en el art. 11.3 LFE, los cuales incluyen cualquier otra circunstancia o atributo específico del Firmante/Suscriptor, y especialmente, cuando se trata de certificados de atributos dinámicos contemplados en el art. 11.4. LFE, que son aquellos que admiten una relación de representación.

Tómese en cuenta que tanto los atributos específicos señalados en el art. 11.3. LFE (v.gr. pertenencia a un colegio profesional) como los atributos dinámicos (v.gr. poder de representación) pueden variar en el transcurso del tiempo, de manera que los datos consignados al momento de la solicitud y perfeccionamiento del contrato de certificación reconocida pueden devenir en cambios o actualizaciones; siguiendo los ejemplos señalados, por expulsión del profesional al colegio al que pertenecía, o por cambio de representante en el caso de personas jurídicas (lo que apareja la emisión de nuevos poderes para el flamante representante), ocasiones todas estas que demandan por parte del Firmante/Suscriptor la comunicación al PSC de las nuevas circunstancias y la nueva información, que deberá ser incorporada en el certificado.

En otras palabras y sintetizando ideas, diremos que recae sobre el Firmante/Suscriptor la carga de notificar cualquier cambio en los datos aportados inicialmente para la creación del certificado reconocido.

viii) Solicitar la suspensión o revocación del certificado oportunamente

Cuando los hechos y las circunstancias lo demanden, el Firmante/Suscriptor esta en la obligación de solicitar al PSC en sentido que proceda a suspender o revocar el certificado reconocido emitido en su favor (art.23.1.d. LFE). En otras palabras, debe informar a la mayor brevedad posible de la existencia de alguna causa de suspensión o extinción del certificado, si es de su conocimiento por supuesto.

Ello ocurrirá en oportunidad de verificarse las causales de extinción y suspensión de un certificado electrónico contenidas en los arts. 8 y 9 LFE, debiendo proceder el PSC de conformidad al procedimiento señalado en el art. 10 LFE.

Las causales más típicas y representativas consisten en la pérdida, violación o puesta en peligro de la clave privada por parte del Firmante/Suscriptor, lo que da lugar a una revocación del certificado y su consiguiente extinción; por otra parte, puede tratarse de una resolución judicial o administrativa que ordene simplemente la suspensión del certificado, oportunidad en la que si el Firmante/Suscriptor ha tenido conocimiento de ello y previamente a que el PSC se anoticie y proceda en consecuencia, debe comunicar al PSC de la situación, la cual no admite excusas, debiendo en todo caso responder el Firmante/Suscriptor por los eventuales daños que puedan ocasionarse, si es que a pesar de su conocimiento de la existencia de causales de extinción o suspensión de certificados, no procede a comunicarlas oportunamente al PSC.

ix) No utilizar la clave privada en caso de suspensión o extinción del certificado

Concatenada con la previsión precedente, se encuentra el deber el Firmante/Suscriptor de abstenerse en todo tipo de uso de su clave privada y del certificado: cuando haya expirado el período de validez del certificado; en ocasión que el PSC tenga formalmente informado en su directorio de certificados que ha procedido a efectuar la suspensión, revocación y/o extinción del certificado reconocido.

En caso contrario asume las eventuales responsabilidades únicamente el Firmante/Suscriptor, quien por su negligencia deberá soportar y hacer frente a la responsabilidad civil que seguramente traerá aparejada la violación a su deber, siempre que se hubiesen ocasionado daños (art.23.1.e. LFE).

En otras palabras el Firmante/Suscriptor no debe utilizar la clave privada ni el certificado asociado a la misma, desde el momento en que éste solicita o es advertido por el

PSC o la ER de la suspensión, revocación y/o extinción del certificado; tampoco una vez expirado el plazo de validez del certificado.

V. Contexto de las Obligaciones del Usuario.-

Analizadas las prestaciones que hacen tanto al PSC como al Firmante/Suscriptor y llegados a este punto, cabe analizar el contenido de las obligaciones que recaen sobre el Usuario del certificado reconocido.

Conforme se tiene adelantado la utilidad práctica de esta labor reside en el hecho que, precisados los deberes del Usuario y establecido el origen de los mismos, podremos integrarlos dentro del concierto de obligaciones que incumben a los otros dos sujetos que participan en las actividades de certificación (PSC y Firmante/Suscriptor), lo que nos permitirá finalmente modular con mayor precisión el régimen de responsabilidad (contractual o extracontractual) que concierne a cada una de las entidades subjetivas involucradas.

Y en el caso específico que alude a la responsabilidad del PSC, resulta de suma importancia determinar los casos en que la conducta del Usuario del certificado será considerada negligente, como consecuencia de la inobservancia de sus obligaciones, debido a que estos factores determinarán finalmente la limitación o exención de responsabilidad del PSC, según sea el caso.

Antes de ingresar de lleno en la materia resulta necesario efectuar algunas matizaciones. De acuerdo a lo analizado hasta el momento, el conjunto de obligaciones que modulan los deberes del PSC y el Firmante/Suscriptor, al margen de configurarse como obligaciones legales, previstas en el contrato de certificación reconocida se modulan como verdaderas obligaciones contractuales.

Nos anticipamos también en señalar que la interrogante surge a momento de considerar el origen de las obligaciones que atingen al Usuario del certificado reconocido, pues salta la duda respecto a cómo es posible que para el Usuario del certificado devengan

una serie de obligaciones desde el momento que acude al directorio y/o servicio de consulta sobre el estado del certificado, el cual ha sido emitido por el PSC en cumplimiento de los deberes que devienen de la relación contractual que éste mantiene con el Firmante/Suscriptor, como consecuencia del perfeccionamiento del contrato de certificación reconocida.

Y ello independientemente del hecho que el Usuario del certificado revista la condición de parte contractual del Firmante/Suscriptor en el ámbito del comercio electrónico en sentido estricto, en virtud de la relación subyacente al intercambio electrónico que existe entre ambos, pues es evidente que el Usuario del certificado respecto del contrato de certificación reconocida es un tercero.

Por lo que desde nuestro punto de vista queda absolutamente claro que los deberes del Usuario del certificado no nacen del contrato de certificación reconocida, lo cual es lógico, pues los contratos únicamente obligan a las partes contratantes (principio de relatividad del contrato art. 1.257 C.c.), no pudiendo atribuirse obligaciones a un sujeto ajeno a la relación contractual.

Somos de la opinión que la respuesta a la interrogante planteada debemos encontrarla - al menos en principio - en la ley. Efectivamente, de conformidad a lo dispuesto por el art. 1.089 C.c. las obligaciones nacen, entre otras fuentes, de la ley. A su vez la doctrina se ha ocupado de reducir la enumeración de las fuentes de las obligaciones a una clasificación bimembre: la autonomía privada (contratos, actos jurídicos mortis causa, etc.) y la constitución heterónoma (actos administrativos y judiciales, obligaciones nacidas de la ley, etc.).⁴⁹⁴

En ese entendido comprendemos que en el caso de Usuario del certificado, los deberes que le conciernen tienen - al menos de inicio - como origen directo a la LFE. Si bien como se ha explicado, tanto la normativa comunitaria como española no se detienen a

⁴⁹⁴ Luís Díez-Picazo, *Fundamentos del Derecho Civil Patrimonial*, vol. II, Madrid, Civitas, 1996, 5ª. ed., pp. 141-155.

enumerar expresamente dichas obligaciones, las mismas se pueden inferir particularmente de la interpretación extensiva que se haga del art. 23.4. LFE.

Con las consideraciones enunciadas, procuraremos a continuación construir e identificar el régimen de las obligaciones generales que recaen sobre el Usuario del certificado, anticipándonos en anunciar que resultarán especial e igualmente orientadoras en esa labor, las disposiciones contenidas en el art. 11 LMFE.

5.1. Obligaciones del Usuario previstas en la LFE.-

i) Observar y cumplir las disposiciones de la LFE

En primer lugar, el Usuario de un certificado reconocido se encuentra obligado a cumplir con las disposiciones generales contenidas en la normativa sobre firma electrónica, toda vez que al ser una norma imperativa, demanda su observancia en todo cuanto le fuera aplicable.

Al mismo tiempo debe observar las disposiciones específicas contenidas en el art. 23.4 de la LFE, el cual, si bien se refiere a los límites de responsabilidad del PSC, por interpretación extensiva contiene verdaderas obligaciones del Usuario, las cuales consisten básicamente en un deber de diligencia, mismas que analizaremos con mayor detenimiento a continuación.

ii) Actuar de manera diligente

La fundamental obligación del Usuario del certificado reside en conducir sus acciones de manera diligente. En ese entendido, debe actuar de modo diligente a tiempo de comprobar la vigencia y verificar la validez de los certificados cuando realiza cualquier operación basada en los mismos.

De hecho en la Exposición de Motivos de la LFE, concretamente el último párrafo de su apartado II, se expresa “*Adicionalmente, la ley establece un marco de obligaciones aplicables a los prestadores de servicios de certificación, en función de si éstos emiten*

*certificados reconocidos o no, y determina su régimen de responsabilidad, **teniendo en cuenta los deberes de diligencia que incumben a los firmantes y a los terceros destinatarios de documentos firmados electrónicamente***” (las negrillas son nuestras).

Este deber de diligencia se desprende del contenido del art. 23.4. LFE, cuyas disposiciones - en base a una interpretación extensiva como se tiene dicho - permiten inferir que el Usuario debe proceder de modo diligente a momento de comprobar la vigencia y validez del certificado reconocido, pues en caso contrario se entenderá que el Usuario actúa de forma negligente, lo que determina que el PSC no será responsable por los daños y perjuicios que pudieran ocasionarse al Firmante/Suscriptor o a terceros de buena fe, recayendo dicha responsabilidad en todo caso, en el Usuario negligente.

A continuación analizaremos con un poco más de detalle en qué consiste este deber de diligencia, que se fracciona en una triple manifestación.

ii.1.) Comprobar la suspensión o extinción del certificado

La diligencia debida en la actuación del Usuario del certificado, en primer lugar, demanda por parte de éste la obligación de comprobar y tener en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados, así como verificar la firma electrónica (art. 23.4.b. LFE)

De modo que el Usuario del certificado debe constatar, pero sobre todo tomar en cuenta si el certificado se halla suspendido, de conformidad a las previsiones del art. 9 LFE, o si el mismo ha sufrido una extinción, de acuerdo con las disposiciones del art. 8 LFE. Además debe verificar de modo efectivo la firma electrónica adjunta al mensaje que recibe por parte del Firmante/Suscriptor⁴⁹⁵, antes de decidir si confía en el certificado.

De manera que si el Firmante/Suscriptor pretende realizar una transacción de comercio electrónico en sentido estricto con su cliente - el Usuario del certificado - éste

⁴⁹⁵ Respecto de la verificación de la firma electrónica, el art. 11.a. de la LMFE señala: “Proceder de la parte que confía en el certificado.- Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para: a) verificar la fiabilidad de la firma electrónica....”

último como primerísima medida debe proceder a comprobar la vigencia del certificado, pues en caso que no tome en cuenta el estado del certificado (suspendido, revocado y/o extinguido) y a pesar de ello proceda a concretar la transacción, el PSC se exonera de cualquier tipo de responsabilidad que podría devenir como consecuencia del uso de un certificado no operativo, siendo en todo caso responsable el Usuario negligente.

En idéntica dirección se pronuncia también el art. 11.b.i. LMFE, el cual señala que cuando la firma electrónica esté refrendada por un certificado, serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para: verificar la validez, suspensión o revocación del certificado.

ii.2.) Tener en cuenta los límites de uso del certificado

La diligencia debida en la actuación del Usuario del certificado, en segundo lugar demanda por parte de éste, la obligación de comprobar y tener en cuenta las restricciones que figuren en el certificado electrónico en cuanto a los posibles usos de las transacciones que puedan realizarse con aquél (art. 23.4.a. LFE). Estas restricciones se denominan también limitaciones *cualitativas* del certificado.

Las restricciones pueden provenir del PSC, quien las hace conocer a través de la DPC y las PC asociadas al certificado reconocido que solicita el Firmante/Suscriptor, o también pueden haber sido solicitadas por el propio Firmante/Suscriptor al momento de la solicitud de emisión del certificado. En cualquiera de los dos casos, dichas restricciones deben figurar además en el propio certificado para que sean accesibles a terceros, uno de ellos precisamente el Usuario, quien debe comprobar pero sobre todo tomar en cuenta las limitaciones de uso del certificado para decidir si confía, o no, en el mismo.

Así por ejemplo, cuando un certificado ha sido emitido para que sea empleado en el ámbito tributario, es decir, para que el Firmante/Suscriptor se relacione electrónicamente con

la Administración Tributaria, o en los casos que el certificado fue emitido con carácter general para el ámbito de relaciones con las Administraciones Públicas, Entidades y Organismos Públicos vinculados o dependientes de las mismas, resulta evidente que éste precisamente constituye el límite de uso de dicho certificado, no pudiendo efectuar otro tipo de operaciones con su respaldo, como por ejemplo transacciones comerciales.

De manera que si el Firmante/Suscriptor pretende realizar una transacción de comercio electrónico en sentido estricto con su cliente - el Usuario del certificado - éste último además de comprobar la vigencia del certificado, se encuentra obligado a verificar el límite de uso del mismo, pues en caso que no tome en cuenta dicho límite y a pesar de ello proceda a cerrar la transacción, el PSC se exonera de cualquier tipo de responsabilidad que podría devenir como consecuencia del uso indebido del certificado, siendo en todo caso responsable el Usuario negligente.

Con idéntico criterio se pronuncia también el art. 11.b.ii. de la LMFE, el cual señala que cuando la firma electrónica esté refrendada por un certificado, serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para: tener en cuenta cualquier limitación (en este caso *cualitativa*) en relación con el certificado.

ii.3.) Tener en cuenta los límites de los importes del certificado

Finalmente, la diligencia debida en la actuación del Usuario del certificado demanda por parte de éste, la obligación de comprobar y tener en cuenta las restricciones que figuren en el certificado electrónico en cuanto al importe individualizado de las transacciones que puedan realizarse con él (art. 23.4.a. LFE). Estas restricciones se denominan también limitaciones *cuantitativas* del certificado, que conforme analizamos anteriormente, dan lugar a los denominados “*Certificados transaccionales*”.

Al igual que en el caso anterior, las restricciones pueden provenir el PSC, quien las hace conocer a través de la DPC y las PC asociadas el certificado reconocido que solicita el Firmante/Suscriptor, o también su inclusión puede haber sido solicitada por el propio Firmante/Suscriptor al momento de la solicitud de emisión del certificado. En cualquiera de los dos casos, dichas restricciones deben figurar además en el propio certificado para que sean accesibles a terceros, uno de ellos precisamente el Usuario, quien debe comprobar pero sobre todo tomar en cuenta las limitaciones del importe individualizado del certificado, para decidir si confía, o no, en el certificado.

Así por ejemplo, cuando un certificado ha sido emitido con un límite de hasta 50.000 euros, resulta evidente que éste precisamente constituye el límite del importe de dicho certificado, no pudiendo efectuar transacciones comerciales que superen dicho monto con su respaldo.

De manera que si el Firmante/Suscriptor pretende realizar una transacción de comercio electrónico en sentido estricto con su cliente - el Usuario del certificado - éste último además de comprobar la vigencia del certificado, se encuentra obligado a verificar el límite del importe del mismo, pues en caso que no tome en cuenta dicho límite y a pesar de ello proceda a cerrar la transacción, el PSC se exonera de cualquier tipo de responsabilidad que podría devenir como consecuencia del uso indebido del certificado, siendo en todo caso responsable el Usuario negligente.

En ese sentido se pronuncia también el art. 11.b.ii. de la LMFE, el cual señala que cuando la firma electrónica esté refrendada por un certificado, serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para: tener en cuenta cualquier limitación (en este caso *cuantitativa*) en relación con el certificado.

iii) Conocer y sujetarse a la DPC y las PC

Finalmente pero no menos importante, el Usuario del certificado reconocido desde el momento que decide confiar de forma voluntaria en el contenido del certificado, esta igualmente obligado a conocer, sujetarse y en definitiva cumplir con lo dispuesto en la DPC y las PC del PSC que emite el certificado.

En otras palabras, el Usuario del certificado debe conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que voluntariamente confía, aceptando por consecuencia someterse a las mismas.

5.2. Factibilidad de la contractualización de las obligaciones del Usuario.-

Revistiendo las obligaciones del Usuario la categoría de auténticas obligaciones legales, al menos en inicio, cabe analizar si es posible su contractualización con el PSC, posibilidad que precisamente exploraremos a continuación, con la advertencia que esta temática es precisamente uno de los asuntos en los que la doctrina se encuentra actualmente dividida, entre quienes defienden el carácter extracontractual de la relación entre el Usuario del certificado y el PSC versus los que abogan por su contractualización.

Para comenzar diremos que en el ámbito del contrato de certificación reconocida celebrado entre el PSC y el Firmante/Suscriptor, surge una auténtica facultad para el Usuario del certificado (art.18 incs. c) y d) LFE), que se materializa en dos prerrogativas indisolublemente vinculadas y complementarias:

- Acceder a la información contenida en el certificado junto con la clave pública asociada al mismo a través de un directorio y, además
- Acceder a un servicio de consulta y verificación (o validación) sobre el estado y vigencia del certificado.

Recordemos que el certificado es precisamente el instrumento tecnológico con el que el Firmante/Suscriptor, respalda su firma electrónica en las transacciones comerciales electrónicas que mantiene con el Usuario.

En relación al primer aspecto, es decir, la facultad de acceder a la información contenida en el certificado junto con la clave pública que lleva asociada, desde el punto de vista de la factibilidad técnica, hoy en día existen diversos sistemas tecnológicos para repartir certificados digitales, pero se pueden clasificar en dos tipos o categorías básicas en función de la forma en que se distribuyen:

- i) sistema *pushing*, en el que el certificado es distribuido inicialmente por el PSC al Firmante/Suscriptor, y luego por éste al Usuario del certificado.
- ii) sistema *pull*, en el que el Usuario obtiene directamente del PSC el certificado a través de un directorio público de certificados u otros medios.⁴⁹⁶

Tómese en cuenta no obstante, que al Usuario para su completa seguridad no le basta únicamente con conocer la información reflejada en el certificado (si bien estos datos son de trascendental importancia), ya que además debe tener la posibilidad de constatar o verificar la vigencia del certificado y la veracidad de la clave pública de la firma electrónica que lleva asociada (la del Firmante/Suscriptor y contraparte en el ámbito del comercio electrónico).

Por esta razón es que independientemente del sistema tecnológico por el que se distribuya el certificado (sistema *pushing* o *pull*), el Usuario requiere adicionalmente acceder a un servicio de consulta y validación sobre el estado y vigencia del certificado.

Contextualizando la temática no olvidemos que en el ámbito de sus transacciones comerciales electrónicas, al recibir un mensaje firmado digitalmente por el Firmante/Suscriptor, el Usuario del certificado reconocido deberá proceder a verificar dicha firma, para lo cual con carácter previo debe acceder al certificado y la clave pública asociada

⁴⁹⁶ Para mayores referencias sobre los sistemas *pushing* y *pull* de distribución de certificados, consultar (A. Martínez, 2001: 204-210) // Un estudio sobre estos sistemas también se puede encontrar en Luis Miguel Rodríguez Caramelo y otros, “*Funcionamiento de los certificados digitales: un modelo didáctico*”, disponible en <http://www.ieid.org/congreso/ponencias/Rodr%EDguez%20Caramelo%20y%20otros.pdf> .

por cualquiera de los medios tecnológicos descritos (directamente del Firmante/Suscriptor - sistema *pushing* - o a través del directorio habilitado por el PSC - sistema *pull* -).

Independientemente del canal por el que obtuvo el certificado, acto seguido el Usuario debe proceder a verificar la firma digital así como el estado del certificado (vigente, suspendido o extinguido), funcionalidad que es proporcionada por el servicio de consulta o también conocido como servicio de verificación de certificados, cuya aplicación únicamente la proporciona el PSC.

Recordemos que el referido servicio de consulta se materializa normalmente a través de la LRC (*Lista de Revocación de Certificados*) y/o el servicio OCSP (*Protocolo de Estado de Certificado en línea*), los cuales deben ser habilitados por el PSC, prestación que constituye una de las obligaciones principales que devienen para el PSC como consecuencia del perfeccionamiento del contrato de certificación reconocida.

De esa manera, cuando el certificado se encuentre vigente y su clave pública asociada corresponde a la clave privada con la que el Firmante/Suscriptor rubricó electrónicamente el mensaje, el Usuario tendrá la certeza de que el certificado es fiable y de que el signatario y titular del mismo es quien dice ser. En consecuencia podrá además confiar en el contenido de la restante información que figura en el certificado, como por ejemplo la referente a los límites de los importes (cuantitativos) o de uso (cualitativos) del certificado, o en caso de tratarse de un certificado con atributos, constatarán los poderes de representación del solicitante en la ocasión que el Firmante/Suscriptor revista categoría de persona jurídica, etc..⁴⁹⁷

⁴⁹⁷ (A. Martínez, 2000: 195-221). Al respecto, Oliver indica que la seguridad a tener en cuenta en una contratación electrónica pasa, adicionalmente de la garantía de autenticidad del mensaje, imposibilidad de rechazo (no repudio en origen ni en destino), integridad y confidencialidad, porque se garantice la **actualidad** y la **disponibilidad** de la información. Respecto del servicio de actualidad, apunta que permite asegurar que no se produzca repetición de informaciones (mensajes) transmitidas previamente; en tanto que la disponibilidad radica en proporcionar un servicio continuo al usuario mediante sistemas de ordenador y comunicaciones «tolerantes a fallos», manteniendo en cifras del orden del cien por cien, lo que incide -corroborando- de forma positiva en el control de acceso al servicio. (R. Oliver, 1999: 94).

En esta parte resulta oportuno recordar que esta identificación se produce de manera simultánea con las demás funciones propias de la firma digital (autenticación, integridad, no repudio y, en su caso, confidencialidad).⁴⁹⁸

Sintetizando ideas diremos que el Firmante/Suscriptor puede distribuir certificados a sus clientes (los Usuarios) para que éstos conozcan la información contenida en el mismo y accedan a la clave pública que lleva asociada (sistema *pushing*), pero no puede proporcionar validación de certificados, facultad que únicamente está reservada al PSC (ora *ex lege*, ora contractualmente). En cambio el PSC está obligado a proporcionar ambas aplicaciones, es decir, proporcionar un directorio público de consulta de certificados (sistema *pull*) y además proporcionar servicios de verificación o validación de certificados.

Nótese en consecuencia que, de inicio, entre el Usuario del certificado y el PSC no existe propiamente una relación contractual, en tanto que la facultad del Usuario deviene de la LFE y las obligaciones del certificador hallan su origen en el contrato de certificación reconocida, salta a la vista que entre éstos evidentemente no han perfeccionado un nuevo contrato; el cumplimiento de las obligaciones del PSC se ubican en la esfera de la ejecución del único contrato, el perfeccionado con el Firmante/Suscriptor, en tanto que las obligaciones del Usuario tienen su origen en la LFE.

Lo afirmado no obstante reviste relatividad, pues si bien es cierto que en entre el PSC y el Usuario del certificado no existe un contrato previo, ello es así al menos en principio, puesto que puede darse la situación en que el Usuario al acudir al «website» del PSC, se vea obligado a aceptar un clausulado general, de manera que estas condiciones generales vincularían contractualmente al Usuario con el PSC, lo que devendría habitualmente en la formalización de un “*Contrato de verificación de certificados*”.

⁴⁹⁸ Sobre los procedimientos de consulta de certificados y validación de firmas digitales, consultar: Fernando Ramos Suárez, “La Firma Digital”, en *REDI: Revista Electrónica de Derecho Informático*, No. 10, España, Alfa-Redi, abril/1999, disponible en: <http://publicaciones.derecho.org/redi/No.%2009%20-%20Abril%20de%201999/1ramos> // Ignacio Alamillo, “Confianza digital basada en certificados”, en *REDI: Revista Electrónica de Derecho Informático*, No. 13, España, Alfa-Redi, agosto/1999, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=315> // Apol-Lònia Martínez Nadal, *Comercio electrónico, firma digital y autoridades de certificación*, Estudios de Derecho Mercantil, Madrid, Civitas, 2ª ed., 2000, pp. 195-221.

A partir de este supuesto, nuestro análisis debe reconducirse a la consideración que las obligaciones que hacen al Usuario del certificado ya no tienen un origen exclusivamente legal, conforme tenemos desarrollado previamente, sino que revisten auténticos deberes contractuales que devienen de un nuevo contrato, el perfeccionado con el PSC a través del cual se modulan sus recíprocas conductas y responsabilidades.

A momento de acudir a la doctrina especializada, constatamos que es precisamente en este sentido que se pronuncia la autora Pérez, cuando afirma:

“Las relaciones jurídicas dimanantes de un contrato de prestación de servicios de certificación, presentan ciertas particularidades con respecto a otros contratos. En particular, es importante reseñar que a la distinción tradicional entre partes contratantes (en el caso de un contrato de prestación de servicios de certificación, firmante y PSC) y terceros, se una la figura del tercero que confía en el certificado (sujeto que recibe un mensaje de datos firmado electrónicamente por el iniciador), figura con la que el PSC tiene, a nuestro juicio, una relación contractual, por cuanto que éste se obliga a mantener un registro actualizado y permitir la consulta sobre los certificados que ha emitido.”⁴⁹⁹

“Cuando el tercero que confía en el certificado, accede al registro de certificados y obtiene información, la relación entre el PSC y el tercero que confía pasa a convertirse en una relación contractual (la obligación del tercero es la de comprobar, al recibir un mensaje de datos firmado, la validez del certificado).”⁵⁰⁰

Criterio al que nos adscribimos y compartimos plenamente, de manera que establecida la naturaleza también contractual de la relación que surge entre el PSC y el Usuario del certificado reconocido, cabe efectuar algunas otras consideraciones adicionales.

Así, podría darse el caso que el PSC sujete el acceso al directorio y/o servicio de consulta sobre vigencia de los certificados al previo pago de un precio o ciertas tarifas,

⁴⁹⁹ (M. Pérez, 2009: 270-271)

⁵⁰⁰ (M. Pérez, 2009: 272).

situación que nos lleva a cuestionarnos al respecto desde una doble perspectiva de análisis: su legitimidad legal y su conveniencia comercial.

Desde el primero de los ámbitos propuestos, cabe señalar que tanto la norma comunitaria (inc. c) Anexo II DFE) como española (art. 18 incs. c. y d. LFE) sobre firma electrónica, exigen que el PSC mantenga un directorio y un servicio de consulta actualizado de certificados, pero no disponen nada respecto del precio, de manera que cabe entender que el PSC queda libre para disponer si estos servicios estarán, o no, sujetos a un pago previo.

Nótese que el PSC dará por cumplida su obligación legal (que deviene en contractual al ser incorporada en el contrato) simplemente con mantener el referido directorio y hacer accesible el servicio de consulta o verificación, independientemente de si cobra o no por ello. En ese sentido, concluimos que desde el punto de vista legal no existe ningún óbice para que el PSC condicione la consulta y/o verificación de certificados a un pago previo.

En todo caso el PSC podrá cobrar un precio por estos servicios, en la medida que el contrato de certificación reconocida celebrado con el Firmante/Suscriptor no lo prohíba expresamente, o desde otro punto de vista, dicho contrato no obligue al PSC a proporcionar gratuitamente el acceso tanto al directorio como al servicio de verificación de certificados.

En base a los razonamientos precedentes, concluimos aseverando que es factible que el PSC cobre un precio por dichos servicios o, que no lo haga, dependiendo ello en todo caso, de las previsiones que sobre el particular se hayan tomado tanto en el contrato de certificación celebrado con el Firmante/Suscriptor, como en las Declaraciones de Prácticas y Políticas de Certificación que forman parte integrante del contrato principal.

Desde el punto de vista de la conveniencia comercial de establecer, o no, un costo a los Usuarios de certificados por acceder a los servicios enunciados, parece ser que las reglas del mercado jugarían un papel preponderante, pues piénsese que aquel PSC que cobre por estos servicios, podría verse superado por su competencia que decidiría abstenerse de hacerlo

en procura de fidelizar mayores clientes y cuotas de mercado, brindando un servicio de certificación que brinde ciertas ventajas, como la apuntada, de manera que los PSC que impongan costos de consulta de certificados podrían verse desplazados por las elementales reglas de la oferta y demanda.

Como conclusión, podemos señalar que si bien desde la perspectiva legal no existen óbices para que el PSC condicione el servicio de validación de firmas electrónicas (que se ejecuta por medio del acceso a un directorio y/o un servicio de consulta sobre vigencia de certificados) al previo pago de un precio o tarifa, no es menos cierto que esta decisión podría no ser comercialmente del todo conveniente, por las razones apuntadas.

En todo caso, la realidad del tráfico español nos demuestra que la opción por la gratuidad constituye la regla prevista en los contratos de certificación, y más concretamente, en las DPC y PC de los certificadores españoles.

5.3. Criterios adversos a la contractualización.-

No obstante todo lo dicho hasta el momento, cabe resaltar que en la doctrina vigente existen autores que propugnan la naturaleza extracontractual de la relación que se entabla entre el PSC y el Usuario del certificado, de modo que a continuación efectuaremos un somero análisis al respecto para posteriormente exponer nuestras conclusiones.

En la doctrina española, uno de los autores que se ha ocupado de analizar el carácter (contractual o extra-contractual) de la relación que se entabla entre el PSC y el Usuario del certificado, como consecuencia del acceso por parte de éste último a los servicios de consulta de certificados y validación de firmas electrónicas, es Ortega Díaz, cuyos razonamientos pasamos a reflejar de manera sintética.⁵⁰¹

El referido autor defiende la tesis por la que ubica al contrato de certificación reconocida como un contrato que incluye una estipulación en favor de tercero, el Usuario del certificado, de conformidad con lo previsto en la segunda parte del art. 1.257 C.c., por la cual

⁵⁰¹ (J.F. Ortega, 2004: 417-418)

se instituye un verdadero derecho a favor del Usuario del certificado, que consiste en la facultad de acceder al referido directorio y/o servicio de consulta sobre vigencia de los certificados de manera gratuita e irrestricta.

A partir de dicho razonamiento sostiene que existe la posibilidad que el PSC imponga al Usuario del certificado, al momento de acceder a los servicios de directorio y/o verificación de certificados, a aceptar una serie de cláusulas generales, las cuales tras su conformidad determinarían hipotéticamente el surgimiento de un vínculo contractual.

Precisamente respecto a estas condiciones generales, lo primero que hace Ortega es negar su carácter contractual, sosteniendo que dichos clausulados generales no constituyen un contrato sino que únicamente adoptan su apariencia, señalando tres razones para fundamentar su afirmación, a saber:

i) Sostiene que exceden la capacidad negocial del PSC, debido a que éste no se encuentra facultado a negociar la entrega de una copia del certificado y la de su clave pública asociada al Usuario del certificado, puesto que sobre el PSC recae el deber de efectuar esa entrega, ya que en caso contrario incumple el contrato de certificación digital celebrado con el Firmante/Suscriptor, reforzando su posición al afirmar que los referidos clausulados generales no constituyen un contrato sino que, simplemente, poseen un mero valor informativo.

ii) Por otra parte opina que la pretendida relación negocial entre el PSC y el Usuario del certificado carecería de causa contractual. Para sostener su posición, menciona que en un primer momento podría pensarse que la identificación del Firmante/Suscriptor constituiría la causa contractual de este contrato aparente, pero a poco niega esta posibilidad, indicando que la identificación es el fin y, por ello, la causa contractual del contrato de certificación digital en favor de terceros (celebrado entre el PSC y el Firmante/Suscriptor), de manera que cumplido este fin mediante el contrato de certificación digital, razona que no parece posible

alegarlo como causa de un nuevo contrato, al que califica de “*superfluo e innecesario*”, lo que le lleva una vez más a negar por aplicación del art. 1.261 C.c., el carácter contractual de dicha relación.

iii) Finalmente señala que existe una prohibición normativa, por lo que sería un contrato *contra legem*.

Señala el autor que tanto en la norma derogada (RDL 14/1999, de 17 de septiembre, sobre firma electrónica) como en la actual, con carácter general se obliga a que todos los PSC permitan el acceso a sus registros de certificados a las personas que lo soliciten, es decir, los Usuarios (art. 11.c RDL; art 18.c. LFE).

Prosigue señalando que en el mismo sentido la normativa profundiza esa obligación para los PSC que emitan certificados reconocidos, exigiendo además, que esa consulta pueda efectuarse mediante la utilización de un servicio rápido y seguro (art. 12.c. RDL; art. 18.d. LFE)

De esta manera Ortega concluye asegurando que esta pretendida relación contractual vuelve a verse negada, en esta ocasión, expresa y normativamente por imperio de la Ley.

5.4. Conclusiones.-

Revisados los argumentos de Ortega y confrontados con el análisis que hiciéramos previamente, al respecto debemos señalar que no compartimos la posición manifestada por el citado autor, en cuanto consideramos que no existe óbice alguno para que el vínculo entre el PSC y el Usuario del certificado revista el carácter contractual.

En ese entendido, hemos señalado que es perfectamente posible que dicho vínculo se configure como una auténtica relación contractual, no siendo suficientes los tres argumentos enunciados por Ortega para negar dicha probabilidad: exceso de la capacidad comercial del PSC, ausencia de causa contractual y prohibición normativa.

En base a nuestros razonamientos precedentes, la dos primeras cuestiones se pueden perfectamente modular y gestionar convenientemente de modo diverso mediante el contrato de certificación, todo dependerá de las concretas previsiones que se adopten tanto en el contrato de certificación como en la DPC y las PC de la entidad certificadora; en tanto que respecto del tercer fundamento referido a la ilegalidad de este tipo de contrato, como hemos dicho, la LFE ni la DFE prohíben expresamente que entre el PSC y el Usuario del certificado se establezca una relación contractual.

Razonamientos que nos llevan a demostrar que en contra de la opinión de algunos sectores doctrinales, entre el PSC y el Usuario se configura una auténtica relación contractual, a través del que hemos denominado “*Contrato de verificación de certificados*”.

De modo tal, que la certificación reconocida se articula fundamentalmente en torno a un elemento objetivo: el certificado reconocido, a cuyo alrededor, a su vez, se interrelacionan tres elementos subjetivos: el PSC, el Firmante/Suscriptor y el Usuario del certificado, lo cual genera un entramado jurídico triangular entre tres entidades subjetivas independientes entre sí, pero vinculados por la operación económica subyacente, esta última, se modula jurídicamente a través del perfeccionamiento de dos contratos autónomos (certificación / verificación) pero funcionalmente afines, que es cabalmente la tesis que adoptaremos en la presente investigación.

Identificados con absoluta claridad el contenido y alcance de las obligaciones que atingen a cada una de las entidades subjetivas involucradas, establecidos el origen contractual de las mismas, aún nos queda modular con precisión el régimen de responsabilidad que surge en el ámbito de la certificación reconocida, labor que acometeremos precisamente en nuestro siguiente y último Capítulo.

CAPÍTULO QUINTO

RESPONSABILIDAD

I. Consideraciones preliminares.-

Desde el instante en que se produce la emisión de un certificado reconocido, pasando por la difusión y empleo del mismo, junto con la eventual suspensión del certificado (art. 9 LFE) hasta la extinción de su vigencia (art. 8 LFE), se genera una potencial situación de riesgo de la que eventualmente pueden surgir daños y perjuicios.

En ese contexto, se debe tomar en cuenta el hecho que en el ámbito de la certificación reconocida se producen una serie de vínculos entre los distintos sujetos involucrados en el sistema de certificados, es decir, el PSC, el Firmante/Suscriptor y el Usuario que confía en el certificado (en determinados casos inclusive, un tercero ajeno al sistema de certificación).⁵⁰²

La situación descrita demanda la necesidad de instituir y delimitar con la mayor claridad posible el régimen de obligaciones, derechos, pero sobretodo responsabilidades que atingen a cada uno de ellos.⁵⁰³ A lo largo de nuestro trabajo (particularmente el Cap. IV), nos hemos ocupado del estudio de las dos primeras cuestiones enunciadas, restando por consiguiente abordar el análisis de la temática referente al régimen jurídico de la responsabilidad.

⁵⁰² Efectivamente en algunas ocasiones podría verse involucrado un tercero ajeno al sistema de certificados, por ejemplo, cuando el titular del certificado suplanta la identidad de dicho tercero y actúa en su nombre con el certificado emitido.

⁵⁰³ Para mayor abundamiento con relación al régimen de responsabilidad que engloba al ámbito de la certificación de firmas electrónicas, consultar: Andrés Felipe Umaña Chaux, "Entidades de certificación: una aproximación a su régimen de responsabilidad.", en Universidad de los Andes, Grupo de Estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática, *Derecho de Internet y telecomunicaciones*, Bogotá, Legis, 2003, pp.437-469 // Paula Vallepuga González, "Responsabilidad de los Prestadores de Servicios de la Sociedad de la Información", en *REDI: Revista Electrónica de Derecho Informático*, No. 30, España, Alfa-Redi, enero/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=615> // Jorge Mario Galdos, "Responsabilidad Civil e Internet. Algunas Aproximaciones", en *REDI: Revista Electrónica de Derecho Informático*, No. 43, Buenos Aires, Alfa-Redi, febrero/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1574> // Mónica Susana Martínez Barbieri, "Responsabilidad de los Operadores de la Red que en su interacción producen daños", en *REDI: Revista Electrónica de Derecho Informático*, No. 41, Buenos Aires, Alfa-Redi, diciembre/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1003> // Catalina Merino Gaberías, "Perspectivas comunitarias en torno a los servicios de la sociedad de la información", en *REDI: Revista Electrónica de Derecho Informático*, No. 07, España, Alfa-Redi, febrero/1999, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=227> // María Pérez Pereira, "La Situación de los Proveedores de Servicios de Certificación en el Real Decreto-Ley 14/1999, Sobre Firma Electrónica", en *REDI: Revista Electrónica de Derecho Informático*, No. 017, España, Alfa-Redi, diciembre/1999, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=384> // Igualmente (R. Lorenzetti, 2001: 88-91).

Para acometer esta labor hemos de centrarnos básicamente en la responsabilidad civil, que por ejercicio de su actividad puede incurrir el principal protagonista en un sistema de certificados, nos referimos al PSC, determinando los casos en que ésta es contractual o extracontractual y estableciendo asimismo el carácter objetivo o subjetivo de la misma.

Debido a los alcances fijados en la presente investigación, no abordaremos la responsabilidad penal ni la civil derivada de delito, como tampoco nos ocuparemos de analizar la responsabilidad administrativa en que incurre el PSC, básicamente por las conductas consideradas como infracciones en el art. 31 LFE; y en ese mismo sentido, debido a que varios incumplimientos del PSC tienen una doble consideración: de incumplimiento contractual y de infracción administrativa, en nuestro trabajo nos abocaremos únicamente al análisis de los aspectos jurídico-privados de las obligaciones contraídas por el PSC.

De igual forma, si bien es evidente que la determinación del lugar de la producción del daño es fundamental para conocer dónde debe responder el PSC por los daños causados (en caso que éstos efectivamente se hayan ocasionado y sean imputables), consideramos que el análisis de esta cuestión tiene su sede más apropiada en el ámbito del Derecho procesal y del Derecho internacional privado, por lo que exceden la finalidad y ámbito (jurídico-privado) de la presente investigación.

Todo lo dicho sin óbice no obstante, de que a lo largo de nuestra exposición nos refiramos tangencialmente al régimen de responsabilidades que atingen al Firmante Suscriptor y/o al Usuario del certificado y dediquemos un espacio para ocuparnos de éstos.

Esbozado nuestro plan de trabajo en los términos señalados, iniciaremos nuestra exposición advirtiéndole que la tarea de discernir el régimen de responsabilidades emergentes para el PSC como consecuencia de sus labores certificadoras, representa un aspecto de esencial importancia y, sin embargo, conforme sostiene Martínez *“confusa en la fase inicial de desarrollo, comercial y legal, de las entidades certificadoras, pues plantea numerosas*

cuestiones tales como la naturaleza de la responsabilidad (objetiva o subjetiva; contractual o extra-contractual), la carga de la prueba, los sujetos frente a los que responde, la eventual existencia de limitaciones de uso, garantías de responsabilidad, etc.”⁵⁰⁴

Desde el momento mismo que se aprobó en 1995 la primera legislación sobre firma electrónica a nivel mundial en el Estado Norteamericano de Utah,⁵⁰⁵ se puso en evidencia que el establecimiento de un sistema específico de responsabilidad para los PSC constituía una necesidad forzosa, la premura por generar confianza en el mercado no permitía otra opción, pues remotamente se iba a confiar en un PSC que no garantizase adecuadamente su capacidad de enmendar perjuicios en caso de producir daños.

Es así que las distintas legislaciones aprobadas en materia de firma y certificados digitales (y por ende de PSC) se han preocupado, con mayor o menor detenimiento, en establecer el conjunto de deberes y responsabilidades de las partes implicadas en un sistema de certificación. La referida Ley de Utah sobre firma digital, aborda la temática delimitando con bastante precisión el conjunto de derechos y obligaciones de las partes intervinientes, al mismo tiempo que define un preciso régimen de responsabilidades.

Por otra parte, la LMFE opta por establecer de manera particularmente detallada los derechos y, en especial, las obligaciones de los sujetos implicados en el sistema de certificación (art. 8, “Proceder del firmante”; art. 9, “Proceder del prestador de servicios de certificación”; art. 11, “Proceder del tercero que confía”) y únicamente de modo indirecto norma la responsabilidad a la que dichos sujetos se encuentran llamados, en la medida que incumplen sus respectivas obligaciones, en el art. 8.2. en el caso del firmante y el art. 9.2. para el caso del PSC.

En el ámbito europeo a momento de encarar la temática de regulación del sistema de firma digital, la necesidad de contar con un marco específico que regule la responsabilidad de

⁵⁰⁴ (A. Martínez, 2004: 332). La naturaleza confusa de la responsabilidad del PSC es igualmente analizada en (R. Illescas, 2001: 139-142) // En idéntico sentido (M. Pérez, 2002: 960-965).

⁵⁰⁵ Utah Digital Signature Act, 1995.

los PSC fue igualmente sentida, debido a que la consecuencia directa de su ausencia significaba que, ante un supuesto de responsabilidad, serían de aplicación las normas del marco de responsabilidad general, lo que al margen de la respuesta ilimitada a la que tendrían que enfrentarse los PSC, suponía un grave perjuicio para los Firmantes/Suscriptores que hubiesen estado obligados a probar, en caso de daño, la falta de diligencia del PSC.⁵⁰⁶

A objeto de resolver y paliar esta situación, la DFE se ocupó específicamente de la responsabilidad del PSC en su art. 6, omitiendo efectuar una regulación completa y sistemática de los derechos y obligaciones de los distintos sujetos intervinientes en el empleo de firma electrónica y certificados.

Las disposiciones del referido art. 6 DFE - en principio - son de observancia por todos los PSC, es decir, emitan o no certificados reconocidos, siendo obligatorias para los primeros y dejando en libertad a los estados europeos para imponerlo a los PSC que emitan simples certificados electrónicos (o no reconocidos); de esa manera nótese que el referido art. 6 DFE permite solucionar con bastante atino los dos inconvenientes a los que nos referíamos previamente.

La norma comunitaria a objeto de impedir el grave perjuicio al que se verían enfrentados los Firmantes/Suscriptores al tener que, en caso de conflicto, probar la falta de diligencia del PSC, adopta la solución por la inversión de la carga de la prueba, lo que significa que el PSC para liberarse de posibles responsabilidades se encuentra en la obligación de probar que su actuación - fruto de la cual se originaron daños - no fue en todo caso negligente.

Al mismo tiempo, la DFE con la finalidad de evitar una responsabilidad ilimitada de los PSC autoriza a que éstos limiten el valor de las transacciones que figuran en el certificado que emiten, no encontrándose por consecuencia en la obligación de dar respuesta más allá del límite económico previamente fijado en el propio certificado.

⁵⁰⁶ (J.F. Ortega, 2004: 420).

Finalmente cabe resaltar a título informativo, sobre el antecedente de una *Propuesta de Directiva sobre responsabilidad civil del prestador de servicios*, que fue presentada por el Consejo a la Comisión Europea, en fecha 9 de noviembre de 1990. Conforme explica Villanueva, dos fueron las razones básicas que motivaron la adopción de una Directiva de éstas características: i) una de orden teleológico, con la finalidad de armonizar las legislaciones de los Estados miembros sobre la materia, como corolario de la realización del mercado interior; y otra de orden sistemático, con el objetivo de reunir en una Directiva horizontal una serie de servicios homogéneos, sobre el modelo de la Directiva 85/374/CEE, de responsabilidad por los daños causados por productos defectuosos.⁵⁰⁷

El centro de imputación de responsabilidad es el empresario profesional que lleva a cabo una prestación remunerada, con independencia de la forma de prestación. De manera que la extendida gama de servicios que pretendía abarcar la norma, no justificó un trato homogéneo de responsabilidad.⁵⁰⁸ De hecho, el criterio de imputación osciló desde la responsabilidad objetiva contemplada en los borradores y el Anteproyecto de Directiva, hasta la responsabilidad por culpa presunta o con inversión de la carga de la prueba prevista en el texto definitivo de la Propuesta de Directiva, que finalmente fracasó.⁵⁰⁹

En criterio de Villanueva “*La razón es evidente: no todas las prestaciones de servicios presentan las mismas características en el modo en que se organizan y ofertan en el mercado, por lo que el tratamiento unitario de la responsabilidad del genérico prestador de servicios profesional se reveló inviable*”.⁵¹⁰

⁵⁰⁷ (C. Villanueva, *Los contratos...*,2009: 570).

⁵⁰⁸ El texto consagraba un modelo de responsabilidad por culpa, pero en su art. 1.2 establecía la inversión de la carga de la prueba, fundamentada en varios argumentos: el carácter único del servicio, a veces intangible, el hecho que el servicio siempre ha desaparecido en el momento del daño y que la víctima carece de conocimientos técnicos y el profesional sí (C. Villanueva, *Los contratos...*,2009: 26).

⁵⁰⁹ (C. Villanueva, *Los servicios...*,2009:186-187).

⁵¹⁰ (C. Villanueva, *Los servicios...*,2009:187).

De modo que tal posición legislativa motivo su rechazo; frente a estas dificultades, la Comisión optó finalmente por retirar la Propuesta de Directiva de responsabilidad civil del prestador de servicios, el día 23 de junio de 1994.

II. Precisión terminológica, nociones básicas y aproximación al C.c. español.-

Con los antecedentes expuestos y a objeto de organizar mejor nuestra exposición, preliminarmente juzgamos necesario efectuar algunas precisiones terminológicas, repasar las nociones básicas que hacen a la responsabilidad civil en general, efectuando una aproximación al Código civil español, para luego ingresar de lleno en el análisis del régimen de responsabilidad civil que resulta aplicable al PSC de conformidad con la legislación española y comunitaria.

De inicio cabe advertir que entre los distintos autores españoles que se ocupan de la materia no existe unanimidad terminológica, ya que a pesar de coexistir dos clases de responsabilidad civil, la expresión “*responsabilidad civil*” se emplea normalmente para hacer alusión únicamente a la *responsabilidad civil extra-contractual*, siendo muy escasos los autores que admiten la denominación de responsabilidad civil como comprensivo e inclusivo de las dos categorías, es decir de la contractual y extra-contractual, con las correspondientes complicaciones que de ello se derivan y que no ocasionan sino otra cosa que dificultades, desde nuestro punto de vista innecesarias.

El origen de esta situación se debe a que por inspiración del Código civil francés, es muy frecuente ubicar la materia de la responsabilidad contractual contenida en la parte que los tratados dedican a los *efectos* de las obligaciones, mientras que la extra-contractual suele venir desarrollada en sede de *fuentes* de las obligaciones, división que a la postre se ha convertido en auténtica *summa divissio*, razonando los autores que si entre el agente y la víctima mediaba contrato, la responsabilidad solamente es la sanción *por el incumplimiento* de una obligación preexistente; en cambio, cuando no existe vínculo alguno entre las partes

antes de que hayan entrado en juego los principios de la responsabilidad *aquiliana*,⁵¹¹ es el propio hecho dañoso el que genera la obligación, poniendo en contacto a las partes.⁵¹²

Al respecto se pronuncia Yzquierdo indicando que “*Vistas así las cosas, es fácil entender que los autores no suelen ocuparse, al hablar de la responsabilidad contractual, de cuestiones que sí tratan, en cambio, al acometer el estudio de la extracontractual: en ésta ... (se estudia)... a) la acción u omisión antijurídica, b) el daño, c) la relación de causalidad entre la conducta y el daño, y d) el factor de atribución o imputación (culpa, dolo, riesgo, etc.) que permita imputar el resultado lesivo a un determinado patrimonio.*”⁵¹³

En otras palabras, los autores al hablar de la responsabilidad contractual, a diferencia de lo que sucede con la *aquiliana*, no hablan propiamente de *responsabilidad* sino de *incumplimiento*. Esta situación determina la apariencia por la cual pareciera que los elementos constitutivos de la responsabilidad civil únicamente correspondan a la responsabilidad civil extra-contractual, cuando lo evidente es que se trata de elementos comunes a ambas modalidades de responsabilidad.⁵¹⁴

Desde ese punto de vista queda claro que los principios de la responsabilidad *aquiliana* constituyen principios comunes y generales en la medida en que se aplicarán cuando entre las partes no se haya convenido - por medio del contrato - un medio voluntario específico.

Como sabemos, para que exista responsabilidad civil se requiere que un hecho (una acción u omisión) guarde en relación con un daño una relación de causalidad; a los que

⁵¹¹ Esta denominación proviene de la *Lex Aquilia de damno*, que en el año 808 sancionó en Roma este tipo de responsabilidad. Mariano Yzquierdo Tolsada, *Sistema de responsabilidad civil, contractual y extracontractual*, Madrid, Dykinson, 2001, p. 80.

⁵¹² (M. Yzquierdo, 2001: 80).

⁵¹³ (M. Yzquierdo, 2001: 84).

⁵¹⁴ En ese sentido Yzquierdo manifiesta que “... los principios de la responsabilidad *aquiliana* constituyen el derecho común de la teoría de la reparación de los daños civiles, siendo aplicables cuando no lo sean los que componen el régimen especial de los contratos y que conceden un medio específico para su resarcimiento: cualquier daño derivado de un hecho del hombre distinto del incumplimiento contractual será extracontractual.” (M. Yzquierdo, 2001: 85).

vendrá a añadirse un debido factor de atribución (culpa, dolo, riesgo, etc.), el cual permite finalmente justificar la imputación del daño a un determinado patrimonio.⁵¹⁵

Ahora bien, la responsabilidad puede derivarse como consecuencia de una serie de actos de diverso tipo; no obstante, todos estos pueden ser agrupados bajo dos clases o categorías básicas:

- a) Existen casos en los que encontrándose dos o más personas vinculadas por una relación obligatoria de carácter previo (un contrato), una de ellas desconoce alguno, varios o finalmente todos los términos pactados, es decir, incumple aquello a lo que se había comprometido.

En ocasiones como la descrita, decimos que existe una responsabilidad civil contractual (o por incumplimiento): el hecho que ha originado un perjuicio viene producido precisamente como resultado del incumplimiento de un contrato, el cual menoscaba el patrimonio de un acreedor que se encontraba previamente determinado por las partes. En casos como el referido, el afamado principio romano *naeminem laedere* se aplica acá en sentido de no dañar a este *concreto acreedor*.

La consumación legal de esta clase de responsabilidad en el ordenamiento civil español, se configura en base al principio de libertad y autonomía privada reflejada en el art. 1.255C.c., siendo el tenor de la obligación el parámetro fundamental (arts. 1.091 y 1.101 C.c.), pero considerando que el deber de prestación queda regido, además, por la ley (especial y después general), los usos y la buena fe, conforme prescribe el art. 1.258 C.c. Resultando aplicables además el art. 1.102 C.c. y ss..

- b) En otras ocasiones, existen sucesos en los que la responsabilidad se origina entre personas que no poseían ningún tipo de vínculo preliminar, es decir, surge entre personas que no se hallan vinculadas por una relación obligatoria de manera previa (no existe un contrato entre ellas).

⁵¹⁵ (M.Yzquierdo, 2001: 109).

En estos supuestos nos referimos a la denominada responsabilidad civil extra-contractual o también conocida como responsabilidad *aquiliana*. En esta ocasión, nótese que el acreedor no constituye una persona concreta y determinada, sino que podría llegar a ocupar este lugar cualquier miembro de la comunidad que sufra un daño, de ese modo, diremos que el deber de no dañar vincula - en principio - a la totalidad de una colectividad, de manera que la obligación de resarcir el daño ocasionado, en este caso no deviene de una relación obligatoria previa en la que el deudor ha incumplido con lo que se había comprometido, sino que proviene del genérico deber de conducta de no dañar a los otros "*alterum non laedere*".

La consumación legal de esta clase de responsabilidad en el ordenamiento civil español se encuentra en el art. 1.902 C.c. al señalar: "*El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado.*" Resultando aplicables además el art. 1.903 C.c. y ss..

Con estas anotaciones preliminares y aproximación general a la legislación civil española, proseguimos, aclarando que el alcance del concepto *responsabilidad civil* que en esta investigación manejaremos, es comprensivo de la responsabilidad contractual como de la extra-contractual o *aquiliana*, según cada caso.

III. Régimen jurídico de la responsabilidad civil del PSC en la LFE.-

Al momento que el Estado español encaró la regulación positiva de la responsabilidad de los PSC, incorporó las mismas soluciones que adoptó la DFE en la materia, inicialmente a través del RDL 14/1999, de 17 de septiembre, sobre firma electrónica (básicamente art.14), y posteriormente en la vigente LFE (principalmente art. 22).⁵¹⁶ Cabe resaltar que la norma española - a diferencia de la comunitaria (art.6 DFE) - optó en base a la libertad que esta última confiere a los estados europeos, por establecer un marco regulador de la

⁵¹⁶ Que es precisamente el artículo que traspone el marco de responsabilidad establecido por la DFE.

responsabilidad con carácter transversal, vale decir, incluyendo de modo general a todo tipo de PSC y no únicamente a los PSC que emiten certificados reconocidos.⁵¹⁷

Antes de proseguir es necesario hacer notar de manera general, que así como dejamos sentado en su oportunidad que la LFE al igual que la DFE - a diferencia de otras legislaciones⁵¹⁸ - no se ocupan de normar exhaustivamente las obligaciones de las partes que intervienen en el sistema de certificados (particularmente las que corresponden a los firmantes y usuarios),⁵¹⁹ en el caso del régimen de responsabilidades que nos incumbe, la normativa española y comunitaria tampoco ofrecen soluciones acabas.

Ello debido a que no se detienen a regular de modo sistémico los distintos supuestos que pueden generar responsabilidades, así como tampoco norman integralmente las responsabilidades que emergen para el conjunto de sujetos involucrados en el empleo de firmas y certificados electrónicos, denotando que sus disposiciones en esta materia se encuentran focalizadas básicamente en el PSC.⁵²⁰ No obstante, la LFE al establecer los límites de responsabilidad del PSC (art.23), aparte de proporcionar una enumeración indirecta de las obligaciones de los Firmantes/Suscriptores y los Usuarios del certificado, determina

⁵¹⁷ Como hace notar J.F. Ortega “esta inclusión no atenta contra la Directiva sino que la complementa” (J.F. Ortega, 2004: 421). No nos olvidemos que la norma comunitaria prevé esta posibilidad al establecer en el art. 6 DFE que la legislación efectuada constituye una regulación de “mínimos”.

⁵¹⁸ Como por ejemplo la Ley de Utah sobre firma digital (Utah Digital Signature Act, 1995) o la Ley Modelo de CNUDMI sobre firma electrónica.

⁵¹⁹ En ese sentido, la LFE adopta un sistema basado en normar la responsabilidad, a partir del cual pueden inferirse una serie de facultades y, sobre todo, de obligaciones que atingen a las partes intervinientes en el sistema de certificación.

⁵²⁰ Al respecto Rodríguez expone: “Lo primero que llama la atención al acercarse a la regulación española, sobre todo si se relaciona con la legislación comparada, es que falta la previsión de la responsabilidad del signatario electrónico, a quien no se le exige expresamente por Ley ningún grado determinado de diligencia en el uso de los elementos sofisticados de que dispone para la contratación mediante firma electrónica, máxime teniendo en cuenta que el empleo de los equipos en cuestión se puede realizar por sus empleados o agentes; esa falta de regulación legal...unida la relación contractual que liga al titular de la firma electrónica con el prestador de servicios de certificación hacen que deba acudirse al contrato que les vincula, en el que sí se contemplará, por lo común, de forma expresa esa responsabilidad. Además, es de hacer notar que ni tan siquiera se regulan las consecuencias que se pueden derivar de la pérdida de la clave privada, qué actuación ha de seguirse en ese caso, y la posible responsabilidad del suscriptor frente al tercero por tal causa (a diferencia de lo que ocurre, por ejemplo, en la legislación del Estado de Utah, tampoco se contempla la responsabilidad civil y penal de quien usa las claves sin autorización), que habrá de ser, ante esta laguna legal, objetiva e ilimitada, cuando doctrinalmente se defiende que debiera haberse limitado la misma, como ocurre respecto de las tarjetas de crédito.” (M. Huerta y D. Rodríguez, 2001: 127-128) // En este sentido se pronuncia también Martínez, para quien la regulación de la responsabilidad en la LFE “...es incompleta e insuficiente y no se tienen en cuenta los intereses en juego de los distintos sujetos implicados.” (A. Martínez, 2004:337) // “Falta, pues, en nuestro ordenamiento una protección de los terceros de buena fe, o parte que confía –también falta la previsión de obligaciones a cargo de esta parte-...” (M. Huerta y D. Rodríguez, 2001: 116).

tangencialmente el régimen de responsabilidad de estos últimos teniendo en cuenta los deberes de diligencia que les incumben.⁵²¹

Volviendo nuestra atención sobre la responsabilidad del PSC, la LFE aborda la temática en el Capítulo II “*Responsabilidad*”, del Título III “*Prestación de servicios de certificación*”, el cual se encuentra conformado por dos artículos, aunque como veremos, se debe acudir a la integración con otros preceptos de la LFE para componer el régimen de responsabilidad del PSC.

- El art. 22 “*Responsabilidad de los prestadores de servicios de certificación*”, determina las nociones fundamentales del régimen de responsabilidad del PSC, subdividiéndose en dos supuestos, a saber: i) supuesto general de responsabilidad (junto a sus características); ii) supuestos específicos de responsabilidad.
- El art. 23 “*Limitaciones de responsabilidad de los prestadores de servicios de certificación*”, en el que se establecen una serie de supuestos que limitan la responsabilidad del PSC, los cuales pueden ser divididos básicamente en dos categorías, a saber: i) limitaciones intrínsecas al certificado; ii) limitaciones extrínsecas al certificado.⁵²²

Conforme se tiene adelantado, aparte de la regulación del Capítulo II aludido previamente,⁵²³ coexisten otras disposiciones dispersas en la LFE que deben integrarse para modular de manera integral el régimen de responsabilidades del PSC, mismas que fueron objeto de análisis a lo largo del Capítulo Cuarto de esta investigación.

⁵²¹ Respecto de ello, el apartado II de la Exposición de Motivos de la LFE indica: “Adicionalmente, la Ley establece un marco de obligaciones aplicables a los prestadores de servicios de certificación, en función de si éstos emiten certificados reconocidos o no, y determina su régimen de responsabilidad teniendo en cuenta los deberes de diligencia que incumben a los firmantes y a los terceros destinatarios de documentos firmados electrónicamente.”

⁵²² En esta parte seguimos la clasificación propuesta por Apol-Lònia Martínez (A. Martínez, 2004: 382 y ss.).

⁵²³ Conforme sostiene Martínez, el Capítulo II del Título III de la LFE “*puede considerarse el núcleo del régimen de responsabilidad*” del PSC en la legislación española sobre firma electrónica (A. Martínez, 2004: 336).

Podemos citar por ejemplo: el art. 13.5. LFE que norma la participación de Entidades de Registro; los arts. 8, 9 y 10 LFE que se ocupan de la extinción y suspensión de certificados, los cuales revisten notorios efectos en la temática de responsabilidad; el art. 20.2 LFE que dispone la constitución por parte del PSC que emite certificados reconocidos de una garantía económica para hacer frente a probables responsabilidades; y, los arts. 31 a 36 LFE que norman los casos de responsabilidad administrativa en que incurre el PSC, enumerando las conductas contraventoras junto a las sanciones aplicables en cada caso.

Cabe igualmente resaltar que a efectos de la responsabilidad del PSC, resulta auxiliar y complementaria la disposición del art. 13.1. de la LSSI, en la que se establece que los prestadores de servicios de la sociedad de la información “*están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley.*”

En los próximos apartados nos dedicaremos precisamente al estudio del núcleo del régimen legal de responsabilidad, constituido por los arts. 22 y 23 LFE.⁵²⁴ De modo tal, que establecido y delimitado el preciso marco normativo en el que nos desenvolveremos para abordar el presente acápite, cabe efectuarse los siguientes cuestionamientos:

- i) Cuáles son los supuestos de responsabilidad civil del PSC que emite certificados reconocidos ?
- ii) En el caso de generación de daños por parte del antedicho PSC:
 - qué tipo de responsabilidad le es imputable (objetiva o subjetiva)?
 - cuál es el origen de dicha responsabilidad (contractual o extra-contractual)?
 - frente a qué sujetos es responsable?
 - cuáles son los límites y casos de exoneración de responsabilidad?

⁵²⁴ En ese sentido la DFE señala en su parte considerativa que los PSC que presten sus servicios al público “...*están sujetos a la normativa nacional en materia de responsabilidad.*”

Planteadas así las interrogantes, procuraremos dar respuesta a las mismas a continuación.

3.1. Supuestos de responsabilidad.-

Para abordar la materia señalaremos inicialmente que el art. 22 LFE prevé dos supuestos de responsabilidad de los PSC: los de carácter general y aquellos que son específicos.

a) Supuesto general de responsabilidad.-

Nos ocuparemos inicialmente del supuesto general: responsabilidad de los PSC por los hechos que ocasionen daños y perjuicios a las personas en el ejercicio de su actividad, cuando incumplan las obligaciones señaladas en la ley (art. 22.1. LFE).⁵²⁵

Esto quiere decir que el régimen de responsabilidad previsto en la legislación española, generaliza su ámbito de aplicación a *todo tipo de PSC*:

- independientemente de si emiten certificados reconocidos o no;
- ya sea que actúen en grupos cerrados (con acuerdos previos para el empleo de firmas electrónicas), o que expidan sus certificados al público en general (sin dichos acuerdos previos);
- indistintamente de si emiten certificados electrónicos o se limitan a prestar otros servicios relacionados con la firma electrónica;⁵²⁶
- por *toda categoría de hechos* que ocasionen daños y perjuicios;
- frente a *toda clase de personas*: naturales o jurídicas, de derecho público o privado;
- conforme a las normas generales sobre la culpa contractual o extracontractual;
- cuando no observan las obligaciones fijadas en la LFE.

⁵²⁵ La DFE se limita a regular la responsabilidad de los PSC que expidan al público certificados reconocidos, no siendo aplicables sus preceptos cuando éstos actúan dentro de comunidades cerradas en las que existen acuerdos privados o cuando expidiendo certificados al público, los mismos no tienen carácter de reconocidos, por lo cual y en los dos últimos casos planteados, la responsabilidad del PSC se rige por el régimen general.

⁵²⁶ Nótese sobre el particular, que de acuerdo con la definición del art. 1.2 LFE puede darse el caso que el PSC no expida certificados, sino que se dedique a prestar otros servicios respecto de la firma electrónica, o finalmente que efectúe ambas funciones de modo simultáneo, de manera que para algunos de sus clientes expida efectivamente certificados y para otros, simplemente les preste otros servicios relacionados con la firma electrónica, como por ejemplo el sellado temporal. En todo caso, en cualquiera de los supuestos planteados, el PSC se encuentra sujeto al régimen de responsabilidad previsto por el art. 22 de la LFE.

b) Supuestos específicos de responsabilidad.-

Al margen del supuesto general de responsabilidad aludido precedentemente, los numerales 2º al 5º del art. 22 LFE, contienen una serie de previsiones respecto de supuestos específicos o *hechos concretos* de responsabilidad,⁵²⁷ los cuales de momento nos limitaremos a enunciar, puesto que su estudio a profundidad lo reservaremos para más adelante, donde procuraremos sistematizar las distintas hipótesis de responsabilidad civil derivadas de los servicios de certificación reconocida.

Los mencionados supuestos específicos de responsabilidad consisten en:

- a) responsabilidad por homologación o garantía de certificados de terceros (art. 22.2. LFE);
- b) responsabilidad en caso de suspensión o extinción de certificados (art. 22.3 LFE);
- c) responsabilidad por las actuaciones de los auxiliares del PSC (art. 22.4. LFE).

Obsérvese que en cualquiera de los dos supuestos analizados, para que se activen los mecanismos de responsabilidad es necesario lógicamente: que la conducta por acción u omisión del PSC efectivamente haya originado un perjuicio y, que el daño le sea imputable.

3.2. Naturaleza de la responsabilidad: objetiva o subjetiva y carga de la prueba.-

Con relación a la naturaleza de la responsabilidad del PSC, la doctrina de forma uniforme viene sosteniendo precisamente que uno de los aspectos más polémicos a momento de delimitar la misma, estriba en discernir su carácter objetivo o subjetivo.⁵²⁸

Como es ampliamente conocido, si un ordenamiento jurídico abriga la solución por la objetividad, el PSC responde por los daños y perjuicios causados en el ejercicio de su

⁵²⁷ La solución adoptada en la norma comunitaria, decanta por una formula casuista en el art. 6.1. DFE, donde establece una lista de supuestos concretos de responsabilidad del PSC, a saber: i) cuando no garantice la veracidad de la información contenida en el certificado reconocido a momento de su expedición (art. 6.1.a); ii) cuando no garantice que al momento de expedir el certificado reconocido obran en poder del firmante los datos de creación de firma (art.6.1.b.); y, iii) cuando no garantice que los datos de creación y verificación de firma pueden emplearse de modo complementario (art. 6.1.c.). Y en el art. 6.2. DFE se añade un supuesto concreto más de responsabilidad del PSC, referente a la ausencia de registro de la revocación del certificado reconocido. / De manera similar se formula la LMFE, al establecer en su art. 9.2. que “*Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1.*”; dicho párrafo enumera en seis incisos - inc. a) al f) - el conjunto de obligaciones que debe observar el PSC, cuyo incumplimiento determinan su responsabilidad, configurándose por consiguiente y al igual que el caso anterior, un catálogo de supuestos específicos de responsabilidad del PSC.

⁵²⁸ Sobre el carácter objetivo o subjetivo de la responsabilidad del PSC: (A. Martínez, 2004: 336 y ss.) // (J.F. Ortega, 2004: 421 y ss.) // (M. Pérez, 2009: 222 y ss.)

actividad en todos los casos e independientemente del nivel de diligencia empleado, en otras palabras, tanto cuando fue diligente así como cuando actuó de manera manifiestamente negligente.

Por contramano, cuando el ordenamiento legal acude a un sistema basado en la subjetividad, el PSC únicamente responde por los daños y perjuicios ocasionados cuando los mismos provengan de una conducta culposa o negligente.

En este ámbito la DFE decanta claramente por la responsabilidad subjetiva, cuando en su art. 6.2. determina que los PSC que emiten certificados reconocidos responden de la exactitud de la información contenida en el certificado reconocido “...*salvo que el proveedor de servicios de certificación demuestre que no ha actuado con negligencia.*”

De esa manera resulta evidente que la norma comunitaria consagra un sistema de responsabilidad por culpa con inversión de la carga de la prueba, lo que significa que el PSC ante la producción de un daño, debe demostrar en todo caso que *no actuó de modo negligente*; solución que como veremos resulta un tanto complicada de poner en práctica, ya que al PSC le será mucho más difícil demostrar que “*no obro negligentemente*”, frente aquella otra por la cual simplemente debe demostrar “*que procedió diligentemente*”.

Aunque parezca simplemente un juego de palabras, su aplicación en la práctica posee una radical diferencia, revistiendo la primera solución como se tiene expuesto, un nivel más complejo de efectivizar, pues no es lo mismo probar *aquello que no se hizo* (un no hecho), que probar *lo que efectivamente se hizo* (un hecho).

A lo reflexionado cabe añadir, que el Capítulo Quinto de los Principios de Derecho Europeo de la Responsabilidad civil (*Principles on European Tort Law*),⁵²⁹ determina las ocasiones en los que se aplicará la responsabilidad objetiva, delimitando un régimen absolutamente restrictivo para su aplicación y dirigido fundamentalmente a los daños

⁵²⁹ Los Principios on European Tort Law, fueron elaborados por el European Group on Tort Law. Disponibles en <http://www.egtl.org>.

causados por actividades “*anormalmente peligrosas*” (art. 5:102), situación que a nuestro juicio no se presenta en los servicios de certificación de firma electrónica.

Por su parte, la legislación española en actual vigencia sigue el modelo adoptado por la DFE, coronando explícitamente el modelo de responsabilidad subjetiva por culpa, el cual resulta de aplicación a todo tipo de PSC (emita certificados reconocidos o no) y en todos los casos en los que por prestación de sus servicios de certificación se generen daños y perjuicios, como consecuencia del incumplimiento de las normas legales, superando de esta manera las dudas que generaba la redacción del art. 14.1. del RDL 14/1999, de 17 de septiembre, sobre firma electrónica.

La norma derogada parecía contemplar de modo simultaneo los sistemas objetivo y subjetivo de responsabilidad, a momento que dicho precepto señalaba que la responsabilidad de los PSC devendría “...*cuando incumplan las obligaciones que les impone este Real Decreto-ley “o” actúen con negligencia. En todo caso, corresponderá al prestador de servicios demostrar que actuó con la debida diligencia.*” (las comillas y negrillas de la vocal “o” en medio del texto son nuestras).

Nótese que de la interpretación del referido artículo, debido al carácter disyuntivo de la vocal “o”, resultaban siendo dos los supuestos de responsabilidad para el PSC: i) el incumplimiento de obligaciones señaladas en la ley, lo que permite inferir una responsabilidad objetiva, toda vez que era el simple hecho del incumplimiento de una obligación del RDL lo que determinaba el surgimiento de la responsabilidad del certificador, sin que medie una valoración subjetiva de su conducta; ii) actuación negligente, el cual sin lugar a dudas determina una responsabilidad subjetiva, basada en la conducta culposa del PSC, consagrando la inversión de la carga de la prueba.

Debido a ello el legislador español a momento de sancionar la LFE en vigencia, aprovechó de clarificar esta situación en el art. 22.1. (equivalente al art. 14.1. del RDL), a fin

que no quedaran dudas sobre la naturaleza de la responsabilidad del PSC, que es, valga la reiteración, eminentemente subjetiva.

La LFE asimismo, considerando lo conflictivo que podría resultar para el Firmante/Suscriptor el hecho de tener que demostrar la negligencia del PSC - sobre todo en los casos que reviste la condición de consumidor - determina al igual que la norma comunitaria una inversión de la carga de la prueba en el art. 22.1 (párrafo segundo, inciso final), cuando dispone que “...corresponderá al prestador de servicios de certificación de mostrar que actuó con la diligencia profesional que le es exigible.”⁵³⁰

Del mismo modo, el aludido inciso establece una inversión de la carga de la prueba basado (aunque no lo exprese así el legislador) en la presunción simplemente legal de la culpa del PSC. Esta figura surge como reacción a los problemas que se suscitan en la responsabilidad extracontractual al probar la culpa,⁵³¹ sobre todo, en hipótesis de responsabilidad que son tan complejas como las que venimos refiriendo.

En efecto, sería - si no prácticamente imposible - extremadamente difícil para el Usuario que confía en el certificado u otros terceros, probar la negligencia del PSC debido a los complejos mecanismos técnicos a través del cual opera el sistema de certificación, a lo que se suma, los vertiginosos cambios que se presentan en el progreso tecnológico.

Sintetizando ideas y a modo de conclusión, indicaremos que en los supuestos de responsabilidad por *culpa*, el PSC se encuentra llamado a responsabilizarse frente a los afectados por su conducta, pudiendo en todo caso liberarse si demuestra que empleo debidamente su diligencia *profesional*, es decir, que recae sobre éste la carga de la prueba.

⁵³⁰ En ese entendido, Martínez explica que de acuerdo con las disposiciones de la LFE “...ante una eventual demanda por responsabilidad no es el demandante el que ha de probar la negligencia de la entidad certificadora sino que es la propia entidad la que, si quiere exonerarse de responsabilidad, ha de probar que actuó con diligencia.” (A. Martínez, 2004: 349). Por su parte, Rodríguez ayuda a clarificar la temática, señalando que la responsabilidad, tanto en el sistema español como en el comunitario es subjetiva, sólo por culpa o negligencia, no objetiva, con inversión de la carga de la prueba, de modo que ha de ser el PSC “...quien ha de probar que ha actuado con diligencia, sin que sea necesario que el prestador pruebe la concurrencia de vaso fortuito o fuerza mayor, y sin que tenga que ser el perjudicado el que haya de acreditar el comportamiento negligente del prestador, ya que se considera que para el usuario del certificado puede ser difícil acreditar la existencia de negligencia del proveedor, quien, demostrando su diligencia, no responderá por los posibles daños ocasionados.” (M. Huerta y D. Rodríguez, 2001: 130-131). En idéntico sentido (R. Illescas, 2001: 140-142).

⁵³¹ Cabe recordar que la culpa extra-contractual no se presume a diferencia de la contractual (M. Yzquierdo, 2001: 109).

No obstante y a pesar de lo dicho, autores como Pérez consideran que en determinados casos, la responsabilidad del PSC puede considerarse objetiva. Explica la referida autora que del contenido del art. 20.2. LFE, se infiere que podemos estar frente a un supuesto de responsabilidad objetiva. Dicho precepto establece la obligación para el PSC de constituir un seguro de responsabilidad civil para afrontar el riesgo de la responsabilidad, por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan.

Sostiene que la referida exigencia de la “*garantía*” es la que objetiviza la responsabilidad del PSC, afirmando más adelante que la inversión de la carga de la prueba establecida por el legislador no viene sino a reforzar la evolución de la culpa en el derecho privado, hacia la denominada teoría del riesgo, con lo que en aras de conseguir la confianza del consumidor, se ha establecido para el PSC un régimen de responsabilidad civil “*subjetiva-objetivada*”, siguiendo precisamente la doctrina del riesgo.⁵³²

Desde nuestro punto de vista y aun admitiendo que la postura de Pérez sea viable, no debemos olvidar que la tradición jurídica española decanta, a nivel general, por la existencia de culpa por parte de quien causa un daño a objeto de atribuir responsabilidad, de modo que se hace necesario aludir a la responsabilidad subjetiva, y de hecho en nuestro caso específico en estudio, conforme se explicó, esa es la previsión contenida tanto en la LFE como en la DFE.

3.3. Origen de la responsabilidad: contractual o extra-contractual.-

Una vez que se ha estudiado la atribución de la responsabilidad, determinando que la misma es eminentemente subjetiva, debemos establecer frente a qué sujetos es responsable el PSC y cuál es el carácter de dicha responsabilidad (contractual o extra-contractual). Hacer estas distinciones resulta fundamental dadas las notables diferencias entre los regímenes de responsabilidad civil que coexisten en el derecho español.

⁵³² (M. Pérez, 2009: 222-223)

De inicio, el art. 22.1 LFE establece que la responsabilidad del PSC será exigible de conformidad con las normas generales sobre la culpa *contractual o extra-contractual*, según proceda, es decir, dependiendo de si existe o no un vínculo jurídico previo con los sujetos implicados en las actividades de certificación, razón por la cual se hace necesario efectuar un análisis en detalle de los distintos supuestos.

3.3.1. Responsabilidad frente al Firmante/Suscriptor.-

Entre el PSC y el Firmante/Suscriptor existe un vínculo que se expresa en los derechos y obligaciones emanadas del contrato de certificación reconocida perfeccionado entre ambos, en consecuencia, debemos concluir que en este caso, la responsabilidad civil del PSC es de naturaleza eminentemente contractual y sujeta a lo dispuesto fundamentalmente en los arts. 1.255, 1.258, 1.091 y 1.101 C.c. Resultando aplicables además el art. 1.102 y ss. C.c..

Esta conclusión es clara en caso de que las hipótesis de responsabilidad se hallen cubiertas por las Prácticas y Políticas de Certificación del PSC, las cuales forman parte integrante de los términos establecidos en el contrato de certificación reconocida. De hecho, como se analizó anteriormente, es común de que las DPC y las PC contengan habitualmente “...de forma detallada el conjunto de derechos y obligaciones, que van surgiendo en las diversas fases del ciclo vital del certificado [desde su emisión, hasta la eliminación del certificado en el directorio de certificados válidamente emitidos], entre los diversos sujetos implicados”.⁵³³ Por lo que las hipótesis de responsabilidad del PSC son cubiertas y delimitadas en la DPC y las PC asociadas al certificado emitido, gestionando así los riesgos que emanan de la actividad que realizan.

⁵³³ (A. Martínez, 2000: 227). Sobre esta temática, Rodríguez afirma que “Con el tiempo, la práctica del comercio electrónico permitirá puntualizar con mayor detalle cuál es el nivel de diligencia del ordenado empresario prestador de servicios de certificación, pero hasta tanto ello ocurra se pueden utilizar como guía las denominadas declaraciones de prácticas de certificación, en las que se contienen los criterios, reglas y pautas por las que se van a regir en sus funciones de expedición de certificados y prestación de otros servicios relacionados con la firma electrónica.” (M. Huerta y D. Rodríguez, 2001: 132).

Sin embargo, es posible que la DPC no prevea total o parcialmente las obligaciones derivadas de la actividad de certificación. En este supuesto es necesario hacernos la siguiente pregunta: ¿es posible hablar de responsabilidad contractual en caso de que el PSC no cumpla una obligación que no se contempla en el contrato, pero que se halla establecido en la Ley?

Nos inclinamos por sostener que igualmente estamos en presencia de una responsabilidad contractual⁵³⁴ dado que, conforme a lo dispuesto con el art. 1.258 C.c. “*Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan, no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley*”.

Este precepto nos debe llevar a la conclusión de que, como bien señala Morales Guillén:

“...los efectos de los contratos, no sólo alcanzan a las cosas o hechos expresados en ellos como objeto determinado o determinable, sino también respecto de todo lo que por imperio de la ley, de los usos o de la equidad corresponda a la naturaleza del contrato. Ha de tenerse en cuenta a este propósito las reglas relativas al principio *accessorium sequitur principale*, por virtud del cual, los efectos de los contratos recaen también sobre los accesorios de la cosa principal objeto de un contrato...se establece la automática inserción de las cláusulas impuestas por la ley, como agregado a las estipuladas en el contrato por las partes en sustitución, inclusive, de las que resultaren eventualmente dispersas”.⁵³⁵

La naturaleza de la obligación de certificar *es dar confianza a las partes que participan en una transacción electrónica*, de lo cual se deriva que los PSC como terceros de confianza, para que sean efectivamente tales, deben emitir certificados cuyos contenidos sean veraces. Esto nos permite sostener que todas las hipótesis de responsabilidad que afecten la

⁵³⁴ En el mismo sentido se pronuncia Pérez al señalar “...un importante sector doctrinal, considera que los daños causados por el incumplimiento de las obligaciones legales, salvo que se pruebe otra cosa, han de configurarse en el ámbito de la responsabilidad civil contractual, siempre que exista relación jurídica contractual entre el dañado y el dañante.” (M. Pérez, 2009: 212). Criterio al nos adherimos.

⁵³⁵ (C. Morales, 1994: 741-742).

veracidad de los certificados emitidos, caen en el ámbito de la responsabilidad contractual en ocasión que el afectado sea el Firmante/Suscriptor, producto de un acto culposo o negligente del PSC.

En lo que respecta a las obligaciones en general que el PSC debe cumplir por mandato de la ley (entre ellas la emisión de certificados veraces) debemos concluir, siguiendo a Morales Guillén, que sus disposiciones “*suplen el silencio de los contratantes*”⁵³⁶ en caso de que éstas no se hallen reguladas en la DPC y las PC.

3.3.2. Responsabilidad frente al Usuario del certificado.-

Entre el PSC y el Usuario del certificado existe igualmente un vínculo que se expresa en los derechos y obligaciones emanados del *Contrato de verificación de certificados* perfeccionado entre ambos, de modo que la responsabilidad civil del PSC es de naturaleza eminentemente contractual.

En consecuencia, debemos concluir que en este supuesto se aplican, *mutatis mutandi*, los razonamientos previamente esgrimidos, argumentos a los que nos remitimos.

3.3.3. Responsabilidad y resolución contractual.-

En una aproximación general diremos que en cualquier relación obligatoria sinalagmática (contrato) resulta necesario referirse, por un lado, a los conceptos de incumplimiento y cumplimiento defectuoso; por el otro, considerando que el tiempo de cumplimiento en un gran número de contratos es de fundamental trascendencia, es igualmente importante determinar el límite entre un cumplimiento tardío o retraso de la obligación, y el incumplimiento propiamente.

El cumplimiento a cabalidad de cualquier obligación trae aparejada la ejecución de la misma dentro del término previsto, lo que en la doctrina y jurisprudencia se conoce como “*término esencial de la obligación*”⁵³⁷, pero no debemos olvidar que el mero retraso no es en

⁵³⁶ (C. Morales, 1994: 742).

⁵³⁷ (L. Díez-Picazo, vol II, 1996: 660).

algunos casos equivalente al incumplimiento, debido a que no siempre el retardo en el cumplimiento de una obligación se traduce en la frustración del fin práctico perseguido con el negocio.

Por ello, a objeto de que prospere la resolución del contrato en ocasión de un retraso, tanto la doctrina como la jurisprudencia consideran que dicho retraso únicamente justifica la resolución contractual.⁵³⁸

- i) cuando supone efectivamente la frustración del fin práctico buscado por el negocio, y/o
- ii) determina en el otro contratante un interés atendible en la resolución.

A mayor abundamiento, expresaremos entonces que cuando el retraso se refiera a un término esencial del contrato cabrá la resolución del mismo, conforme lo establecido en el art. 1.124 C.c.; pudiéndose optar por el cumplimiento o la resolución de la obligación, además de la indemnización por daños y perjuicios, si éstos efectivamente se ocasionaron. En caso que el retraso no se considere término esencial, la responsabilidad sería la ordinaria por retraso.

Se hace necesario distinguir, además, la responsabilidad por incumplimiento de elementos esenciales del contrato o de elementos accesorios del mismo. De modo que si el elemento esencial del contrato se ha incumplido, podrá optarse por el cumplimiento forzoso o la resolución del contrato, además de la correspondiente indemnización por los daños y perjuicios ocasionados. Cuando se trata de un elemento accesorio, puede optarse por el cumplimiento forzoso o la disminución proporcional en el precio del servicio.

Respecto de la eficacia de la resolución, diremos que en relaciones duraderas extingue el vínculo contractual con puros efectos *ex nunc* e impone entre las partes los consiguientes deberes de liquidación de la situación.⁵³⁹

⁵³⁸ (L. Díez-Picazo, vol II, 1996: 662).

⁵³⁹ (L. Díez-Picazo, vol. II, 1996: 724).

Con relación a los efectos que ocasiona la resolución contractual, la doctrina se refiere a la eficacia liberatoria y la eficacia restitutoria. En el primer caso, nos referimos al hecho que la resolución del contrato trae como consecuencia la desvinculación de las partes de la relación obligatoria, de modo que la parte que no hubiera ejecutado la prestación a la que se encontraba obligada, deja de tener el deber jurídico de realizarla.

En el segundo supuesto, hablamos en sentido de que cuando alguna de las prestaciones hubiera sido ejecutada, se debe constituir a cada una de las partes en el deber de reintegrar o de *restituir* a la otra tal prestación, de conformidad con la regla del art. 1.123 C.c.. La restitución debe ser en principio específica o *in natura*, es decir, respecto de los mismos bienes que hubieran sido objeto de la prestación, pero cuando ello no sea posible (v.gr. supuestos en los que la obligación ejecutada es una prestación de hacer, caso de los servicios), la restitución debe producirse a través del equivalente pecuniario.⁵⁴⁰

Finalmente, no debe confundirse la restitución con la deuda de resarcimiento. El art. 1.124 C.c. confiere por cuerda separada al contratante perjudicado por el incumplimiento, el derecho al resarcimiento por los daños y perjuicios, de manera que técnicamente se produce la transformación de la obligación primitiva en una obligación de indemnización, ésta última siempre es una obligación pecuniaria y debe ser considerada como deuda de valor y no como deuda de dinero, por cuanto su cuantía no ha de establecerse a la fecha en que se produzca el incumplimiento, sino al momento de la definitiva condena de reparación.⁵⁴¹

La doctrina es prácticamente uniforme en sostener que el resarcimiento debido debe ser situado en el marco del llamado interés positivo, que se refiere al derecho de ser colocado en la misma situación económica y patrimonial que se tendría si el contrato hubiera sido perfectamente ejecutado, de modo que debe centrarse en la diferencia entre el valor de la prestación adversa en el momento del contrato y el que tuviera en el momento de la

⁵⁴⁰ (L. Díez-Picazo, vol. II, 1996: 722-723).

⁵⁴¹ (L. Díez-Picazo, vol. II, 1996: 691).

resolución. Y conforme argumenta Díez-Picazo “*no cabe duda que el demandante de la resolución puede pedir ex. Art. 1.106 C.c. el lucro cesante*”.⁵⁴²

En nuestro caso en concreto, la responsabilidad civil del PSC frente al Firmante/Suscriptor y/o al Usuario del certificado, dado que existe un vínculo previo, no escapa a la aplicación de las normas generales sobre cumplimiento de contratos a las que hemos hecho referencia previamente.

Con todo y no obstante lo señalado, si hacemos un análisis más detallado, debemos caer en cuenta que en las obligaciones principales del PSC (e incluso en las accesorias), tanto a momento de emitir y poner a disposición del certificado, como en ocasión de mantener los servicios de directorio y el de verificación de certificados, el tiempo de cumplimiento constituye el factor trascendental para satisfacer el interés primario del acreedor, de manera que si éste no se cumple conforme el programa contractual, se frustra el fin práctico buscado por el negocio, con lo cual, prácticamente en todas las ocasiones estaremos ante un auténtico incumplimiento resolutorio.

A objeto de respaldar nuestras afirmaciones, pasaremos a efectuar un sintético análisis de entre diversas posibilidades.

- Retardo/mora.-

Supongamos que se solicita un certificado para determinada fecha debido a que el Firmante/Suscriptor ha previsto cerrar transacciones comerciales con un cliente, pero el PSC se demora. En este caso si bien es evidente que materialmente aún es posible la realización de la prestación, no obstante, el retraso determina la ausencia de sentido en el negocio jurídico, lo cual es lógico, ya que la obtención del certificado más allá de un momento específico no es de utilidad para el Firmante/Suscriptor, que muy probablemente se vea perjudicado por no haber podido concretar sus negocios.

⁵⁴² (L. Díez-Picazo, vol. II, 1996: 726-727).

Otro ejemplo donde el factor tiempo resulta relevante, lo encontramos en ocasión que la vigencia de un certificado se encuentra suspendida o extinguida. Supongamos que el PSC no hace constar dichas circunstancias en los servicios de directorio y verificación de certificados, conforme los plazos y procedimientos de seguridad establecidos; debemos arribar a la conclusión, en aplicación de los mismos razonamientos del caso anterior, que el resultado es la frustración del fin práctico buscado por el negocio: identificación segura y oportuna en el caso del Firmante/Suscriptor, verificación del certificado segura y oportuna en el caso del Usuario.

- Cumplimiento defectuoso.-

En este caso el PSC ha procedido a emitir el certificado observando diligentemente el plazo comprometido al efecto, pero ha consignado datos erróneos o bien ha omitido datos en el certificado. Al igual que en los ejemplos anteriores, si bien aún es posible que se emita un nuevo certificado debidamente llenado, no obstante, el defecto determina la ausencia de sentido en el negocio jurídico, lo cual es lógico, ya que la identificación correcta del Firmante/Suscriptor más allá de un momento específico no es de utilidad para el Firmante/Suscriptor.

- Incumplimiento parcial.-

Finalmente analicemos la probabilidad de que el PSC emita en término el certificado debidamente cumplimentado, pero no lo publique en el directorio como tampoco brinde el acceso al servicio de verificación de certificados, o una vez emitido debidamente lo coloque en el directorio pero el servicio de validación no se encuentre operativo. En estos casos nos encontramos ante un incumplimiento parcial, o visto de otro modo, un cumplimiento parcial de sus obligaciones.

Al igual que los casos anteriores consideramos que se frustra el fin práctico del negocio, porque tanto el Firmante/Suscriptor como el Usuario no van a ver satisfecho su

interés, en el primer caso de identificarse, en el segundo de efectuar la validación del certificado, ya que es muy probable que luego de una fecha determinada ello ya no tenga sentido.

En todos los ejemplos analizados previamente, constatamos finalmente que independientemente de la manera en que se lesione el derecho de crédito (retardo, cumplimiento defectuoso, incumplimiento parcial) en los hechos y en atención a las características peculiares que denota la certificación, el elemento gravitante para evaluar si existe o no incumplimiento radica en la consideración del *término esencial*, pues todos los demás factores lesivos al derecho de crédito se subordinan y supeditan a aquél.

Vistas así las cosas, la inobservancia del *término esencial* se traduce en un verdadero incumplimiento, debido a que si el PSC no cumple con sus obligaciones principales e incluso accesorias dentro del plazo esencial, no se traslada la utilidad al acreedor (llámese Firmante/Suscriptor, llámese Usuario), por lo que se frustra el fin práctico buscado por el negocio.

Es cierto que ante la presencia de hechos lesivos al derecho de crédito corresponde al acreedor:

- i) evaluar en definitiva cuándo éste se considera o no satisfecho con la prestación del deudor (v.gr. la ejecución de una obra que objetivamente se desvía en cuanto a las características acordadas - defectuosa - pero no obstante es dada por bien hecha y recibida por el acreedor);
- ii) decidir - en caso de insatisfacción - respecto de los mecanismos de defensa que empleará para ver satisfecho su derecho subjetivo de crédito, eligiendo de entre el conjunto de facultades o acciones que le otorga la ley para ello;

Pero desde nuestro punto de vista y analizada objetivamente la situación, en el caso concreto de estudio que nos ocupa, lo más sensato es considerar que en los hechos

prácticamente en la generalidad de todos los casos un incumplimiento de estas características acarrearía como consecuencia lógica la resolución del vínculo contractual y la consiguiente indemnización por los daños y perjuicios, por supuesto en caso que éstos efectivamente se hayan producido y sean imputables al PSC.

Cabe resaltar que los daños causados por el PSC en el desarrollo de su actividad certificadora tendrán, prácticamente en la generalidad de los casos, la categoría de daños patrimoniales,⁵⁴³ por lo que a estos efectos - como bien sabemos - la función de las normas de responsabilidad civil es de naturaleza eminentemente indemnizatoria.

Por otra parte, a diferencia de otras legislaciones la LFE no establece ninguna regulación relativa a los daños indemnizables. Por lo anterior consideramos que este asunto deberá ser resuelto conforme a las normas generales (art. 1.124 C.c.), las cuales permiten concluir que los daños indemnizables son los daños materiales, tanto el daño emergente como el lucro cesante, de conformidad con el art. 1.106 C.c. y las disposiciones específicas del art. 1.107 C.c.. Todo lo anterior, en la medida que dichos daños sean directos y ciertos.

3.3.4. Responsabilidad frente a terceros *strictu sensu*.-

Cuando el titular de la acción de perjuicios es un *tercero* (en sentido estricto) y completamente ajeno al sistema de certificación, sobre la naturaleza de la responsabilidad civil del PSC, basta decir que es claramente extra-contractual ya que no existe una relación jurídica previa de éste con dicho tercero.

Producto de lo anterior, el PSC está obligado a responder en la medida que produzca un daño imputable a su negligencia o culpa derivado de cualquiera de las hipótesis de responsabilidad de conformidad a lo dispuesto por el art. 22.1. LFE y en aplicación fundamentalmente de los arts. 1.089 y 1.902 del C.c. respectivamente.

⁵⁴³ Conforme hace notar Pérez “*En principio, la actividad que típicamente desarrolla el PSC es susceptible de causar daños a terceros, principalmente de carácter patrimonial, tanto a consecuencia de negligencia, error, omisiones propias o de los empleados, pérdida, robo, destrucción de documentos, etc. como consecuencia de defectos en los productos ofrecidos o servicios prestados...*” (M.Pérez, 2009:251).

3.4. Cláusulas limitativas de responsabilidad contractual.-

Al margen de los supuestos legales de limitación de responsabilidad de los PSC previstos en el art. 23 LFE, conforme al principio de la autonomía de la voluntad consagrado en el Código Civil español (principalmente en el art. 1.255), es posible que las partes establezcan modificaciones al régimen de responsabilidad contractual entre ellas, estableciendo cláusulas que agravan las responsabilidades, que establezcan cláusulas penales o que limiten la responsabilidad de las partes implicadas.⁵⁴⁴

En todo caso, debe quedar claro que en ningún caso es posible la limitación de responsabilidad cuando las estipulaciones sean contrarias a la ley, a la moral y al orden público (art.1.255 C.c.), y desde luego nunca cuando ésta procede del dolo, conforme la disposición del art. 1.102 C.c..

3.5. Exoneración de responsabilidad.-

Para concluir con esta parte, es necesario referirnos a los casos en que el PSC se ve exonerado de responsabilidad. En primer lugar debemos aludir al caso fortuito, ya que de conformidad con el art. 1.105 C.c. *“fuera de los casos expresamente mencionados en la ley, y de los en que así lo declare la obligación, nadie responderá de aquellos sucesos que no hubieran podido preverse, o que, previstos, fueran inevitables”*.

Conforme sostiene Diez-Picazo, es legítimo entender el precepto legal referido *“en el sentido de que, con independencia de que el acreedor pueda fundar su demanda de*

⁵⁴⁴ Sobre las formas que pueden revestir las cláusulas modificatorias de la responsabilidad civil contractual véase Christian Larroumet, *Responsabilidad Civil Contractual*, Santiago, Jurídica de Chile, 1998, pp. 22 y ss. // En lo que respecta a cláusulas limitativas de la responsabilidad del PSC cuando contrata con consumidores, debemos tener en consideración de que el PSC en su calidad de *profesional* (conforme a los términos establecidos en el art. 2.2. de la LCGC), no puede limitar su responsabilidad civil en términos absolutos, dado que el art. 8.2. de la LCGC establece que *“serán nulas las condiciones generales que sean abusivas, cuando el contrato se haya celebrado con un consumidor...”*. En ese sentido, el art. 83 del TRLGDCU prescribe que *“1.- Las cláusulas abusivas serán nulas de pleno derecho y se tendrán por no puestas. 2.- La parte del contrato afectada por la nulidad se integrará con arreglo a lo dispuesto por el artículo 1.258 del Código Civil y al principio de buena fe objetiva”*. Es decir, que las cláusulas abusivas no producirán efecto alguno en los contratos de adhesión (caso que se presenta en el contrato de certificación reconocida, dado que la DPC y las PC están establecidas por el PSC). Así también, el art. 82 TRLGDCU, señala que *“1. Se considerarán cláusulas abusivas todas aquellas estipulaciones no negociadas individualmente y todas aquellas prácticas no consentidas expresamente que, en contra de las exigencias de la buena fe causen, en perjuicio del consumidor y usuario, un desequilibrio importante de los derechos y obligaciones de las partes que se deriven del contrato”*. De la revisión del art. 86 TRLGDCU, se constata que el numeral 2 establece como cláusula abusiva *“La exclusión o limitación de la responsabilidad del empresario en el cumplimiento del contrato, por los daños o por la muerte o por las lesiones causadas al consumidor y usuario por una acción u omisión de aquél”*. Teniendo presente lo anterior, se puede decir que el PSC podrá limitar su responsabilidad civil frente al Firmante/Suscriptor y/o el usuario del certificado, cuando éstos revistan la condición de consumidor, en la medida de que no importen una cláusula abusiva como la recién expuesta.

responsabilidad en el dolo (art. 1.102) o en la negligencia (arts. 1.103 y 1.104), la responsabilidad del deudor subsiste mientras no se produzca una causa de exoneración, que es la mencionada en el art. 1.105”.

En este contexto, el caso fortuito contemplado en la ley exonera de responsabilidad al deudor (el PSC), toda vez que rompe la relación de causalidad entre las acciones u omisiones del deudor y los daños experimentados por el acreedor. Interviene un hecho impeditivo que no se halla bajo control del PSC. Ello no priva al PSC de su deber de diligencia profesional sino por el contrario, únicamente un deudor diligente podrá exonerarse de responsabilidad, porque si el hecho ha podido ser previsto con la diligencia exigible o evitado con una actividad diligente, no habrá propiamente caso fortuito o fuerza mayor.

No obstante, por disposición del propio art. 1.105 C.c. esta exoneración no tiene carácter absoluto, pues viene delimitada por dos excepciones: a los casos expresamente mencionados en la ley (que estudiaremos precisamente más adelante); y, en ocasión que exista un expreso pacto por virtud del cual el deudor deba responder de los casos fortuitos o de alguno de ellos, lo que constituiría una cláusula de agravación de la responsabilidad del deudor.

En segundo lugar, la imputación al PSC de la lesión al derecho del acreedor tiene que cesar cuando es un acto o una omisión del propio acreedor o de un tercero. En estos casos, debemos razonar que no existe en rigor un caso fortuito, sino una ruptura de la relación de causalidad entre la conducta del PSC y la lesión del derecho de crédito.⁵⁴⁵

IV. Hipótesis de responsabilidad civil derivadas de los servicios de certificación reconocida.-

En el presente apartado, dilucidaremos las hipótesis de responsabilidad derivadas exclusivamente de las obligaciones y servicios de certificación reconocida que prestan los PSC, conforme se encuentran previstos en la legislación española sobre la materia (LFE).

⁵⁴⁵ (L. Díez-Picazo, vol. II, 1996: 596-597).

Ello sin perjuicio no obstante, de que efectuemos las referencias necesarias a la normativa comunitaria (DFE), así como a las disposiciones contenidas en la LMFE u otras legislaciones cuando se juzgue conveniente.

Las hipótesis de responsabilidad civil del PSC y que emergen precisamente de los servicios de certificación reconocida que presta, se pueden clasificar para su mejor estudio y discernimiento principalmente en cuatro grandes grupos:

- i) aquellas que son previas o consustanciales a la emisión del certificado;
- ii) las derivadas de la certificación propiamente tal;
- iii) las que sobrevienen del servicio de homologación;
- iv) por las actuaciones de los auxiliares del PSC.

Dependiendo el caso en concreto, tres sujetos se encuentran llamados a demandar la responsabilidad del PSC: el Firmante/Suscriptor y titular del certificado reconocido, el Usuario verificador que confía en el certificado y, en determinadas ocasiones, inclusive un tercero ajeno al entorno de la certificación. Nótese por consiguiente que pueden prestarse distintas circunstancias de responsabilidad civil.

En adelante iremos dilucidando las hipótesis que afectan a cada sujeto y, en cada caso, describiremos la naturaleza de las relaciones jurídicas que pueden presentarse así como los daños por los que podría responder el PSC.

4.1. Hipótesis de responsabilidad previas o consustanciales a la emisión del certificado.-

En este primer caso de responsabilidad abordaremos los dos supuestos típicos referentes a: i) la generación del juego de claves (datos de creación y verificación de firma) cuando este servicio - que es distinto del servicio de certificación propiamente - es efectuado por el propio PSC y, ii) el incumplimiento de la obligación de emitir el certificado.

4.1.1. Responsabilidad por generación del juego de claves.-

La generación del par de claves (pública y privada) que configuran la firma digital, es el paso previo a la emisión del certificado y constituye en consecuencia una obligación precontractual del PSC. La veracidad del certificado depende, en gran medida, de los mecanismos técnicos de seguridad con los que la firma fue generada a fin de que ésta no sea obtenida por terceros a través de “ataques” computacionales.

En efecto, si la clave privada se hace accesible a terceros por esta vía, el Firmante/Suscriptor pierde el control exclusivo sobre la firma, cuestión que puede provocar daños tanto para éste como al Usuario que confía en el certificado y eventualmente otros terceros, producto de los fraudes que el atacante puede efectuar al suplantar al Firmante/Suscriptor.

Por lo mismo, en caso de que el PSC asuma el servicio de generar el juego de claves y en el proceso forje una firma tecnológicamente vulnerable - a consecuencia de su negligencia o culpa - el PSC será civilmente responsable por los daños que puedan causarse, toda vez que constituye una de sus obligaciones garantizar la complementariedad del par de claves así como su seguridad (art. 12.d. LFE).

Lo mismo puede decirse en caso que el PSC proceda a almacenar o copiar la clave privada, contraviniendo la prohibición expresa que existe en ese sentido (art. 18.a. LFE). Esto debido a que la clave puede ser tomada por un tercero, lo cual, puede dar pie a fraudes por parte de dicho tercero. De esta manera, al almacenar o copiar los datos de creación de firma el PSC incumple con sus obligaciones, por lo que cualquier perjuicio que se ocasione producto de esta circunstancia es imputable al PSC.

Nótese por consiguiente que en estos supuestos surge para el PSC una responsabilidad pre-contractual, de la que pueden devenir las siguientes consecuencias: i) calificado por el juez que el incumplimiento pre-contractual del deber de garantizar la complementariedad del

par de claves así como su seguridad por parte del PSC, constituye un supuesto de anulabilidad del contrato por dolo causal, ello conduce en el ordenamiento español a los arts. 1.300 y siguientes del C.c.; ii) Si la conducta del PSC ha causado un daño, con independencia de que finalmente se anule o no el contrato, se podrá solicitar la indemnización de daños y perjuicios (art. 1.101 C.c.). Respecto del sujeto frente al que responde el PSC, resulta claro que en principio es el Firmante/Suscriptor.

4.1.2. Responsabilidad por ausencia de emisión del certificado.-

La emisión y puesta a disposición del certificado en favor del Firmante/Suscriptor es la prestación más elemental a la cual se obliga el PSC al celebrar el “*contrato de certificación reconocida*”. Como se tiene analizado, luego de que el PSC o la ER delegada proceden a la confirmación de la identidad y demás datos relevantes proporcionados por el solicitante, el PSC debe generar y remitir el certificado al Firmante/Suscriptor.⁵⁴⁶

En caso que ello no sucediera, es fácil advertir que esta hipótesis de responsabilidad constituye el incumplimiento total de la obligación de emitir el certificado, producto de lo cual, pueden originarse perjuicios al firmante.

Por lo mismo, con relación al sujeto frente al que responde el PSC, de manera semejante con el supuesto anterior, resulta evidente que es el Firmante/Suscriptor.

4.2. Hipótesis de responsabilidad derivadas de la certificación.-

En este segundo grupo nos abocaremos básicamente a cuatro supuestos típicos, referentes a la responsabilidad: i) por inexactitud de los datos del certificado emitido; ii) por vulnerabilidad del directorio de certificados; iii) derivada de los servicios de extinción (revocación) y/o suspensión de certificados; y iv) responsabilidad en caso de extinción (revocación) y/o suspensión de certificados por causas atribuibles al PSC.

⁵⁴⁶ Recordemos que el solicitante pasa a ser Firmante/Suscriptor a momento de perfeccionarse el contrato. Tratándose de certificados emitidos a nombre de personas jurídicas, el Firmante/Suscriptor es la entidad a cuyo nombre se emite el certificado, en tanto que se mantiene la denominación de solicitante para referirse la persona física que actúa en representación de la persona jurídica, sobre quien recae finalmente la responsabilidad de custodia material de la clave privada (los datos de creación de firma).

4.2.1. Responsabilidad por la inexactitud de los datos del certificado.-

En esta circunstancia, el certificado emitido contiene datos erróneos y/o falsos en cuanto a la identidad y/o atributos del Firmante/Suscriptor, lo cual, en la medida que se configure un daño efectivo contra una persona y provenga de una actuación culposa o negligente del PSC, determinaría su responsabilidad.

Sin embargo, la responsabilidad del PSC derivada de este supuesto se configura desde el momento *en que efectivamente se distribuye el certificado*, debido a que es a partir de dicho instante que su contenido se hace accesible al público en general. Como hemos señalado, la legislación española opta por el sistema de directorios de certificados y servicios de consulta (art. 18.c. y d. LFE) como el medio de distribución de los certificados emitidos por un PSC.⁵⁴⁷ Esto revela la íntima relación entre el servicio de directorios y/o consultas respecto a la hipótesis en estudio.

Hecha esta prevención, referiremos que la responsabilidad por la inexactitud de los datos del certificado, puede tener origen en *circunstancias previas* a la emisión del certificado *o con posterioridad a la misma*. Respecto del momento que se trate, estamos en presencia de dos servicios distintos. En el primer caso estamos en presencia del *Servicio de registro*, mientras que en el segundo, se presenta el *Servicio de actualización o modificación de datos del certificado*. Trataremos por separado dichos momentos.

a) Por circunstancias previas a la emisión del certificado.-

En este supuesto de responsabilidad por la inexactitud de los datos contenidos en el certificado derivado de circunstancias *previas* a su emisión, estamos aludiendo al instante en que se solicita al PSC la emisión de un certificado, debiendo verificarse la información proporcionada a tal efecto, es decir, a momento de consignar los datos personales del solicitante del certificado.

⁵⁴⁷ Sin embargo, la eventual responsabilidad derivada del servicio de directorios y/o consultas no se agota únicamente con la emisión de certificados con datos erróneos. Por lo mismo, se ha decidido tratarlo de forma separada de la hipótesis de responsabilidad.

Hacemos mención por tanto al *Servicio de registro* (art. 12.a. LFE), que hemos descrito en su momento. Este servicio es una de las formas en que se puede configurar la hipótesis de responsabilidad que venimos estudiando, debido a que los datos recopilados en esta fase son los que se expresarán posteriormente al momento de emitir el certificado reconocido.

De este servicio se deriva de la obligación de *verificar los datos* identificativos o de atributos del solicitante, como asimismo deviene la posterior obligación del PSC en verificar que la información contenida en el certificado es exacta y se incluye toda la información necesaria que hace a un certificado reconocido (art. 12.b. LFE).

Dentro de esta obligación se incluye el deber de comprobar la identidad del solicitante, como también la comprobación de la veracidad de los datos suministrados por éste, acudiendo inclusive a la consulta de los registros públicos correspondientes cuando ello sea pertinente, caso de un empresario mercantil, lo que obliga al PSC a acudir al Registro Mercantil para verificar la información proporcionada por el solicitante, respecto de la adecuada inscripción en dicha entidad. En efecto, el solicitante se puede identificar con documentos públicos y/o privados adulterados con la intención de suplantar a otra persona.

No obstante, cabe advertir que en la responsabilidad del PSC por inexactitud de los datos contenidos en el certificado, debemos observar la clase de certificado que se compromete emitir conforme las condiciones establecidas en sus Políticas de Certificación.

En efecto, cuando el PSC va a emitir un “*certificado reconocido*” está obligado a *comprobar fehacientemente* la identidad del solicitante, de conformidad con el procedimiento previsto en el art. 13 LFE. Para ello debe requerir la comparecencia personal y directa del solicitante o de su representante legal si se tratare de una persona jurídica.

En caso de no cumplir con esta obligación, esto es, que el PSC: no compruebe fehacientemente la identidad del solicitante; compruebe negligentemente la identidad del

solicitante; no requiera la comparecencia personal del mismo o su representante en caso de ser una persona jurídica, estamos frente a una situación que puede generar daños por la falsedad de los datos contenidos en el certificado, en la medida que dichos hechos sean imputable al PSC.

De ese modo, si un PSC se compromete a comprobar la veracidad de los datos contenidos en el certificado, en particular, la identidad del solicitante y Firmante/Suscriptor de un certificado reconocido, el PSC compromete su responsabilidad si ha actuado culposa o negligentemente al verificar los datos del solicitante al momento de la petición del certificado.

Por el contrario, cuando se emite un simple certificado electrónico (o no reconocido), si el PSC acredita en su DPC que el certificado emitido da fe únicamente de la identidad que el titular aportó pero sin una verificación de dichos datos, o que la solicitud se hizo únicamente por vía *on line*, es razonable sostener que en dichos casos, el PSC no respondería civilmente acerca de la verificación de los datos y por ende de la veracidad de los datos contenidos en el certificado, debido a que no puede hacerse responsable al PSC a más de lo que éste se ha comprometido.

Por lo demás, el Usuario que confía en el certificado reconocido tiene la carga de revisar el contenido de éste (incluido los datos de generación del certificado donde se contienen los procedimientos de verificación de identidad) para que efectivamente pueda confiar en dicho documento electrónico. Por lo mismo, si confía en un certificado que no reúne dichas características de certeza, es el propio Usuario quien debe soportar el posible daño debido a su propia negligencia, producto de no haber revisado la declaración del PSC que consigna los medios de verificación de la identidad del Firmante/Suscriptor.

Respecto de los sujetos frente a quien es responsable el PSC en la hipótesis que venimos analizando, debemos descartar en principio al Firmante/Suscriptor, dado que,

verificados los datos del solicitante y aprobada la emisión del certificado, el PSC remite una copia del certificado al Firmante/Suscriptor para que: o bien ratifique su contenido, o bien haga notar los errores que existen a objeto que el PSC proceda a emitir un nuevo certificado debidamente cumplimentado. En caso de aceptación, la ratificación se pone de manifiesto de expresa o tácitamente, en este último caso cuando el Firmante/Suscriptor empieza a hacer uso del certificado.

Nótese en consecuencia, que con carácter previo a aceptar el contenido del certificado, el Firmante/Suscriptor tuvo la oportunidad de detectar las inexactitudes de los datos verificados por el PSC, lo que exime de responsabilidad al PSC respecto del Firmante/Suscriptor, en ocasión que éste último haya confirmado el contenido del certificado con datos erróneos, debido a que el Firmante/Suscriptor necesariamente actuó: ya sea dolosamente (v.gr. se percató del error pero deliberadamente no manifestó dicho hecho); ya sea de forma culposa o negligente (v.gr. no fue diligente en revisar el contenido del certificado remitido por el PSC). Se trata entonces de un supuesto de culpa por omisión de la diligencia debida, conforme a lo prescrito en el art. 1.104 C.c., atribuida por consiguiente únicamente al Firmante/Suscriptor.

Con relación al Usuario que confía en el certificado, cabe anotar que al fiarse de un certificado con datos erróneos, podría configurarse algún perjuicio derivado de la falsa identidad o atributos del Firmante/Suscriptor.

En efecto, por ejemplo el Usuario del certificado “*podría resultar engañado por confiar en un certificado falso como consecuencia de actuaciones del suscriptor (que, p. ej. suministra datos falsos a la autoridad de certificación, o está suplantando la personalidad de un tercero)*”.⁵⁴⁸ En este suceso resulta evidente que el PSC no es responsable frente al Usuario, salvo que hubiese actuado negligentemente, por lo que la atribución de responsabilidad recaería en el Firmante/Suscriptor, quien se encuentra en la obligación de dar

⁵⁴⁸ (A. Martínez, 2000: 74).

declaraciones exactas y completas respecto de los datos de su identidad personal, u otras circunstancias objeto de certificación, conforme se infiere del art. 23.1.a. LFE.

La apreciación de esta circunstancia podría ser relevante al momento de dilucidar la responsabilidad del PSC. Esto debido a que en los casos en que se haga uso de documentos fraguados, la calidad de la falsificación puede ser tal, que exceda la debida diligencia del PSC. Además, este acto doloso hace que el uso del certificado pase a ser un uso fraudulento por parte del Firmante/Suscriptor, cuestión por la cual no responde el PSC.

Por último, frente a estos servicios proporcionados por el PSC se pueden derivar perjuicios en contra de terceras personas (distintos del Usuario que confía en el certificado), por ejemplo, “*aquella a la que ha suplantado el suscriptor, que también resulte perjudicada por el certificado falso (por daños en su prestigio personal o profesional, gastos de abogados, etc.)*”. En dicho caso, “*esta persona puede actuar contra el suscriptor y, en su caso, contra la autoridad de certificación*”.⁵⁴⁹

b) Por circunstancias posteriores a la emisión del certificado.-

En este supuesto de responsabilidad por la inexactitud de los datos contenidos en el certificado derivado de circunstancias *posteriores* a su emisión, estamos aludiendo a las ocasiones en que se produce una variación de la información consignada inicialmente en el certificado. Nos encontramos por consiguiente, frente a las posibles responsabilidades derivadas del *Servicio de actualización o modificación de datos del certificado*.

Ahora estamos frente a un certificado que ha sido emitido y publicado válidamente, que surte todos sus efectos y que cumple con el requerimiento jurídico de la autenticación del Firmante/Suscriptor. Sin embargo, en esta circunstancia los datos identificativos o de atributos que se certifican han cambiado (por ejemplo, los poderes para representar a una persona jurídica han sido revocados respecto del apoderado que consta en el certificado).

⁵⁴⁹ (A. Martínez, 2000: 249).

Antes del aviso de actualización de datos, el perjuicio que se pudiera derivar de esta omisión es en principio imputable al Firmante/Suscriptor, ya que es él a quien la ley obliga dar inicio a la rectificación de los datos del certificado a través de la solicitud de modificación (art. 23.b. LFE).

Excepcionalmente, el PSC podría responder civilmente en caso de que éste haya tenido efectivo conocimiento de la enmienda de dichos datos por medios diversos a la solicitud de actualización del Firmante/Suscriptor, y a los cuales, se comprometiera a modificar automáticamente conforme su DPC.

Así por ejemplo, el PSC se puede comprometer a verificar periódicamente por su cuenta los poderes de representación de las sociedades mercantiles que constan en el Registro Mercantil, a fin de que dichos poderes guarden consonancia con los certificados de atributos que emiten respecto de los Firmantes/Suscriptores de un certificado de esta naturaleza, de conformidad a lo previsto en el art. 19 LFE, el cual señala que los PSC harán constar en su DPC “...*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.*”

Sin embargo, una vez que el PSC *ha recibido la solicitud de modificación* de los datos contenidos en el certificado, la situación es diametralmente distinta. Al igual que en el servicio de registro, el PSC (o la ER delegada) deberá comprobar la identidad del Firmante/Suscriptor que solicita el *servicio de actualización de certificados*, revisar la veracidad de los datos que presenta para identificarse, comprobar que dicho cambio en los datos identificativos o de atributos del Firmante/Suscriptor se han producido efectivamente, de lo cual responderá en los mismos términos que hemos señalado anteriormente.

Además de lo señalado, existe una *obligación adicional* en este caso, toda vez que se introduce la necesidad de que la modificación de los datos en ciertas circunstancias se haga de manera *perentoria*, aspecto este último que resulta relevante y permite diferenciarlo en términos sustantivos de la hipótesis de responsabilidad que emana de los servicios de registro (circunstancias *previas* a la emisión del certificado).

En efecto, si por ejemplo la ampliación de los poderes de representación de una persona no es consignada oportunamente después de efectuada la solicitud de modificación en un certificado de atributos, podrán derivarse perjuicios en contra del Firmante/Suscriptor que, producto del retardo negligente del PSC en la actualización, no pudo celebrar un contrato electrónico dada la negativa de la contraparte de celebrarlo, debido a que en el certificado no constaban los poderes de representación para efectuar tal operación, lo cual obligó al Firmante/Suscriptor a viajar al lugar físico donde se encontraba la contraparte para celebrar tal contrato físicamente (con los gastos que implica aquello: pasajes, alojamiento, alimentos, etc.).

Si bien es cierto que la LFE no regula puntualmente tal situación, debemos concluir que el PSC es responsable por el retardo culposo o negligente en la modificación de los datos en base a la interpretación extensiva del art. 18.d. LFE, el cual obliga al PSC a mantener un servicio de consulta sobre la vigencia de los certificados “*rápido y seguro*”.

Esto se justifica tanto frente a una responsabilidad contractual como extracontractual. En el primer caso la responsabilidad del PSC frente al Firmante/Suscriptor se funda en el art. 1.258 C.c., que al consagrar el principio de buena fe en la ejecución de los contratos, dispone que el contrato obliga en todo aquello que emane de la naturaleza de la obligación, donde podemos colegir que al momento de prestar el servicio de modificación de datos se debe ser razonablemente perentorio, deviniendo la responsabilidad contractual conforme el conjunto normativo que se tiene analizado a dicho efecto.

En el segundo caso, cuando el afectado sea un tercero (por ejemplo, la misma contraparte que prestó la negativa de celebrar electrónicamente el contrato y, debido a esta circunstancia, tuvo que trasladarse al lugar físico donde se encuentra el Firmante/Suscriptor), la responsabilidad extracontractual se fundará básicamente en los arts. 1.089 y 1.902 del C.c..

Determinar que existió un retardo en la prestación del servicio imputable a culpa o negligencia del PSC -y que de eso se perjudica a una persona- es una cuestión que depende de cada ocasión y conforme a lo que el juez decida. A ello podría aportar de manera relevante, la existencia en la DPC del certificador de un procedimiento regulado para llevar a cabo este servicio (en particular, la existencia de plazos en que el PSC debe proceder a modificar los datos), facilitando con ello la decisión del juez, quien tendrá una base objetiva con la que podrá formar su opinión para dilucidar si el PSC es responsable o no.

Respecto de los sujetos frente a los que se encuentra llamado a responder el PSC en caso que se ocasionen daños, pueden ser indistintamente los Firmantes/Suscriptores, los Usuarios que confían en el certificado, o incluso otros terceros, en términos análogos a las hipótesis de responsabilidad derivadas del servicio de registro detallado con anterioridad.

4.2.2. Responsabilidad por la vulnerabilidad del directorio de certificados.-

Al tratar la hipótesis de responsabilidad derivada de la inexactitud de los datos del certificado, consignamos el hecho que la responsabilidad del PSC derivada de este supuesto se configura desde el momento *en que efectivamente se distribuye el certificado*, debido a que es a partir de dicho instante que su contenido se hace accesible al público en general.

Con ello, resaltamos que en la hipótesis de responsabilidad citada mediaba necesariamente el servicio de directorio, pero que sin embargo, producto del servicio de directorio se podían configurar otras hipótesis de responsabilidad diversas a la emisión de

certificados con datos inexactos o erróneos.⁵⁵⁰ Sobre este supuesto precisamente ingresaremos a continuación.

La presente hipótesis de responsabilidad parte de la base que el PSC ha emitido y publicado certificados que *no* contienen datos erróneos, pero que producto de otros actos u omisiones culposas o negligentes del PSC, produce perjuicios a una persona en razón de las *condiciones de seguridad* en que debe ser mantenido el servicio de directorio para que sea un medio eficaz, fiable y seguro de distribución de certificados.

En efecto, la seguridad en el mantenimiento de información veraz de acceso público es de vital trascendencia en el sistema de distribución del certificado. Ello porque dicha publicación de directorios se hace normalmente por medios electrónicos - lo que los convierte en blancos de “ataques informáticos” de terceros - con lo cual se puede alterar su contenido, perdiendo la consonancia con los datos que efectivamente contenían los certificados al momento de su emisión o modificación.⁵⁵¹

Ahora bien, en caso que el PSC haya sido negligente en el mantenimiento y actualización de los mecanismos de seguridad destinados a repeler los ataques de terceros, o definitivamente haya culposamente permitido la intromisión de éstos, debemos concluir que el PSC es responsable civilmente por los daños que se devienen como consecuencia del cambio de dichos datos (sin perjuicio de que lo es también el tercero atacante).⁵⁵²

Como se advierte, esta hipótesis de responsabilidad se asemeja a las anteriores en la medida que afecta la veracidad de los certificados, pero que a diferencia de los supuestos precedentes, la falta de veracidad de dichos certificados es posterior al ingreso de los datos

⁵⁵⁰ Recuérdese que los certificados erróneos están relacionados con la gestión de los *servicios de registro de solicitantes* de un certificado y con el *servicio de modificación de datos*.

⁵⁵¹ Por ejemplo, el directorio de certificados es alterado por un tercero, quien modifica los datos de un Firmante/Suscriptor “X”, cambiándolo por la identidad de un Firmante/Suscriptor “Y”, lo que impide a X efectuar alguna transacción comercial; o que producto del mismo ataque se defrauda a un tercero que razonablemente confía en el certificado publicado, quien contrata con el Firmante/Suscriptor en atención de tratarse de “Y”.

⁵⁵² Esta responsabilidad civil es claramente delictiva, ya que no media relación contractual alguna con la persona afectada por dicho ataque.

identificativos del Firmante/Suscriptor y producto de la intromisión de atacantes en el servicio de directorio.

Con todo, la seguridad del sistema de certificados emitidos por el PSC, se halla respaldada con la firma electrónica avanzada del propio PSC que se adjunta al certificado (art. 1.2.d. LFE), lo cual dificulta que un atacante logre falsificar por completo el certificado (en particular la firma del PSC, la cual garantiza la integridad del certificado).⁵⁵³

De hecho, el éxito de este ataque se hace aún más improbable en caso de que la firma del PSC se halle a su vez certificada por otro PSC. A pesar de ello, no puede descartarse que el PSC emita certificados con una firma electrónica tecnológicamente insegura que posibilite también su falsificación. A esto se suma la posibilidad de que el PSC “*autocertifique*” su propia firma, con lo que se deja el paso libre para afectar la integridad de los certificados consignados en el directorio.

La LFE prevé esta situación para los PSC que emiten certificados reconocidos, estableciendo para ellos una serie de obligaciones destinadas a que el PSC cuente con altos niveles de seguridad en la publicación de los certificados.

Sobre el punto, destaca el art. 20.1.g. LFE que establece la obligación de “*Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad*”.

De esta manera, para que un PSC pueda emitir certificados reconocidos deberá demostrar, entre otras cosas, que posee los mecanismos técnicos para garantizar la debida seguridad del servicio de directorio frente a ataques de terceros.

⁵⁵³ Como bien sabemos, la firma del PSC permite corroborar al Usuario que confía en el certificado si los contenidos emitidos por el PSC en el certificado han sido, o no, alterados.

En definitiva, podemos concluir sobre la base de esta serie de obligaciones, que la seguridad del servicio de directorio se halla en mejor pié en el caso de los PSC que emiten certificados reconocidos, lo que no obsta, que aun así el PSC incurra en responsabilidad civil por este servicio.

En lo relativo a los sujetos frente a los que responde el PSC, podrán serlo tanto el Firmante/Suscriptor, el Usuario que confía en el certificado, como también un tercero diverso del anterior.

Respecto del Firmante/Suscriptor, podrá verse afectado dado que la integridad del certificado que utiliza para identificarse ha sido alterado, lo cual le impediría en ciertos casos celebrar alguna operación (por ejemplo, el Firmante/Suscriptor “A” producto de la alteración del certificado no puede identificarse frente a terceros dado que la identidad que figura en el certificado es de una persona “B”, lo cual le impide celebrar una transacción electrónica).

Por su parte, el Usuario que confía en el certificado puede sufrir también una serie de perjuicios al confiar razonablemente en el certificado (por ejemplo, el Usuario cree contratar con el Firmante/Suscriptor “A”, pero en realidad ha sido defraudado producto de que la identidad que se consignaba en el certificado era falsa).

Por último, un tercero diverso al Usuario que confía en un certificado podrá verse afectado en caso de que producto del ataque, éste figure como Firmante/Suscriptor de un determinado certificado que dañe su prestigio personal.⁵⁵⁴

4.2.3. Responsabilidad derivada de los servicios de extinción (revocación) y/o suspensión de los certificados.-

Como sabemos la pérdida de vigencia de un certificado puede ser definitiva o temporal. En el primer caso se habla de la extinción o invalidez del certificado, ya sea una invalidez por finalización del plazo de vigencia (art.8.1.a. LFE) o una invalidez anticipada

⁵⁵⁴ Por ejemplo, un sitio web que promueve la intolerancia religiosa acredita el dominio del sitio por medio de un certificado. Luego, acontece que un tercero atacante altera la integridad del certificado en el directorio del PSC, estableciendo que el sitio web es de propiedad del sujeto “X”. En tal caso la reputación de “X” se vería degradada, debido a que la comunidad asumiría que efectivamente “X” es promotor de intolerancia religiosa.

por causas no previstas (art. 8.1. incs. b) al h) LFE), lo que en criterio de Martínez nos conduce a la revocación del certificado.⁵⁵⁵ En el segundo caso hablamos de la suspensión del certificado (art. 9.1. LFE).

En cualquiera de estas posibilidades la causa fundamental y prototípica que determina la extinción (revocación) o suspensión de un certificado - dependiendo las circunstancias - gira básicamente en torno al riesgo que por cualquiera manera, la seguridad y confidencialidad de la clave privada se ha visto comprometida.⁵⁵⁶

De modo tal que el certificado deja de dar fe sobre los datos que contiene, toda vez que la relación exclusiva entre un par de claves con determinada persona deja ser de hecho efectiva.⁵⁵⁷ De aquí surge la necesidad del servicio de revocación o suspensión de certificados como un medio para hacer frente a estos riesgos, privando de validez al certificado, de manera definitiva en el primer caso, de modo temporal en el segundo.

El PSC en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión (a través del Firmante/Suscriptor o por cualquier otra fuente), se encuentra en la obligación de hacer constar inmediatamente y de forma precisa estas circunstancias en el servicio de consulta sobre la vigencia de los certificados (art. 10.1. LFE).⁵⁵⁸

En caso contrario y de conformidad con la previsión del art. 22.3. LFE, el PSC “...responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la

⁵⁵⁵ (A. Martínez, 2004: 142). Fernández nos explica, que luego de la revocación, se incluye la misma en la lista de revocaciones de certificados digitales LRC (en inglés CRL). Las LRC son descargables de la red y pueden ser muy extensas, ya que crecen con el número de usuarios. Requieren una actualización periódica, lo que no evita que exista un período intermedio entre la revocación y la inclusión en las LRC, período éste al que se lo denomina: “ventana gris”. Para solucionar el problema de las ventanas grises están apareciendo estándares técnicos a ese fin, pudiendo mencionar entre ellos el OCSP - *On Line Certificate Status Protocol* (H. Fernández, 2000: 259).

⁵⁵⁶ Lo aseverado por supuesto al margen de otras posibilidades, como la expiración del período de validez del certificado; fallecimiento o extinción de la personalidad jurídica del Firmante/Suscriptor; cese de la actividad del PSC u otros previstos en la DPC.

⁵⁵⁷ En ese entendido, cuando el PSC a solicitud del titular procede a revocar (art. 8.1.b. LFE) o suspender (art. 9.1.a. LFE) el certificado; la motivación de esta solicitud *puede* deberse a la pérdida del control exclusivo de la clave privada.

⁵⁵⁸ Además, por disposición del art. 10.2. LFE: “*El prestador de servicios de certificación informará al firmante acerca de esta circunstancia de manera previa o simultánea a la extinción o suspensión de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto. En los casos de suspensión, indicará, además, su duración máxima, extinguiéndose la vigencia del certificado si transcurrido dicho plazo no se hubiera levantado la suspensión.*”

*falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico”.*⁵⁵⁹

No obstante, debemos hacer notar que la extinción (revocación) o suspensión de un certificado consta de una serie concatenada de momentos, fases o etapas. Durante dicho procedimiento y dependiendo la fase de tramitación, pueden surgir situaciones de responsabilidad imputables no únicamente al PSC, sino también al Firmante/Suscriptor, por ejemplo cuando no da aviso oportuno de la pérdida de confidencialidad de la clave privada;⁵⁶⁰ e inclusive al Usuario del certificado, quién no obstante de tener la carga de verificar la vigencia confía en el certificado cuando ya se encontraba formalmente extinguido o suspendido.⁵⁶¹

Por lo expuesto, la consideración del elemento temporal en la hipótesis de responsabilidad que venimos tratando, resulta a todas luces relevante a fin de distribuir adecuadamente la responsabilidad entre los diversos sujetos implicados. En efecto, como se tiene adelantado no en todas las etapas el PSC es responsable civilmente.

Dichas etapas pueden estudiarse en cuatro fases, de la manera en que pasamos a exponer a continuación.⁵⁶²

i) Primera fase.-

En esta etapa “...*la seguridad de la clave se ha visto comprometida y es utilizada por un tercero, para suplantar al titular del certificado, que todavía no conoce la puesta en*

⁵⁵⁹ Disposición que se complementa además, con las reglas de conducta contenidas en los arts. 20.b. y 18 incs. c) y d) LFE. Nótese la estrecha relación de la presente hipótesis de responsabilidad con la que deviene de la generación del juego de claves y en el proceso forje una firma tecnológicamente vulnerable. Pueden incluso configurarse ambas hipótesis (subiendo el monto de los daños a indemnizar), pero en una secuencia cronológica distinta: la primera, al momento de crear la firma, y la segunda, al momento de llevar a cabo la revocación del certificado. La revocación en este caso, constituye una forma de aminorar los daños que ya se están produciendo producto de la creación de una firma digital defectuosa.

⁵⁶⁰ Mediante la interpretación extensiva del art. 23.1.c. LFE, se infiere que el Firmante/Suscriptor está obligado a custodiar adecuadamente su clave privada, asegurando en todo momento su confidencialidad y protegiéndola del acceso por parte de terceros no autorizados.

⁵⁶¹ El Usuario del certificado en base a la interpretación extensiva del art. 23.4.b. LFE, se encuentra obligado a comprobar la vigencia del certificado, debiendo tomar en cuenta antes de confiar en el mismo, si se encuentra suspendido o ha perdido definitivamente toda vigencia.

⁵⁶² Para el estudio y construcción de esta sección han resultado de mucha guía y orientación los trabajos de A. Martínez, los cuales seguiremos en gran medida por lo esclarecedor y orientadores que resultan en la materia. Al respecto consultar (A. Martínez, 2001:279-295); también recomendamos (A. Martínez, 2004: 364-381).

*peligro, o conociéndola, todavía no la ha notificado a la entidad de certificación solicitando la revocación del certificado... ”*⁵⁶³

En este primer momento, parece razonable sostener que el PSC no debe responder civilmente de los perjuicios que se produzcan al Usuario del certificado o al mismo Firmante/Suscriptor, dado que aún no se halla en condiciones de prestar el servicio de revocación o suspensión, toda vez que desconoce de la puesta en peligro de la clave.

Como bien señala Martínez Nadal, del PSC no se puede esperar en este momento actuación alguna, por cuanto aún no se le ha solicitado su intervención. Por consiguiente no existe responsabilidad del PSC así como tampoco del Usuario del certificado, de manera que la responsabilidad en este caso, será en principio, del Firmante/Suscriptor.⁵⁶⁴

ii) Segunda fase.-

En este periodo el PSC ha recibido la solicitud de revocación o suspensión, pero aún no ha adoptado la decisión de revocar, o habiéndola adoptado, aún no ha procedido a eliminar el certificado del registro de certificados válidamente emitidos.

En este momento “...*el titular solicita la revocación del correspondiente certificado pero un tercero la utiliza (la clave privada), suplantando al titular, durante el periodo entre la petición de revocación del titular, y la adopción de la decisión y la inclusión en la lista por la entidad de certificación de la revocación del certificado*”.⁵⁶⁵

Se debe tomar en cuenta que durante el intervalo de tiempo en que el PSC decide eliminar o suspender el certificado (cuya firma se encuentra comprometida) del registro de certificados válidamente emitidos, el tercero que suplanta al Firmante/Suscriptor puede realizar múltiples operaciones provocando graves perjuicios al propio Firmante/Suscriptor y/o a los Usuarios que confían en el certificado.

⁵⁶³ (A. Martínez, 2004: 364).

⁵⁶⁴ (A. Martínez, 2004: 364-367).

⁵⁶⁵ (A. Martínez, 2004: 370).

Incluso, por más diligente y rápido que sea el PSC en la operación de revocación o suspensión del certificado, existirá necesariamente un lapso temporal en que el tercero intruso pueda causar dichos perjuicios. Por ejemplo, si el servicio de revocación o suspensión se realiza en el lapso de una hora desde la solicitud correspondiente (lo que supone un servicio muy eficiente) el tercero cuenta con ese lapso para provocar fraudes y perjuicios con la suplantación del Firmante/Suscriptor.

En esta hipótesis, es admisible concluir que el PSC es civilmente responsable frente al Firmante/Suscriptor y el Usuario que confía en el certificado, por las actuaciones culposas o negligentes al momento de prestar el servicio de revocación o suspensión. Sin embargo, a fin de determinar las posibles responsabilidades que el PSC debiera soportar, es importante tener en cuenta dos factores:

- El primero tiene relación con la *verificación de la identidad* del solicitante de la revocación o suspensión. En efecto, inicialmente el PSC debe efectuar la referida verificación dado que es posible que dicha solicitud sea falsa con los daños que de ello se derivarían (v.gr. la persona que efectúa la solicitud no sea efectivamente el Firmante/Suscriptor, lo cual produce perjuicios a éste como consecuencia de la indebida revocación o suspensión de su certificado).
- El segundo factor que debe considerarse, es la *perentoriedad* con el cual el PSC debe dar curso a la revocación o suspensión del certificado y eliminación del registro de certificados válidamente emitidos, en caso de una revocación. Este hecho, permitirá determinar al juez si el PSC fue o no lo suficientemente diligente al prestar este servicio. Lo anterior no obsta a que el PSC se comprometa contractualmente a ciertos estándares de rapidez en sus procedimientos de revocación y suspensión, lo cual ciertamente facilitará la función del juez.

Creemos que estos factores se deben apreciar de la misma manera en que tratamos la hipótesis de responsabilidad por inexactitud de los datos del certificado, sin perjuicio de que la perentoriedad en este caso pueda apreciarse más estrictamente, dado lo sensible que es el tiempo en la presente hipótesis.

iii) Tercera fase.-

En este periodo la decisión de revocar o suspender el certificado ha sido tomada por el PSC. La eliminación del certificado del registro de certificados vigentes o la inclusión de su condición de suspendido, respectivamente, ha sido formalmente adoptada, pero el Usuario que confía en el certificado puede que no tenga los medios de conocerla todavía, debido a la modalidad de comunicación que emplea el PSC a efectos de dar a conocer estas circunstancias.

Esto nos conduce a repasar los sistemas de comunicación sobre el estado de los certificados que puede adoptar el PSC.⁵⁶⁶

- Sistema de comunicación periódica

Conforme este sistema las listas de certificados válidamente emitidos se van renovando cada cierto tiempo, de manera que el Usuario que confía en el certificado no conocerá de la revocación o suspensión: hasta que se efectúe la eliminación del certificado o se incluya la suspensión del mismo, en la siguiente renovación periódica de la lista de certificados válidamente emitidos.

Conforme las disposiciones de los arts. 8.3. y 9.2. LFE, la extinción (revocación) y la suspensión de certificados son únicamente oponibles frente a terceros (entre ellos el Usuario que confía en el certificado) cuando la indicación de dichas circunstancias se incluyan en el servicio de consulta sobre vigencia de certificados. Como en este caso ello aún no ha ocurrido, un Usuario podría verse perjudicado al confiar de buena fe en un certificado que

⁵⁶⁶ La LFE evidentemente no se inclina por ningún sistema de comunicación de estos hechos en particular, de manera que es el propio PSC mediante su DPC y las PC quien establece el modelo a implementar.

adolesce de extinción (revocación) o suspensión, debiendo atribuirse la responsabilidad en este caso al PSC.

- Sistema de comunicación inmediata

En esta modalidad, el PSC habiendo adoptado la decisión de revocar o suspender el certificado y disponiendo su eliminación o inclusión como suspendido - respectivamente - en las listas de certificados válidamente emitidos, procede inmediatamente a renovar y publicar las nuevas listas, con lo que desaparece el lapso temporal que media entre la decisión adoptada por el PSC y su correspondiente comunicación, inherente a la modalidad anterior. A partir de ahí, la revocación o suspensión se hace oponible a terceros, quien confíe en el certificado posteriormente lo hará bajo su propio riesgo.

En definitiva, para determinar la responsabilidad del PSC en la fase que analizamos, habrá que dilucidar primeramente el modelo de comunicación sobre el estado de los certificados que éste emplea, por lo que la hipótesis de responsabilidad para estos supuestos se acota al sistema de comunicación o renovación periódica de las listas de certificados válidamente emitidos.

En ese contexto, el PSC se hace responsable únicamente en el caso que, producto del retardo negligente o culpable de la renovación periódica de las listas en la cual se elimina el certificado revocado o se anota el suspendido, se derivan perjuicios contra el Firmante/Suscriptor (que obró diligentemente) o el Usuario que confía, producto de las actuaciones de los terceros intrusos que se hallan en control de la firma electrónica.

iv) Cuarta fase.-

En este último período el certificado revocado ha sido efectivamente eliminado del directorio de certificados válidamente emitidos o, el suspendido ha sido anotado efectivamente como tal en el servicio de consulta sobre vigencia de certificados.

Durante esta fase debe descartarse toda clase de responsabilidad por parte del PSC, dado que el certificado ha dejado de ser confiable y es oponible a terceros, por lo que el riesgo de asumir daños se traslada a los propios terceros que negligentemente confíen en un certificado de esta clase.⁵⁶⁷

Hasta acá hemos procedido a identificar los supuestos de responsabilidad que devienen de los servicios de extinción y/o suspensión de los certificados, dividiendo la temática en cuatro fases o etapas para su mejor discernimiento. Llegados a este punto, resta analizar frente a qué sujetos responde el PSC por eventuales daños que surjan en las hipótesis descritas.

Desde nuestro punto de vista, deducimos que dichos sujetos podrán ser tanto el Firmante/Suscriptor como el Usuario que confía en el certificado. Sin embargo, todo dependerá del momento en que se halle la revocación o suspensión del certificado. De esta manera, el Firmante/Suscriptor no podrá pretender la responsabilidad del PSC en el periodo que abarca entre la pérdida del control exclusivo de la clave privada y la solicitud de revocación o suspensión. Por otra parte, debe descartarse que ambos sujetos puedan dirigirse contra el PSC una vez que éste ha procedido a eliminar el certificado revocado de la lista de los certificados válidamente emitidos o a procedido a anotar la suspensión del certificado, haciéndola notoria y visible para todos.

4.2.3.1. Necesidad de un servicio de sellado temporal.-

En base a lo analizado previamente, se evidencia que el factor temporal en la revocación o suspensión de certificados, reviste especial trascendencia al momento de determinar las responsabilidades que pueden surgir en ocasión de la pérdida de vigencia de un certificado (definitiva o temporal), puesto que, como se tuvo oportunidad de estudiar, las

⁵⁶⁷ Al respecto de la LMFE es categórica al indicar en su art. 11.b.i. que “Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:...b) cuando la firma electrónica esté refrendada por un certificado: i) verificar la validez, suspensión o revocación del certificado...”

responsabilidades se van asignando conforme a los periodos en que opera la revocación o suspensión del mismo.

En consecuencia, resalta la necesidad de contar con un *servicio de sellado temporal* a efectos de distribuir adecuadamente entre los sujetos involucrados, las responsabilidades que puedan surgir en los supuestos de revocación o suspensión de certificados. Y así se prevé precisamente en el art. 20.b. LFE.

Además, el sellado temporal es una herramienta fundamental para determinar la responsabilidad del PSC conforme al criterio de “perentoriedad”, ya que sin la existencia de un sellado temporal, se pone en serio riesgo a las partes implicadas.

En efecto, no deviene la misma responsabilidad para el PSC, cuando el Firmante/Suscriptor ha perdido el control exclusivo de su clave no habiendo comunicado aún de tal hecho al PSC; que cuando el PSC ha recibido la solicitud de revocación o suspensión. En idéntico sentido, se valorará de diverso modo la responsabilidad del PSC cuando habiendo recibido la solicitud de revocación o suspensión de parte del Firmante/Suscriptor, el PSC se demora en adoptar las medidas correspondientes; que cuando el PSC ha procedido a eliminar el certificado revocado de la lista de los certificados válidamente emitidos o a procedido a anotar la suspensión del certificado, haciéndola notoria y visible para todos.

Ahora bien, en caso de no sellarse temporalmente los mensajes firmados y certificados digitalmente, es imposible acreditar con certeza qué mensajes fueron emitidos en el momento previo a la solicitud de revocación/suspensión del certificado, y qué mensajes fueron emitidos con posterioridad a dicha petición, lo cual impide determinar quiénes son los llamados a responder civilmente.⁵⁶⁸

⁵⁶⁸ Los correos electrónicos suelen establecer fechas de emisión y recepción de los mensajes. Sin embargo, estos sistemas son adulterables tanto por el emisor y el receptor de un mensaje.

Por otra parte, en ocasión de las responsabilidades que eventualmente devienen para el Firmante/Suscriptor frente a terceros por los mensajes emitidos, el sellado temporal es importante para “evitar responsabilidad por los contratos firmados con clave revocada”⁵⁶⁹

Dado que el Firmante/Suscriptor, al no tener medio para probar la fecha en que la oferta del contrato fue remitida, podría verse en la imposibilidad de demostrar que esta oferta no fue emitida por él, para lo cual ciertamente serviría el hecho de demostrar que en dicho instante el PSC había revocado o suspendido el certificado que respaldaba su firma, a consecuencia de la pérdida el control exclusivo de la clave privada al momento en que se celebró tal contrato.

4.2.4. Responsabilidad en caso de extinción (revocación) o suspensión de los certificados por causas atribuibles al PSC.-

Al margen de los supuestos de responsabilidad del PSC proveniente de los servicios de extinción (revocación) o suspensión de los certificados previamente analizado, en los que se ha dejado establecido que el certificador debe responder por los daños que ocasione al firmante o a terceros de buena fe, por la ausencia o el retraso en la inclusión en el servicio de consulta de la extinción o suspensión de la vigencia del certificado; sobreviene otra hipótesis de responsabilidad que pasamos a explicar.

La presente hipótesis alude a la responsabilidad del PSC como consecuencia de la extinción (revocación) o suspensión de los certificados, por causas (acciones u omisiones) culposas atribuibles al propio PSC, mismas que pueden devenir - entre otros - como resultado de los siguientes hechos: i) cese voluntario de las actividades del PSC; ii) cancelación de las certificaciones obtenidas; y iii) causas técnicas.-

En situaciones como las expuestas el certificado pierde su validez definitiva o temporal de manera anticipada, consecuencia de lo cual, el Firmante/Suscriptor puede sufrir menoscabos en su patrimonio, dado que el periodo validez del certificado ha sido acortado

⁵⁶⁹ (A. Martínez, 2000: 279).

por causas ajenas a su voluntad o culpa, lo que importa en principio un incumplimiento negligente del contrato por parte del PSC.⁵⁷⁰

Pasaremos a continuación a efectuar un sintético análisis de cada uno de los supuestos planteados.

a) Cese voluntario de las actividades del PSC.-

El art. 21.1. LFE determina que el PSC en ocasión de cesar voluntariamente en su actividad, se encuentra forzado a comunicarlo previamente a cada uno de los titulares de firmas electrónicas certificadas por aquél, debiendo además - cuando no exista oposición por parte de los titulares - transferir sus certificados a otro PSC que los asuma en la fecha en que el cese se produzca.

Pero si existe oposición, dejarán sin efecto los certificados respecto de los cuales el titular se haya opuesto a la transferencia. La citada comunicación se debe llevar a cabo con una antelación mínima de dos (2) meses al cese efectivo de la actividad.

Esta obligación es común a toda clase de PSC, teniendo por finalidad que el Firmante/Suscriptor, o bien tome las medidas pertinentes a fin de evitar que la cancelación del certificado le produzca perjuicios; o bien decidida que su certificado sea traspasado a otro PSC.

Efectivamente, el PSC se hará responsable por la oportuna comunicación de las circunstancias aludidas dentro de los plazos que para este efecto establece la ley. En caso que el PSC no informe el cese de actividades, o si lo ha hecho pero fuera del margen de los dos meses que prescribe la Ley, deviniendo como consecuencia la producción de daños para el Firmante/Suscriptor, es indudable que el PSC debe asumir la responsabilidad correspondiente frente a aquél.

⁵⁷⁰ Excepto en el caso de expiración del periodo de validez, conforme el art. 8.1.a. LFE, que para el caso de certificados reconocidos es como máximo de cuatro años, según el art. 8.2. LFE.

Por último, en caso de que se haga traspaso de los certificados a otro PSC con la anuencia del Firmante/Suscriptor, es necesario concluir que los costos que ello demanda correrán por cuenta del PSC.⁵⁷¹

b) Cancelación las certificaciones técnicas obtenidas.-

La cancelación de las certificaciones técnicas obtenidas por el PSC,⁵⁷² es consecuencia de una serie de hechos graves, básicamente por incumplimiento del PSC de los requisitos necesarios para obtener dichas certificaciones, que hacen que la prestación de sus servicios o los productos de firma electrónica que proporciona (v.gr. Tarjetas inteligentes, token USB, etc.) no resulten acordes a las exigencias contempladas en la certificación emitida ni con las condiciones que se requiere para ello, conspirando de esta manera contra el sistema de confianza del cual se reviste esta clase de PSC “*certificado*”.

Por consiguiente, razonamos en sentido que si el PSC o los productos que proporciona han perdido su calidad de encontrarse “certificados”, éste tiene la obligación de proceder a revocar los certificados emitidos que se encuentren afectados.

Cuando la pérdida anticipada de vigencia del certificado se deba a la cancelación de las certificaciones que el PSC haya obtenido, consideramos que éste deberá hacerse responsable del incumplimiento culposo o negligente de las obligaciones que dieron lugar a la cancelación de la certificación de la que era beneficiario, y de la cual se podrían derivar daños que afecten al Firmante/Suscriptor como consecuencia de la pérdida anticipada de validez de su certificado.

En este sentido es elocuente lo establecido en el art. 22.1. LFE, al instituir un supuesto de responsabilidad general del PSC por los daños y perjuicios que causen a

⁵⁷¹ Estos costos se harán bajo cuenta del PSC como compensación al incumplimiento del contrato que celebró con el Firmante/Suscriptor. En definitiva, este traspaso gratuito constituye la forma en que se indemniza al Firmante/Suscriptor en el caso del cese voluntario del PSC o como consecuencia de la cancelación de la certificación de éste. Al contrario, en caso de que el Firmante/Suscriptor se niegue al traspaso de su certificado a otro PSC, es forzoso concluir que el PSC deberá indemnizar en principio con la devolución del precio que pagó su cliente en proporción al tiempo faltante para que el certificado extinga su vigencia. Lo anterior es sin perjuicio de que se puedan configurar daños de lucro cesante.

⁵⁷² Recordemos que la certificación técnica de un PSC, implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público, misma que es emitida por una entidad cualificada pública o privada (art. 26 LFE).

cualquier persona en el ejercicio de su actividad. Por ejemplo, en el caso que el Firmante/Suscriptor actúa confiado en que los procedimientos de seguridad del PSC se encuentran conformes a la certificación inicialmente obtenida, pero en la práctica la ausencia de fiabilidad en la actividad del PSC ocasiona que un tercero se introduzca en el sistema de certificados, modificando el contenido de los mismos y sobreviniendo perjuicios al Firmante/Suscriptor y/o a los Usuarios del certificado.

Respecto de los sujetos frente a los que el PSC debe asumir responsabilidad por los eventuales perjuicios en las hipótesis descritas, debemos concluir que podrán ser el Firmante/Suscriptor y/o el Usuario que confía en el certificado.

c) Por causas técnicas.-

De igual manera, si la pérdida de vigencia del certificado es consecuencia de la extinción (revocación) o suspensión del certificado “por causas técnicas”,⁵⁷³ el PSC podrá ser responsable en caso de que dichos problemas técnicos le sean imputables por culpa o negligencia, cuando fruto de dichas conductas se deriven perjuicios.

Así por ejemplo, en caso que el Firmante/Suscriptor se hallara impedido de celebrar una transacción electrónica a consecuencia de este suceso y/o se encontrara forzado a celebrar una transacción por medios físicos dado que estaba impedido de realizarlos electrónicamente, por lo cual se originaron perjuicios.

Respecto del sujeto activo de la acción de responsabilidad y eventual indemnización de daños y perjuicios, es claro que el Firmante/Suscriptor es el principal afectado de las situaciones planteadas, aunque llegado el caso, también el Usuario del certificado puede verse perjudicado por la negligencia del PSC, con lo cual, consideramos que se encontraría

⁵⁷³ Las mencionadas causas técnicas se refieren - entre otros hechos - por ejemplo, a eventos relacionados con cortes en la alimentación eléctrica y aire acondicionado en las instalaciones del PSC, exposición de sus equipos al agua, incendios, etc. que afecten temporalmente el normal desenvolvimiento de sus actividades, o incluso, atenten de modo definitivo contra sus sistemas de almacenamiento de información, ocasionándoles un daño permanente.

igualmente facultado para ser indemnizado por los daños ocasionados en las situaciones expuestas.

4.3. Hipótesis de responsabilidad derivadas del servicio de homologación.-

Con carácter previo se tiene estudiado que de acuerdo con la disposición del art. 14 LFE (que hace referencia a la equivalencia internacional de certificados reconocidos), los certificados electrónicos que se emiten al público como reconocidos por los PSC que se encuentran establecidos en un Estado que no sea miembro del Espacio Económico Europeo (EEE) - conforme a la normativa aplicable en dicho Estado - serán equivalentes a los emitidos por los PSC establecidos en territorio español, siempre que se cumpla alguna de las condiciones especificadas en los incs. a), b) o c) de dicho artículo, las cuales se corresponden en el ordenamiento comunitario con los incs. a), b) o c) del art. 7 de la DFE.⁵⁷⁴

El precepto contemplado en el art. 14, inc. b) LFE impone como condición dos aspectos: i) el hecho que el certificado esté garantizado por un PSC establecido en el EEE, y ii) que el PSC observe los requisitos establecidos en la DFE para la emisión de certificados reconocidos. De ese modo se configura la prestación del *servicio de homologación* de certificado reconocido, el cual es brindado por un PSC establecido en el EEE que cumple las normas comunitarias de firma electrónica.

La homologación consecuentemente puede ser efectuada por un PSC establecido en España, que como se tiene dicho constituye un servicio por el cual, el PSC radicado en territorio español y previo acatamiento a las disposiciones comunitarias (y españolas consideramos), avala la calidad de los certificados emitidos con carácter de reconocidos por un PSC extranjero, igualando sus efectos a los certificados emitidos por los PSC establecidos en España y, por consiguiente, a los radicados dentro del EEE.

⁵⁷⁴ Asimismo, en la Ley Modelo de la CNUDMI sobre firmas electrónicas es posible encontrar en el art. 12.2. una referencia respecto del reconocimiento de certificados extranjeros.

Recordemos que el servicio de homologación, contrariamente a lo que podría pensarse, no es prestado a los Firmantes/Suscriptores de los certificados emitidos,⁵⁷⁵ sino que son los terceros Usuarios que confían en los certificados emitidos por el PSC extranjero y que han sido homologados por el PSC domiciliado en España, los verdaderos destinatarios de este servicio.

En suma, lo que se pretende con la homologación es extender la validez de los certificados de firma electrónica avanzada emitidos como reconocidos por PSC extranjeros, así como extender la responsabilidad derivada de la certificación del PSC extranjero al PSC establecido en territorio español. De esa manera el Usuario que confía en el certificado, cuenta con dos responsables a los que se puede dirigir en caso de que sufra perjuicio, producto de un acto culposo o negligente del PSC extranjero en la certificación que efectúa.

Con ello evita el problema de tomar acciones legales contra al PSC extranjero en un país foráneo con todos los costes que ello implica, pudiendo dirigirse contra el PSC domiciliado en España quien asumirá la responsabilidad. No obstante, tómesese en cuenta que llegado el caso el PSC domiciliado en España podrá repetir en contra el PSC extranjero.

Ahora bien, para determinar si el PSC establecido en España actuó o no diligentemente en la homologación, de conformidad con el art. 22.2. LFE se tendrá en consideración el hecho de que el PSC haya cumplido con las obligaciones fijadas en la LFE, especialmente las señaladas en los incs. b) al d) del art. 12 LFE, los cuales se refieren a la verificación de la información contenida en el certificado, garantizar que el Firmante/Suscriptor se encuentra en posesión efectiva del juego de claves así como garantizar la complementariedad de aquellas, cuando ambas fueron generadas por el PSC extranjero.

⁵⁷⁵ Sin perjuicio de que el Firmante/Suscriptor sea efectivamente el destinatario del servicio de homologación, en caso de que un PSC extranjero homologue los certificados de firma electrónica avanzada en su país. Sin embargo, acá hacemos referencia a la homologación que efectúa el PSC establecido en España, y por ende, dentro del EEE.

En el supuesto que el PSC establecido en España haya dado estricto cumplimiento a dichas obligaciones, desde nuestro punto de vista no puede imputarse a éste los daños que sufra el Usuario que confía el certificado.

El sujeto legitimado para exigir la responsabilidad del PSC domiciliado en España derivado del servicio de homologación, será en este caso el Usuario que confía en el certificado emitido por el PSC extranjero, avalado precisamente por el PSC español.

4.4. Hipótesis de responsabilidad por actuaciones de los auxiliares del PSC.-

Debido a que el PSC puede valerse de auxiliares para cumplir con sus obligaciones, ya sea que se trate de su propio personal o de entidades en las que delegan ciertas funciones, es lógico concluir que el PSC asume la responsabilidad por las actuaciones de aquellos.

Y así lo prevé precisamente el art. 22.4. LFE al disponer que “*Los prestadores de servicios de certificación asumirán toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.*”⁵⁷⁶

El supuesto típico de delegación de funciones en terceros sujetos, se encuentra representado - entre otros - por las Entidades de Registro (ER).⁵⁷⁷

Cuando en el servicio de registro intervienen las ER, encargadas de la recopilación y verificación de datos del solicitante de un certificado, en caso que medie culpa o negligencia de la ER provocando que el PSC consigne certificados con datos inexactos ¿quién debe responder civilmente por los eventuales daños que surjan? ¿el PSC o la ER?

Conforme expone Martínez Nadal, el sujeto llamado a responder en estos casos sería el PSC, ya que “*...es indudable que, por la esencialidad de esta función para el servicio de*

⁵⁷⁶ El art. 1.903 C.c. dispone a su vez que “*La obligación [de reparar el daño causado] que impone el artículo anterior es exigible, no sólo por los actos u omisiones propios, sino por los de aquellas personas de quienes se debe responder... Lo son igualmente los dueños o directores de un establecimiento o empresa respecto de los perjuicios causados por sus dependientes en el servicio de los ramos en que los tuvieran empleados, o con ocasión de sus funciones.*”

⁵⁷⁷ Cabe recordar que las ER pueden formar parte estructural e integrante de la empresa certificadora y operan como unidades desconcentradas pero dependientes de la misma (a modo de agencias o sucursales), o pueden ser entidades completamente ajenas e independientes a la empresa certificadora con las que el PSC ha suscrito un contrato o convenio correspondiente, haciendo notar no obstante que en cualquiera de los casos la ER delegada actúa por cuenta y en nombre del PSC, es decir, en representación de aquél.

*certificación que está ofreciendo, la responsable última es la autoridad de certificación, con independencia de que desempeñe esta función directamente o a través de terceros, dependientes o independientes”.*⁵⁷⁸

Por nuestra parte compartimos dicha aseveración, dado que el PSC da fe de la veracidad de sus certificados conforme a sus prácticas de certificación (DPC), debe hacerse responsable de las actuaciones negligentes de la ER en quien han delegado el servicio de registro de solicitantes.

Y es precisamente esa la solución adoptada por el art. 13.5. LFE al disponer que “*Los prestadores de servicios de certificación podrán realizar las actuaciones de comprobación previstas en este artículo por sí o por medio de otras personas físicas o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación.*”

Rodríguez nos proporciona mayores luces al respecto, cuando afirma “*De hecho, preexiste la relación contractual entre el prestador y el titular del certificado, que obliga al primero al cumplimiento de las obligaciones que le impone expresamente la ley, en las que interviene, en su caso, defectuosamente, el tercero auxiliar, por cuya conducta se hace responsable al prestador, sin necesidad de que haya incurrido en culpa in eligendo ni en culpa in vigilando, pues se trata de una responsabilidad objetiva, en la que incluso se impide al deudor principal acreditar su falta de culpa.*”⁵⁷⁹

Lo aseverado consideramos, sin inconveniente de que con posterioridad el PSC repita contra de la ER por los perjuicios que ha soportado al responder por un hecho ajeno, conforme lo estipulado por el art. 1.904 C.c..

Además, es necesario reparar en el hecho que tanto el Firmante/Suscriptor como el Usuario del certificado gozan de acción directa contra la ER, como consecuencia de la existencia de un concurso de responsabilidad contractual, el cual se materializa por medio del

⁵⁷⁸ (A. Martínez, 2000: 256).

⁵⁷⁹ (M. Huerta y D. Rodríguez, 2001: 133)

ejercicio de la correspondiente acción de responsabilidad contractual contra el PSC, y la extracontractual contra la entidad delegada, a fin de satisfacer la reparación de daños y perjuicios.⁵⁸⁰

V. Limitaciones a la responsabilidad del PSC contempladas en la LFE.-

Habiendo efectuado un análisis detallado de las diversas hipótesis de responsabilidad civil a las que eventualmente se podría ver enfrentado el PSC, resta por encarar el estudio de los supuestos de limitación legal a dicha responsabilidad, conforme se encuentran contemplados en la LFE. Esa es precisamente la tarea en la que nos focalizaremos a continuación.

Debido a que la responsabilidad de los PSC que no cuentan con normativa específica que regule la materia es potencialmente alta e imprevisible, ya que en estos casos la responsabilidad inevitablemente debe ser modulada por las reglas generales de responsabilidad,⁵⁸¹ varias legislaciones se ocupan precisamente de contemplar una serie de supuestos limitativos a dicha responsabilidad con la finalidad de paliar el enorme riesgo al que se verían sometidos los PSC.

Un ejemplo de lo indicado constituye precisamente la legislación española, que siguiendo el criterio del art. 6 (incs. 3 y 4) de la DFE se ocupa en el art. 23 LFE de regular determinadas limitaciones de responsabilidad que benefician al PSC. Aprovechamos de hacer notar al mismo tiempo, que la LFE no contempla limitaciones a favor del resto de sujetos implicados en el sistema de certificados, en particular el Firmante/Suscriptor, quien en determinados casos podría incluso llegar a contraer una responsabilidad objetiva sin que la ley prevea ningún límite que lo beneficie, lo que podría conducir a resultados excesivamente

⁵⁸⁰ (M. Huerta y D. Rodríguez, 2001: 133-134)

⁵⁸¹ Indistintamente que la naturaleza de la responsabilidad sea contractual o extra-contractual.

onerosos y el Firmante/Suscriptor podría verse enfrentado con riesgos potencialmente elevados.⁵⁸²

Como se tiene adelantado, el art. 23 LFE establece una serie de supuestos que limitan la responsabilidad del PSC, los cuales pueden ser divididos básicamente en dos categorías, a saber:

i) limitaciones intrínsecas al certificado, que son aquellas que dependen del contenido del certificado (art. 23.1.f. LFE); subdividiéndose a su vez en: cualitativas (art.11.2.h. LFE) y cuantitativas (art.11.2.i. LFE); y

ii) limitaciones extrínsecas al certificado, que son aquellas que dependen de la actuación de los distintos sujetos implicados en el sistema de certificados: el PSC (art. 23 numerales 5 y 6 LFE); el Firmante/Suscriptor (art. 23 numeral 1, en sus incisos a) al e) así como numerales 2 y 3 LFE); y, el Usuario del certificado (art. 23 numeral 4 LFE).

En las dos últimas posibilidades hablamos de limitaciones a la responsabilidad del PSC por acciones u omisiones atribuibles ya sea al Firmante/Suscriptor, ya sea al Usuario del certificado.⁵⁸³

Toda vez que de alguna manera estos supuestos de limitación a la responsabilidad del PSC fueron objeto de previo análisis,⁵⁸⁴ en el entendido que la interpretación extensiva del art. 23 LFE permite inferir, que dicha disposición contiene verdaderas obligaciones a las que tanto el Firmante/Suscriptor como el Usuario del certificado están llamados a observar, no vamos a redundar acá sobre lo ya expuesto remitiéndonos al apartado correspondiente, pero sí aprovecharemos de clarificar el modo en que la doctrina clasifica estos eximentes de responsabilidad así como analizaremos sintéticamente su contenido.

⁵⁸² Por ejemplo, cuando como consecuencia de la pérdida de la clave privada, se han efectuado operaciones por un tercero que devienen en daños y perjuicios, debiendo el Firmante/Suscriptor asumir toda la responsabilidad independientemente de si la pérdida de su clave se debió, o no, a su negligencia.

⁵⁸³ Un estudio bastante completo sobre las limitaciones de responsabilidad del PSC intrínsecas y extrínsecas al certificado (art. 23 de la LFE) puede ser consultado en (A. Martínez, 2004: 382-399).

⁵⁸⁴ Concretamente a momento de estudiar la temática que hace a las obligaciones que asumen tanto el Firmante/Suscriptor como el Usuario que confía en el certificado, lo que hemos denominado *Contenido del contrato de certificación reconocida*.

5.1. Limitaciones intrínsecas al certificado.-

Las limitaciones intrínsecas al certificado son aquellas limitaciones a la responsabilidad del PSC que dependen del contenido del certificado, mismas que fueron consignadas ya sea, porque el PSC los introdujo de manera unilateral (precisamente para limitar su responsabilidad contractualmente) o bien, porque fue el propio Firmante/Suscriptor quien solicitó la inclusión de dichos límites a momento de solicitar el certificado.

Se encuentran reguladas en el art. 23.1.f. LFE y se subdividen a su vez del modo siguiente:

5.1.1. Limitaciones intrínsecas de carácter cualitativo.-

Efectivamente, el art. 23.1.f. LFE establece de modo categórico que el PSC no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, en los casos que el Firmante/Suscriptor haga empleo del certificado con inobservancia: de los límites en cuanto a sus posibles usos.

Se hace notar que la inclusión en el certificado de límites cualitativos se encuentra prevista en el art. 11.2.h. LFE así como en el art. 6.3. de la DFE.

5.1.2. Limitaciones intrínsecas de carácter cuantitativo.-

En el mismo sentido, el citado art. 23.1.f. LFE establece igualmente que el PSC no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, en los casos que el Firmante/Suscriptor haga empleo del certificado con inobservancia: del monto autorizado para cada transacción individualizada.

Se hace notar que la inclusión en el certificado de límites cuantitativos se encuentra previsto en el art. 11.2.i. LFE así como en el art. 6.4. de la DFE.

En ambos casos es necesario remarcar, que el legislador prevé la posibilidad de que el PSC se exonere de responsabilidad, cuando se superen los límites en cuanto a los posibles usos y/o al monto autorizado, previstos por el propio PSC en su DPC y las PC para cada

certificado. En el fondo, lo que está contemplando el legislador es la posibilidad de que el PSC pueda establecer en relación a un determinado certificado, cláusulas que lo exoneran de responsabilidad.

Si bien a nivel contractual ello es posible (excepto cuando revista categoría de cláusula abusiva en contrato celebrado con consumidores), el asunto es de sumo interés dado que se está admitiendo que las cláusulas que determinan los usos y/o montos autorizados de los certificados válidamente emitidos, pueden exonerar de responsabilidad extracontractual al PSC frente a terceros. En definitiva, lo que el art. 23.1.f. LFE permite es que el PSC pueda limitar su responsabilidad extracontractual por medio de cláusulas limitativas de responsabilidad.

Creemos por consiguiente, que en el caso de los terceros (*strictu sensu*) esta limitación no podría operar, debido a que para la efectividad de este eximente, es necesario que la cláusula limitativa de responsabilidad sea reconocible por terceros, cuestión imposible en el supuesto que analizamos, dado que el tercero nunca tuvo la carga de consultar los datos de certificado.

Además, se requiere que el daño tenga su origen en el empleo indebido o fraudulento de un certificado de firma electrónica, cuestión que dicho tercero tampoco pudo hacer, dado que las hipótesis de responsabilidad que lo afectan en nada tienen que ver con estas circunstancias; en consecuencia consideramos que el referido artículo debe ser interpretado restrictivamente.

5.1.3. Inobservancia a las condiciones de uso del certificado.-

Finalmente, la redacción final del art. 23.1.f. LFE, denota que el PSC tampoco será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, cuando el Firmante/Suscriptor emplee el certificado emitido a su favor con inobservancia a las *condiciones establecidas para su uso*, mismas que figuran en la Declaración de Prácticas y

las Políticas de Certificación asociadas al certificado y que fueran comunicadas oportunamente (a tiempo de solicitarse la emisión del certificado) por el PSC.

5.2. Limitaciones extrínsecas al certificado.-

Nos referimos a limitaciones extrínsecas al certificado, aludiendo aquellas limitaciones a la responsabilidad del PSC que dependen de la actuación de los distintos sujetos implicados en el sistema de certificados: el Firmante/Suscriptor, el Usuario del certificado, e inclusive el propio PSC. Detallaremos a continuación cada uno de estos supuestos.

5.2.1. Provenientes de la actuación del Firmante/Suscriptor.-

Se encuentran normados en el art. 23 numerales 1, 2 y 3 LFE, constituyendo limitaciones a la responsabilidad del PSC por acciones u omisiones atribuibles al Firmante/Suscriptor.

Así, el art. 23.1. LFE establece que el PSC no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos: por inexactitud inicial de los datos consignados en el certificado (inc. a); por inexactitud devenida del certificado - es decir falta de comunicación de cambio de datos - (inc. b); ausencia de diligencia en la custodia de los datos de creación de firma - clave privada- (inc. c); incumplimiento del deber de solicitar la revocación o suspensión del certificado (inc. d); empleo extemporáneo de un certificado extinguido (inc. e).

Por otra parte, el art. 23.2. LFE que se refiere a los casos en que se emite un certificado de atributos dinámicos por el cual se consigna un poder de representación del firmante, establece que el PSC estará exento de responsabilidad en ocasión que tanto el firmante como la persona o entidad representada (cuando tenga conocimiento de la emisión del certificado), no procedan a solicitar la revocación o suspensión de la vigencia del certificado de conformidad a las previsiones que la LFE contempla para dicha tramitación.

Finalmente, el art. 23.3. LFE determina que el PSC no se hará responsable en los casos de certificados emitidos a favor de personas jurídicas, cuando el solicitante actué con inobservancia de las obligaciones contempladas en el numeral 1 del art. 23, lo que nos remite directamente a lo señalado previamente, a momento de estudiar el contenido del art. 23.1. LFE.

5.2.2. Provenientes de la actuación del Usuario del certificado.-

Se encuentran normados en el art. 23.4. incisos a) y b) LFE, constituyendo limitaciones a la responsabilidad del PSC por acciones u omisiones atribuibles al Usuario del certificado, que determinan una verdadera conducta negligente de su parte.

De esa manera, el art. 23.4.a LFE establece de modo categórico que el PSC no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, en los casos que el Usuario del certificado (*destinatario de los documentos firmados electrónicamente*) no proceda a comprobar y tenga en cuenta los límites: i) en cuanto a sus posibles usos y/o ii) en cuanto al monto autorizado para cada transacción individualizada, mismos que figuran en el propio certificado, ya sea porque el PSC los introdujo de manera unilateral (precisamente para limitar su responsabilidad contractualmente) o bien porque fue el propio Firmante/Suscriptor quien solicitó la inclusión de dichos límites a momento de solicitar el certificado.

El supuesto del inc. i) constituye una limitación extrínseca de carácter cualitativo, haciendo notar que la inclusión en el certificado de límites cualitativos se encuentra prevista en el art.11.2.h. LFE así como en el art. 6.3. de la DFE.

En tanto que el supuesto del inciso ii) constituye una limitación extrínseca de carácter cuantitativo, haciendo notar que la inclusión en el certificado de límites cuantitativos se encuentra previsto en el art.11.2.i. LFE así como en el art. 6.4. de la DFE.

Finalmente, el art. 23.4.b. LFE establece que el PSC no se hará responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, en los supuestos que el Usuario del certificado: i) no tome en cuenta la suspensión o pérdida definitiva de vigencia del certificado publicada en el servicio de consulta sobre vigencia de los certificados; o ii) no proceda a verificar la firma electrónica.⁵⁸⁵

5.2.3. Provenientes de la actuación del PSC.-

Se encuentran normados en el art. 23 numerales 5 y 6 LFE, constituyendo limitaciones a la responsabilidad del PSC por acciones diligentes atribuibles al propio PSC.

Como sabemos, en caso que el Solicitante y futuro Firmante/Suscriptor acredite una serie de datos que figuran en un registro público (v.gr. escrituras de constitución de la empresa, poderes de representante legal, etc. mismos que deben figurar inscritos en el Registro Mercantil), el PSC tiene el deber de comprobar si efectivamente dicha información cursa en el citado registro con carácter previo a la emisión del certificado. En ese entendido, el art. 23.5. LFE establece como una limitación a la responsabilidad del PSC, el hecho que la información acreditada mediante documento público por el Firmante/Suscriptor y comprobada por el PSC conforme se explicó previamente, adolezca de inexactitudes que luego determinen el surgimiento de daños y perjuicios.

En otras palabras, el PSC no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, por la inexactitud de los datos que consten en el certificado, si éste ha cumplido diligentemente con su obligación de verificar (de manera inmediatamente anterior a la emisión efectiva del certificado) la constancia en el registro público correspondiente, de los documentos presentados por el Solicitante a momento de hacerse presente ante las oficinas del PSC o la ER delegada, a objeto de solicitar el certificado.

⁵⁸⁵ Con relación a esta limitante de responsabilidad del PSC, el art 11 de la LMFE establece que “Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para: a) verificar la fiabilidad de la firma electrónica; o b) cuando la firma electrónica esté refrendada por un certificado: i) verificar la validez, suspensión o revocación del certificado; y ii) tener en cuenta cualquier limitación en relación con el certificado.”

Por último, el art. 23.6. LFE dispone que el PSC no será responsable frente a terceros de los daños que se podrían ocasionar por su actividad certificadora, cuando éste desarrolle sus funciones con la debida diligencia profesional que le resulta aplicable. En todo caso, sobre el PSC recae la carga de probar los niveles de diligencia que efectivamente aplicó si quiere exonerarse de responsabilidad.

VI. Responsabilidad civil emergente para el Firmante/Suscriptor.-

Llegados a este punto, procuraremos esbozar en líneas generales el régimen de responsabilidad civil que se observa en el caso del Firmante/Suscriptor. Como se tiene analizado, los supuestos de responsabilidad devienen para este sujeto como consecuencia de las acciones u omisiones previstas en los incisos a) al f) del art. 23.1. de la LFE, los cuales se configuran a manera de catálogo de verdaderas obligaciones legales, mismas que devienen en contractuales al ser incorporadas en el contrato de certificación reconocida, que es lo que normalmente ocurre, o por lo menos, debería ocurrir.⁵⁸⁶

Como es suficientemente conocido, una de las bases principalísimas en que se fundamenta el sistema de seguridad para el empleo de firmas y certificados digitales, lo constituye la posesión exclusiva y confidencial de la clave privada por parte de su titular, quien es al mismo tiempo Firmante/Suscriptor del certificado, de manera que su custodia diligente constituye una de las obligaciones principales por parte de éste, de conformidad con la interpretación extensiva del art. 23.1.c. LFE.

En consecuencia, resulta totalmente llamativo el hecho que tanto en la legislación española como la comunitaria sobre firma electrónica, no se determine ningún tipo de responsabilidad atingente al Firmante/Suscriptor, así como tampoco se prevén los daños y perjuicios que como consecuencia del empleo indebido que se haga del certificado o de la pérdida de confidencialidad de la clave privada podrían devenir; mucho menos se encuentra

⁵⁸⁶ Con relación a la responsabilidad del firmante, el art. 8.2. de la LMFE señala que “Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1.”; dicho párrafo enumera en tres incisos - inc. a) al c) - el conjunto de obligaciones que debe observar el firmante, cuyo incumplimiento determinan su responsabilidad, configurándose por consiguiente un catálogo de supuestos específicos de responsabilidad del Firmante/Suscriptor.

previsto un debido procedimiento a seguir en el caso de que estos incidentes se originen; ni el tipo de responsabilidad que por estos eventos deviene para el Firmante/Suscriptor frente a terceros.⁵⁸⁷

En suma, no queda lo suficientemente claro cuál es el régimen de responsabilidad que surge para el Firmante/Suscriptor en el sistema de certificados. En todo caso, de verificarse la generación de daños y perjuicios como consecuencia de la conducta del Firmante/Suscriptor, debemos procurar identificar los siguientes aspectos:

6.1. Naturaleza de la responsabilidad: objetiva o subjetiva.-

La problemática se centra en establecer si el Firmante/Suscriptor responde únicamente en aquellos casos en que haya incurrido en negligencia, por ejemplo en la custodia de la clave privada que ha perdido confidencialidad o, si debe responder en todo caso, de forma independiente a que si su conducta fue negligente o diligente.

Ante la realidad descrita en sentido de no existir un marco de responsabilidad específico, entendemos que la responsabilidad del Firmante/Suscriptor será - al menos en principio - objetiva, sujetándose consecuentemente a la normativa general. El simple hecho del incumplimiento de sus obligaciones señaladas en la ley, determinará el surgimiento de responsabilidad sin que medie una valoración subjetiva de su conducta.

Desde este punto de vista, cáigase en cuenta que la responsabilidad del Firmante/Suscriptor evidentemente resulta a todas luces ilimitada, lo que puede enfrentar a este sujeto a asumir un riesgo potencialmente elevado “...*cuando doctrinalmente se defiende que debiera haberse limitado la misma*”.⁵⁸⁸

Por consiguiente, resulta evidente que para el Firmante/Suscriptor resulta más beneficioso la aplicación de la responsabilidad de carácter subjetiva y por culpa (de acuerdo con el principio general de responsabilidad por culpa establecido en el Código Civil

⁵⁸⁷ (J.F. Ortega, 2004: 418 y ss.).

⁵⁸⁸ (M. Huerta y D. Rodríguez, 2001: 128).

arts.1.103 y 1.104) ya que en este caso únicamente habrá de responder cuando - entre su conducta y el daño efectivamente ocasionado - haya mediado culpa de su parte, lo que reduce considerablemente los riesgos para éste.⁵⁸⁹

Frente a la solución descrita, el acoger una responsabilidad de carácter objetivo significaría que el Firmante/Suscriptor se vea llamado a responder por los daños o perjuicios ocasionados por su conducta en todos los casos, es decir, independientemente si medio o no culpa de su parte, si actuó de modo diligente o manifiestamente negligente; lo que como se viene manifestando, resulta a todas luces bastante desventajoso, pues el Firmante/Suscriptor se verá compelido a responder por daños de modo ilimitado, conduciendo a resultados excesivamente onerosos.

Esta situación en criterio de Rodríguez, podría paliarse estableciendo limitaciones cuantitativas de responsabilidad, como ocurre en el caso de los clausulados de los contratos de emisión de tarjetas de crédito.⁵⁹⁰

6.2. Sujetos frente a los que responde el Firmante/Suscriptor.-

Los sujetos frente a los que el Firmante/Suscriptor debe responder por eventuales daños y perjuicios, dependiendo el caso en concreto serían:

El PSC.-

Respecto del cual si bien es cierto que el certificador no sufre un daño directo, toda vez que el uso ilegítimo de la clave privada (por un tercero que se apoderó de ella como consecuencia de la pérdida sufrida por el Firmante/Suscriptor) no representa para el PSC un perjuicio inmediato; no obstante, cáigase en cuenta que deviene un perjuicio indirecto (nada superfluo por cierto) consistente en su descrédito y la pérdida de fiabilidad entre sus clientes

⁵⁸⁹ Pero como hace notar García Más: “No obstante, aún siendo ésta la posición mayoritaria de la doctrina, no es compartida unánimemente, defendiendo algunos autores que el régimen general de responsabilidad no debe ser alterado y que, por tanto, el carácter ilimitado de la responsabilidad debe producirse en todo caso”. F.J. García Más, “La contratación electrónica: La firma y el documento electrónico”, *RCDI*, N° 65, 1999, pp. 765-790.

⁵⁹⁰ Efectivamente, el referido autor señala que la responsabilidad por posibles utilizaciones ilegítimas de la clave de firma, desde el momento de su pérdida hasta la publicación de la revocación del certificado correspondiente, recae en la persona que, como ocurre en la tarjetas de crédito extraviadas, es titular del certificado y de la clave de la firma respectiva, razón por la cual defiende que en el futuro, al igual que en las tarjetas de crédito, se fije un límite de tal responsabilidad “*Rige, por tanto, en ese tracto temporal el que se denomina principio de autorresponsabilidad.*” (M. Huerta y D. Rodríguez, 2001: 137). En igual sentido (A. Martínez, 2004: 369).

y la comunidad en general, pues se pone en entredicho su capacidad de generar confianza, con los consecuentes efectos de mala imagen.

Al encontrarse establecida la custodia de la clave privada como una obligación contractual y ante el incumplimiento por parte del Firmante/Suscriptor, lo más probable es que el certificador proceda a resolver el contrato y revoque el certificado expedido, con la consiguiente indemnización de daños y perjuicios.

El Usuario del certificado.-

Respecto del cual el Firmante/Suscriptor mantiene una relación comercial habitual, pues llevan a cabo una serie de transacciones de comercio electrónico en sentido estricto, para lo cual precisamente el firmante ha tenido que hacerse con carácter previo de una firma y un certificado que la avale, a objeto de respaldar la firma electrónica que emplea para rubricar electrónicamente los documentos que hacen a su relación comercial con su cliente - el Usuario del certificado - quien podría sufrir daños y perjuicios como consecuencia del empleo indebido de la clave privada.

Por ejemplo, en el caso que un tercero en posesión de la clave extraviada y haciéndose pasar por el titular del certificado (es decir un firmante ilegítimo), cierra con el Usuario del certificado transacciones que por su origen fraudulento, signifiquen el surgimiento de perjuicios para el Usuario (v.gr. pérdidas de mercado, pérdidas de oportunidad, etc.). En este caso, el Usuario podrá exigir que el Firmante/Suscriptor asuma la responsabilidad correspondiente.

Tercero perjudicado.-

Finalmente piénsese que al igual que en el caso anterior, podría presentarse la situación que ante la pérdida de la clave privada por parte del Firmante/Suscriptor, un tercero que se apodera de la misma (firmante ilegítimo) y se hace pasar por el titular del certificado, esta vez no frente a un cliente habitual del firmante (el Usuario habitual del certificado) sino

que cierra con otro tercero transacciones que por su origen fraudulento, signifiquen el surgimiento de perjuicios económicos para dicho tercero (v.gr. pérdidas de tiempo, costos de oportunidad, etc.). En este caso, dicho tercero podrá igualmente exigir que el Firmante/Suscriptor asuma la responsabilidad correspondiente.

6.3. Origen de la responsabilidad: contractual o extra contractual.-

Respecto del PSC.-

Entre el Firmante/Suscriptor y el PSC es más que evidente que media una relación contractual como consecuencia del perfeccionamiento del contrato de certificación reconocida suscrito, razón por la cual el carácter que reviste la responsabilidad del Firmante/Suscriptor es eminentemente contractual y sujeta a lo dispuesto fundamentalmente en los arts. 1.255, 1.091, 1.101, 1.258 C.c. Resultando aplicables además el art. 1.102 y ss. C.c..

Respecto del Usuario del certificado.-

Por otra parte, entre el Firmante/Suscriptor y el Usuario del certificado también existe una relación contractual pero de naturaleza electrónica, como consecuencia de las transacciones electrónicas que llevan a cabo de manera habitual, es decir, comercio electrónico en sentido estricto.

El carácter que reviste la responsabilidad del Firmante/Suscriptor es también y al igual que el supuesto anterior contractual, puesto que lo más probable es que las partes hayan introducido determinadas cláusulas en el contrato electrónico que prevén precisamente situaciones de responsabilidad por conductas que atenten contra la seguridad, integridad y confidencialidad de sus comunicaciones, siendo de aplicación las normas sobre responsabilidad que tenemos referidas previamente.

En todo caso resultarán también siendo auxiliares y en lo que fuera aplicable, las normas de la Ley 34/2000 (LSSI), particularmente las contenidas en el Título IV

“Contratación por vía electrónica”, artículos 23 al 29 y, la dispuesta en el art. 32 “Solución extrajudicial de conflictos”.

Respecto del tercero perjudicado.-

Cosa diversa es la naturaleza de la responsabilidad del Firmante/Suscriptor con relación al tercero perjudicado con el que contrató el firmante ilegítimo (el que se apropió de la clave privada). En este supuesto, nótese que entre el Firmante/Suscriptor y el tercero perjudicado no media ningún tipo de relación previa, por consiguiente no existe entre ellos un contrato, pero como consecuencia de la conducta negligente en la conservación de la clave privada del Firmante/Suscriptor, se han producido daños y perjuicios debido al empleo fraudulento de su clave privada.

En este caso el tercero perjudicado podrá exigir extracontractualmente del Firmante/Suscriptor la cobertura e indemnización por los daños y perjuicios sufridos, de conformidad con el art. 1.902 C.c. y las disposiciones del art. 1.089 C.c..

Conclusiones

I.-

Hoy en día el intercambio cotidiano de información tiene como elemento esencial a la *firma electrónica*, instrumento creado como mecanismo de identificación de su titular, que lleva aparejada un triple propósito: la firma electrónica acredita la identidad de la persona o entidad que está al otro lado de la transacción (autenticación); asegura que no ha existido ninguna manipulación posterior de la información o los datos que conforman el negocio (integridad); y en su caso, protege los datos de revelaciones o accesos a la información por parte de personas no autorizadas (confidencialidad).

Además, utilizando el sistema criptográfico de clave pública o asimétrica, el documento digital es firmado por el titular imprimiendo su clave privada secreta de la que solamente él tiene conocimiento y acceso. De esta manera, el autor queda vinculado a la firma digital que se verifica con la correspondiente clave pública, sin la posibilidad de negar su autoría (no repudio o irrevocabilidad).

II.-

La denominación “*firma electrónica*” hace alusión al género, comprende un amplio abanico de todos los medios tecnológicos que permiten firmar electrónicamente (desde los de existencia actual u otros de mayor avance tecnológico que surjan en el futuro), posibilitando la identificación del signatario o firmante, ya sea mediante: scaneo o digitalización de una firma manuscrita; firmas basadas en tecnologías de criptografía simétrica o clave única (v.gr. números PIN o Passwords); firmas basadas en tecnologías de criptografía asimétrica o doble clave, una privada y otra pública (v.gr. firmas digitales). De hecho, esta última constituye la tecnología más difundida hoy en día para la generación de firmas electrónicas seguras.

Asimismo existen firmas basadas en tecnologías biométricas (v.gr. individualización a través del reconocimiento de la retina del ojo o huellas digitales); firmas que no se basan en una tecnología específica, pero que como mínimo deben garantizar autenticación, integridad, no rechazo y confidencialidad (v.gr. firmas electrónicas avanzadas, que cuando emplean tecnologías de criptografía asimétrica coinciden con la denominación de firmas digitales).

A ésta última, de conformidad con la legislación española se suma además la *firma electrónica reconocida*, que no es otra cosa que una firma electrónica avanzada basada en un certificado electrónico reconocido y generada mediante un dispositivo seguro de creación de firma.

III.-

La noción de “*certificado electrónico*” hace alusión igualmente al género, constituye un documento electrónico que refleja determinada información de su titular y otros aspectos (v.gr. límites cuantitativos y/o cualitativos de empleo) que se encuentra firmado electrónicamente por una entidad de certificación que goza de la confianza de una determinada colectividad de usuarios de certificados. Al interior de este concepto general tienen cabida distintos tipos de certificados, cuyas finalidades, también pueden ser diversas.

Entre los certificados de mayor relevancia se encuentra el *certificado digital* o de clave pública, mediante el cual la clave pública de la firma digital se asocia de manera segura a una persona o entidad determinada. En ese entendido, un certificado digital es aquel que se encuentra refrendado con la firma digital de una tercera parte de confianza, nos referimos a la entidad de certificación, la cual ha procedido con carácter previo a la emisión del certificado a la confirmación de la identidad (u otros atributos) del titular de la respectiva clave privada, por ello se denominan también “*certificados identificativos*”, toda vez que relacionan a una persona con determinada clave pública.

Cuando para la emisión del certificado digital el PSC ha observado las normas contenidas en la LFE (art. 11 y ss.), entonces jurídicamente se denomina *Certificado reconocido*. Este tipo de certificado lleva asociada, por consiguiente, una *firma electrónica reconocida*.

IV.-

De la revisión del articulado de la LFE, se infiere que sus disposiciones son de aplicación transversal, vale decir, que sus preceptos rigen: en comunidades que para el empleo de firmas electrónicas han celebrado acuerdos previos y/o sin ellos; en entornos de comunicación cerrados y/o abiertos; para el caso del comercio electrónico en sentido amplio y/o el comercio electrónico en sentido estricto.

En cuanto al régimen jurídico de las firmas y los certificados electrónicos, la legislación española regula tres categorías de firmas, a saber: firma electrónica simple o genérica; firma electrónica avanzada; firma electrónica reconocida. Por otra parte, el legislador español aprueba la coexistencia de dos tipos o categorías de certificados: certificados electrónicos ordinarios (simples o en general) y certificados reconocidos.

Respecto del régimen jurídico de los servicios de certificación, los mismos se modulan en la LFE a lo largo de varios artículos fragmentarios centrados fundamentalmente en el PSC, que configuran una serie de deberes y obligaciones generales aplicables a todo tipo de certificadores (personas físicas o jurídicas; de derecho público o privado; gocen -o no- de una certificación técnica; tanto cuando emitan certificados ordinarios o reconocidos, como cuando se limiten a prestar otros servicios relacionados con la firma electrónica) dedicando un conjunto de obligaciones específicas para los PSC que emitan certificados reconocidos.

Por otra parte, la LFE no se ocupa de regular las obligaciones del Firmante/Suscriptor así como tampoco las del Usuario del certificado, a diferencia de lo que ocurre con el PSC, para quien dedica de forma más o menos meticulosa varios artículos que señalan sus obligaciones y específicamente dos artículos para abordar la temática de la responsabilidad (art.22 LFE) y los límites a la responsabilidad (art.23 LFE) *-sin agotar no obstante la materia-* articulado del cual se infieren ciertas obligaciones que recaen sobre el Firmante/Suscriptor y el Usuario del certificado. En todo caso se debe recurrir a efectuar una interpretación integral del texto normativo, para que a partir de ello, se coligue en qué consisten dichas obligaciones.

V.-

Se ha de entender por *contrato de certificación de firma electrónica*, aquel en virtud del cual una de las partes contratantes (PSC) asume la prestación de generar a favor de la otra

(*Firmante/Suscriptor*) un certificado electrónico, mediante el cual se acredita la identidad del Firmante/Suscriptor frente a terceros (*Usuarios del certificado*) en redes de comunicación electrónica, vinculando de modo seguro los datos de creación de firma con los datos de verificación de firma electrónica del Firmante/Suscriptor; asumiendo además el PSC (*frente al Firmante/Suscriptor y los Usuarios del certificado*), la obligación de gestionar el ciclo vital de los certificados electrónicos y colocar a disposición todos los componentes tecnológicos que hacen al funcionamiento propio de la certificación electrónica, garantizando con la debida diligencia y medios las funciones de seguridad y confianza del sistema. En tanto que la otra (*Firmante/Suscriptor*), asume la contraprestación de entregar al PSC una cantidad de dinero (*precio cierto y determinado*) por concepto de pago del servicio recibido.

VI.-

Los *contratos de certificación de firma electrónica* se pueden clasificar de diversas maneras, de las cuales hemos identificado como relevantes para nuestro estudio las siguientes. En primera instancia, según el ámbito de uso del certificado: para uso con otros sujetos pertenecientes a grupos cerrados o empleo del certificado en entornos abiertos de comunicación. En segundo lugar, según el tipo de certificación, ésta puede ser de personas o de sitios. En tercera instancia, atendiendo al destinatario de los servicios: se presentan contratos de certificación con consumidores o con empresarios (individuales o colectivos). En cuarto lugar, según la categoría de firma electrónica que contiene el certificado, existen contratos para certificar firmas electrónicas simples, avanzadas o reconocidas.

En una quinta categoría, por la naturaleza del PSC que emite el certificado, los servicios de certificación pueden ser brindados por personas físicas o jurídicas; de derecho público o privado; distinguiéndose además, los casos en que el PSC cuenta o no con una certificación para el desempeño de sus actividades. Finalmente, desde el punto de vista del ámbito territorial en que se presta el servicio, cabe distinguir la certificación a nivel nacional (en España), a nivel intracomunitario (en el Espacio Económico Europeo) y con alcance internacional (fuera de dichas fronteras).

VII.-

Atendiendo a la clasificación precedente, hemos procedido a circunscribir nuestro objeto de estudio, al supuesto donde los servicios de certificación de firma electrónica se prestan: para el empleo del certificado en entornos abiertos de comunicación, donde la certificación es de personas, el destinatario de los servicios es un empresario (individual o colectivo), la categoría de firma electrónica a certificarse es reconocida y el PSC que emite el certificado es también empresario, con lo que nos encontramos propiamente ante una prestación de servicios de certificación reconocida de firma electrónica, la cual se formaliza mediante el denominado *Contrato de certificación reconocida de firma electrónica* (o simplemente certificación reconocida).

En ese sentido, concluimos que la correspondencia del extendido *Contrato de certificación de firma electrónica* con respecto al *Contrato de certificación reconocida*, es la de género a especie.

VIII.-

Enmarcándonos en la realidad que denota hoy en día el tráfico, cual es la emisión de certificados digitales, se ha de entender por *Contrato de certificación reconocida de firma electrónica*, aquel en virtud del cual una de las partes contratantes (*PSC*) asume la prestación de generar a favor de la otra (*Firmante/Suscriptor*) un certificado reconocido, mediante el cual se acredita la plena identidad del Firmante/Suscriptor a momento de efectuar transacciones comerciales frente a terceros (*sus clientes al mismo tiempo que Usuarios del certificado*) en redes abiertas de comunicación, vinculando de modo seguro la clave privada con la clave pública del Firmante/Suscriptor. Asumiendo el PSC además, las obligaciones de habilitar los servicios de directorio y verificación del certificado así como gestionar su ciclo vital, colocando a disposición todos los componentes tecnológicos que hacen al funcionamiento propio de la Infraestructura de Clave Pública, garantizando con la debida diligencia las funciones características del sistema (*autenticación, integridad, no repudio y confidencialidad*). En tanto que la otra (*Firmante/Suscriptor*), asume la contraprestación de entregar al PSC una cantidad de dinero (*precio cierto y determinado*) por concepto de pago del servicio recibido.

IX.-

El empresario (individual o colectivo), que desea efectuar negocios comerciales valiéndose de una red abierta (*Internet*), con un número indeterminado de potenciales clientes, es decir actuando en un sistema *sin acuerdos previos* para el uso de firmas electrónicas, deberá acudir a un PSC debidamente establecido y de reconocido prestigio, quien es un empresario que se dedica típica y profesionalmente a la actividad de certificación prestando servicios al público, a objeto que previa celebración del *Contrato de certificación reconocida*, le emita un certificado reconocido con el cual avalará su plena identidad - en sentido amplio - ante sus clientes en la red, dotando a su firma y los documentos electrónicos suscritos con ella de la validez y eficacia jurídica, que la ley reconoce a las firmas manuscritas y los documentos privados respectivamente, estando facultado para contratar electrónicamente y así desarrollar negocios de comercio electrónico (en sentido estricto), cuyo objeto contractual consistirá en bienes de naturaleza tangible o intangible. Los primeros se articulan a través de contratos de compraventa o suministro (*comercio electrónico indirecto*); en tanto que los segundos, mediante contratos de cesión de derechos y/o contratos de prestación de servicios (*comercio electrónico directo*).

X.-

Resulta conveniente asimismo, diferenciar la certificación reconocida, en el que opera una prestación de servicios a objeto de identificar de manera indubitada a una persona física o jurídica, de otros contratos de certificación especiales. Entre estos últimos figuran: el contrato de certificación de sitios web, donde lo que se busca es identificar la pertenencia de un establecimiento virtual a una persona en concreto; el contrato de firma de códigos, cuya funcionalidad consiste en impedir cualquier posible violación de los derechos de la propiedad intelectual de códigos informáticos, manteniendo los derechos morales de su creador; y por último, el contrato de visados electrónicos, en el que mediante el visado electrónico el mensaje de datos se firma y se señala una única vez, con el objetivo de que terceros utilicen tales mensajes de datos de manera equivalente al soporte papel.

Si bien los servicios de certificación especiales, guardan una directa relación con el contrato de certificación de firma electrónica reconocida, toda vez que en algunas ocasiones resulta necesaria la certificación de firma para poder brindar otro tipo de certificaciones, lo evidente es que habitualmente se presentan en el tráfico como figuras contractuales independientes y diferenciadas.

XI.-

La función económica que cumple la certificación reconocida es la identificación - en sentido amplio - de los operadores económicos en el tráfico virtual, como requisito imprescindible para generar un entorno seguro, de manera que tanto los consumidores como las empresas puedan tener confianza en que sus transacciones no serán interceptadas, ni modificadas y se tenga la certeza que tanto el comprador y vendedor (emisor y receptor de un mensaje de datos) son efectivamente quienes dicen ser. La identificación en sentido amplio, debe entenderse como funcionalidad omnicomprendensiva de las restantes características de seguridad que aporta una firma electrónica reconocida, además de la identificación, vale decir: autenticación, integridad, no repudio y confidencialidad.

En todo caso, no debemos olvidar que la función identificativa de la firma electrónica, es tan solo una de las dos funciones que desde una perspectiva jurídica resulta relevante. Su función como instrumento para prestar el consentimiento en las relaciones contractuales de sus titulares, al igual que ocurre con la firma manuscrita en el ámbito tradicional, es su auténtica y definitiva finalidad, lo que se conoce como equivalente funcional.

XII.-

La certificación reconocida (*que es analizada en este estudio desde una triple perspectiva: de conformidad con la legislación española, la normativa comunitaria europea que hacen a la materia y los principios contenidos en las Leyes Modelo de CNUDMI sobre firmas y comercio electrónico*) reviste las características de una relación contractual consensual, siguiendo el principio general de libertad de forma consagrado en el ordenamiento jurídico. Asimismo se trata de un contrato sujeto a condiciones generales, perfeccionado por adhesión, pues su contenido vendrá impuesto por el PSC al Firmante/Suscriptor sin que exista, por tanto, negociación entre las partes. Cuando en su celebración intervienen empresarios, resulta siendo un contrato mercantil. Denota igualmente las características de contrato bilateral-sinalagmático, oneroso y conmutativo, no reviste calidad de *intuitu personae* y denota una relación obligatoria duradera de tracto continuo.

XIII.-

Atendiendo al propósito contractual concreto de la certificación reconocida, determinamos su carácter atípico pues carece de regulación específica en el ordenamiento, sin que exista la posibilidad de la aplicación analógica del régimen jurídico de otros tipos contractuales. No obstante, el fin objetivo del tipo contractual que estudiamos nos permite enmarcarlo dentro de los denominados contratos de actividad, y más apropiadamente, dentro del genérico "*contrato de servicios*".

Evidentemente, dentro de los amplios contornos del *contrato de servicios* encuentran acomodo muy diversas modalidades contractuales y, entre ellas, el contrato de certificación reconocida de firma electrónica objeto de nuestro estudio. De este modo se incardina en una

categoría - si bien de carácter doctrinal más no tipificada legalmente - que facilita su tratamiento jurídico.

XIV.-

Todo PSC tiene el deber con carácter preliminar a ofrecer sus servicios en el mercado, de elaborar una Declaración de Prácticas y Políticas de Certificación, debiendo ponerlas a disposición del público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

Asimismo, en la fase preliminar al perfeccionamiento del contrato de certificación reconocida, básicamente devienen dos deberes de conducta principales para ambas partes contratantes: el deber de proceder conforme la buena fe, y deberes de conducta e información recíprocos, de modo que ambas partes deben ejecutar los distintos pasos de la manera debida y prudente, con la intencionalidad de perfeccionar el contrato.

El solicitante y futuro Firmante/Suscriptor debe suministrar al PSC toda la información necesaria para realizar una correcta y plena identificación, garantizando su exactitud y veracidad. En tanto que el PSC debe informar entre otras cosas, sobre las condiciones en las que presta el servicio, respecto de los clausulados predispuestos y prácticas de certificación, las medidas de seguridad que se deben adoptar, el método empleado para comprobar la identidad del solicitante, las condiciones y límites (cuantitativos y/o cualitativos) de empleo del certificado, las garantías con las que cuenta para afrontar eventuales daños, las certificaciones obtenidas para desarrollar su actividad, los procedimientos para resolución extrajudicial de conflictos y finalmente debe informar respecto a los precios de sus servicios.

XV.-

El contenido del contrato de certificación reconocida se extiende más allá de lo expresamente pactado por las partes contratantes, a *“todas las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso y a la ley”*, debiendo por consecuencia integrarse de conformidad con lo dispuesto en el art. 1.258 C.c., en primer lugar, el conjunto de normas imperativas que le resultan aplicables, fundamentalmente las que devienen de la LFE. En segundo lugar, se deben integrar las normas dispositivas, éstas serán, fundamentalmente, las normas y principios generales que modulan la regulación de los denominados contratos de actividad, y más concretamente, las que regulan el genérico *contrato de servicios*, toda vez que, como ya se tiene señalado, el contrato de certificación reconocida se integra dentro de las señaladas categorías doctrinales. También, por supuesto, las normas dispositivas generales sobre obligaciones y contratos establecidas en el Libro I, Título IV del Código de Comercio y en el Libro IV del Código Civil.

Por último, para la integración del contrato resulta necesario tomar en cuenta, las reglas contenidas en los denominados instrumentos de autorregulación en general, y particularmente, las ofrecidas en la Declaración de Prácticas de Certificación (DPC) y las Políticas de Certificación (PC) asociadas al certificado, que el propio PSC ha elaborado individualmente. Entendemos que estas reglas deben integrar el contenido contractual, en aplicación de la buena fe contractual, pues el Firmante/Suscriptor habrá confiado legítimamente en su aplicación. Evidentemente, el contenido de la DPC y las PC adoptadas por el PSC pueden determinar, sin duda, que el Firmante/Suscriptor se haya decidido por éste

y no por otro prestador del servicio de certificación. Estas normas servirán además de criterio de interpretación de las condiciones generales que rijan el contrato.

XVI.-

Con relación a las obligaciones principales que surgen del contrato, el PSC está obligado, por un lado, a emitir y poner a disposición el certificado reconocido a favor de su cliente, el Firmante/Suscriptor; por el otro, a publicar los certificados manteniendo un directorio actualizado de consulta pública que refleje su estado (vigente, suspendido o extinguido), garantizando un servicio de verificación o validación de los mismos. La obligación principal del Firmante/Suscriptor consiste en el pago de un precio como contraprestación por el servicio contratado.

XVII.-

Respecto del pago del precio, en la mayoría de los casos consistirá en la entrega de una suma de dinero, configurándose por tanto, una obligación pecuniaria. El precio quedara fijado unilateralmente por el PSC, debiendo el cliente aceptarlo o rechazar la celebración del contrato; en caso afirmativo, el precio deberá ser satisfecho en el momento establecido en el contrato.

Asimismo, el Firmante/Suscriptor se obliga a la conservación diligente de su clave privada (datos de creación de firma); actuar dentro del marco general proporcionado por la Declaración de Prácticas y Políticas de Certificación; comunicar al PSC los casos en los que su clave privada se ha puesto en peligro, ha sido extraviada o de cualquier otra manera se ve comprometida; notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez; informar al PSC a la mayor brevedad posible, de la existencia de algún motivo que comprometa el mantenimiento de la confidencialidad de la clave privada; abstenerse en todo tipo de uso de su clave privada en caso de suspensión o extinción del certificado; y finalmente, emplear los certificados de conformidad con las condiciones establecidas y comunicadas a éste oportunamente por el PSC, respetando los límites cuantitativos y cualitativos que figuran en el certificado.

XVIII.-

En lo que se refiere a las obligaciones principales del PSC, debemos observar que no se trata de obligaciones independientes a cargo del prestador, pues todas ellas contribuyen, de igual modo, a la satisfacción del interés primario del acreedor, que es la identificación (en sentido amplio) en el tráfico virtual. Dicho de otro modo, todas las conductas del PSC necesarias e imprescindibles para satisfacer el propósito contractual, constituyen el objeto de la obligación principal.

Evidentemente, la primera conducta debida del PSC consiste en generar el certificado reconocido, pero sin su entrega al Firmante/Suscriptor, éste último no podrá adjuntar a los mensajes de datos que remita, ninguna evidencia que confirme la vinculación de su clave privada con la pública, dado que en ausencia de certificado (que es precisamente el instrumento que contiene la clave pública) no es posible efectuar la distribución de ésta entre los usuarios verificadores del certificado. Por consiguiente, no basta con que el PSC genere el certificado sino que además debe ponerlo a disposición del Firmante/Suscriptor.

Con todo, la emisión y puesta a disposición del certificado no bastan ni son suficientes para conseguir el propósito contractual, a lo sumo satisfacen la *auto-identificación* del Firmante/Suscriptor, pero evidentemente sin ninguna utilidad práctica. Si bien el PSC emite una única vez el certificado reconocido, haciendo entrega de éste a su titular, no obstante, debemos tener presente que el propósito del contrato es la identificación del Firmante/Suscriptor y no la mera entrega del certificado, que tan sólo es un medio para conseguir el fin.

Para que dicha identificación sea posible, es imprescindible que el tercero usuario del certificado posea una copia del mismo y de la clave pública asociada que le permita verificar la firma, elementos éstos que debe obtener del propio PSC. De esa manera, la entrega del certificado al Firmante/Suscriptor pero sin la distribución a los terceros usuarios de una copia del mismo junto con la clave pública asociada, no constituye un acto de identificación del Firmante/Suscriptor. Únicamente **los dos actos realizados conjuntamente** lo constituyen. Así, cuando el Firmante/Suscriptor contrató dicha prestación con el PSC, éste se obligó a cumplir las dos actuaciones: la entrega del certificado al Firmante/Suscriptor y la de una copia a los terceros usuarios que lo soliciten.

Todo lo antedicho nos lleva a la conclusión de que el PSC, a la par de la obligación de generar y entregar el certificado al Firmante/Suscriptor, también está obligado a proporcionar una copia de aquél al tercero que confía en el mismo, debiendo proceder por consiguiente, además, a publicar el certificado en un directorio de consulta por parte de terceros, a objeto que accedan a la clave pública asociada al certificado, con la cual llevaran a cabo la validación de la clave privada del Firmante/Suscriptor, lo cual únicamente se consigue con la prestación de un servicio ulterior de consulta sobre vigencia o verificación de certificados.

En otras palabras, la utilidad del servicio no se traslada al Firmante/Suscriptor únicamente con la emisión y puesta a disposición del certificado por parte del PSC, pues por sí solos no satisfacen el servicio útil, el propósito global e integral del contrato de certificación reconocida, por tanto, la prestación principal del PSC no se limita simplemente a emitir y entregar el certificado sino que se encuentra consustancialmente vinculada con otras dos prestaciones fundamentales, cuales son proporcionar los servicios de directorio y los de validación o verificación de certificados.

XIX.-

A efectos de la presente investigación, nos desmarcamos de aquellos sectores doctrinales que entienden que el único objeto aceptable del contrato de certificación reconocida es la emisión de certificados y que, la prestación de otros servicios vinculados a la certificación, quedan descartados.

Reconociendo que la emisión de certificados constituye un objeto fundamental del contrato estudiado, no estamos de acuerdo con los autores que sostienen y defienden la independencia contractual de prestaciones claramente asociadas - tanto en el plano jurídico como en el económico - así como tampoco nos parece lógico limitar su objeto a la simple emisión de certificados, toda vez que la identificación inequívoca del titular de firma y certificado reconocido no se circunscribe al momento de emisión del certificado, sino que ésta debe poder llevarse a cabo durante todo el tiempo de vigencia del certificado.

XX.-

Se ha establecido que a lo largo de las diversas etapas del ciclo vital del certificado reconocido (desde la emisión hasta su extinción), se generan un entramado de relaciones jurídicas entre los diversos sujetos implicados.

De esa manera, constatamos que entre el PSC y el Firmante/Suscriptor existe una relación contractual, instrumentalizada precisamente por el contrato de certificación reconocida.

Entre el Firmante/Suscriptor y el Usuario del certificado, se desarrolla una transacción de comercio electrónico ya sea en sentido amplio o estricto, dependiendo el caso en concreto. En el último supuesto verificamos la existencia de un verdadero contrato electrónico entre las partes contratantes (por tanto sometido a las reglas de la contratación electrónica), para cuyo perfeccionamiento de modo seguro y certeza de identidad de las partes es que el Firmante/Suscriptor, con carácter previo, precisamente debe hacerse de un certificado reconocido, por medio del cual refrendará el contrato en su relación electrónica con su contraparte, el Usuario del certificado y viceversa.

Entre el PSC y el Usuario del certificado, se ha sostenido que de inicio no existe una relación contractual, las facultades del Usuario para acceder a los servicios de directorio y verificación de certificados devienen de la LFE, en tanto que las obligaciones del certificador hallan su origen en el contrato de certificación reconocida. Es notorio que entre éstos evidentemente no han perfeccionado un nuevo contrato; el cumplimiento de las obligaciones del PSC se ubican en la esfera de la ejecución del único contrato, el perfeccionado con el Firmante/Suscriptor, en tanto que las obligaciones del Usuario tienen su origen en la LFE.

XXI.-

La afirmación precedente, no obstante, ha sido sujeta a relatividad, pues si bien es cierto que en entre el PSC y el Usuario del certificado no existe un contrato previo, ello es así al menos en principio, puesto que puede darse la situación en que el Usuario al acudir al «website» del PSC, se vea obligado a aceptar un clausulado general, de manera que estas condiciones generales vincularían contractualmente al Usuario con el PSC, lo que devendría habitualmente en la formalización de un “*Contrato de verificación de certificados*”.

A partir de este supuesto, nuestro análisis se recondujo a la consideración que las obligaciones que hacen al Usuario del certificado ya no tienen un origen exclusivamente legal, conforme tenemos desarrollado previamente, sino que revisten auténticos deberes contractuales que devienen de un nuevo contrato, el perfeccionado con el PSC a través del cual se modulan sus recíprocas conductas y responsabilidades.

El PSC podrá cobrar un precio por estos servicios, en la medida que las Declaraciones de Prácticas y Políticas de Certificación y el contrato de certificación reconocida celebrado con el Firmante/Suscriptor no lo prohíba expresamente, o desde otro punto de vista, dicho contrato no obligue al PSC a proporcionar gratuitamente el acceso tanto al directorio como al servicio de verificación de certificados. En todo caso, desde el punto de vista legal, tanto la norma comunitaria (DFE) como española (LFE) no disponen ningún óbice para que el PSC condicione la consulta y/o verificación de certificados a un pago previo.

En síntesis, la certificación reconocida se articula fundamentalmente en torno a un elemento objetivo: el certificado reconocido, a cuyo alrededor, a su vez, se interrelacionan tres elementos subjetivos: el PSC, el Firmante/Suscriptor y el Usuario del certificado, lo cual genera un entramado jurídico triangular entre tres entidades subjetivas independientes entre sí, pero vinculados por la operación económica subyacente; esta última, se modula jurídicamente a través del perfeccionamiento de dos contratos autónomos (certificación / verificación) pero funcionalmente afines, que es cabalmente la tesis que hemos adoptado en la presente investigación.

XXII-

Las obligaciones fundamentales del Usuario del certificado (*que se configuran como obligaciones legales o contractuales, según el caso*) consisten en comprobar y tener en cuenta las restricciones que figuren en el certificado reconocido en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él; tener en cuenta la suspensión o pérdida de vigencia del certificado publicada en el servicio de consulta sobre la vigencia de los certificados, así como verificar la firma electrónica reconocida.

XXIII.-

Los PSC están sujetos a un régimen de responsabilidad muy estricto por las actividades que realizan. Esta responsabilidad nace cuando han incumplido las obligaciones que se les imponen en la Ley o cuando, de acuerdo con los principios de responsabilidad contractual y/o extracontractual, hayan causado daños a terceros.

Es importante resaltar la inversión de la carga de la prueba que tanto el texto normativo comunitario como el español establecen. La confianza que se deposita en el buen hacer de estos prestadores obliga a que se imponga un sistema de responsabilidad casi objetiva, de manera que, una vez acreditado el daño y la relación de causalidad, el prestador de servicios deba probar su diligencia para eximirse de responsabilidad.

Asume responsabilidad subjetiva por los daños ocasionados frente al Firmante/Suscriptor y/o el Usuario del certificado (contractualmente), o terceras partes (extra-contractualmente) que se hayan visto perjudicadas por sus acciones u omisiones que determinan un comportamiento negligente, es decir que sobre el PSC recae un régimen de responsabilidad por culpa con inversión de la carga de la prueba, pues corresponde a éste en todo caso, demostrar que actuó con la debida diligencia profesional, para que no le sea imputable el daño ocasionado.

Con relación a los casos específicos en los que la actividad del PSC se encuentra sometida a límites de responsabilidad, se observa que dicha limitación respecto del Firmante/Suscriptor, opera, entre otros supuestos, cuando por ejemplo éste último no ha proporcionado al PSC información veraz, completa y exacta sobre los datos que deban constar en el certificado reconocido; o por negligencia en la conservación de sus datos de creación de firma. Respecto del usuario, opera, entre otros supuestos, cuando éste no compruebe y tenga en cuenta las restricciones que figuren en el certificado (*en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él*); cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados; o cuando no verifique adecuadamente la firma electrónica.

XXIV.-

Para garantizar la seguridad y la confianza en el tráfico mercantil, el PSC que expida al público un certificado presentado como reconocido o que garantice al público tal certificado, debe ser responsable como mínimo, por el perjuicio causado a cualquier entidad o persona física o jurídica que confíe razonablemente en el certificado, en cuanto lo que respecta a: i) la veracidad en el momento de su expedición, de toda la información contenida en el certificado reconocido y la inclusión en el certificado de toda la información prescrita para los certificados reconocidos; ii) la garantía de que en el momento de la expedición del certificado, obraban en poder del Firmante/Suscriptor identificado en el certificado reconocido los datos de creación de firma correspondientes a los datos de verificación de firma que constan o se identifican en el certificado; y iii) la garantía de que los datos de creación y de verificación de firma pueden utilizarse complementariamente, en caso de que el PSC genere ambos; salvo que el PSC demuestre que no ha actuado con negligencia.

Asimismo y por idéntica razón, el PSC que haya expedido al público un certificado presentado como certificado reconocido, debe ser responsable por el perjuicio causado a cualquier entidad o persona física/jurídica que confíe razonablemente en dicho certificado, cuando no ha registrado la revocación del certificado, salvo que el PSC pruebe que no ha actuado con negligencia.

Es posible que esta responsabilidad esté limitada cuando el PSC consigne en un certificado reconocido límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles para terceros. El PSC no deberá responder de los daños y perjuicios causados por el uso de un certificado reconocido que exceda de los límites indicados en el mismo. Así, el PSC puede consignar en el certificado reconocido un valor límite de las transacciones que puedan realizarse con el mismo, siempre y cuando los límites sean reconocibles para terceros y con ello limitar la cuantía de su potencial responsabilidad. El PSC no sería responsable por los perjuicios que pudieran derivarse de la superación de este límite máximo. Ello, sin perjuicio de que sí pueda imponerse la responsabilidad ilimitada cuando ese límite pudiera plantear algún conflicto con la normativa española de defensa de consumidores y cláusulas abusivas.

XXV.-

El Firmante/Suscriptor asume una responsabilidad objetiva o subjetiva (dependiendo el caso concreto) por las acciones u omisiones dañosas ocasionadas frente al PSC y/o el usuario del certificado (contractualmente), o terceras partes (extra-contractualmente) que se hayan visto perjudicadas por su comportamiento doloso o culposo.

XXVI.-

El funcionamiento conjunto entre la firma digital y el sistema de certificación reconocida conforme se tiene estudiado, constituye - por lo menos en la actualidad - el mecanismo tecnológico más adecuado para dotar de niveles mínimos de seguridad a las transacciones electrónicas celebradas en entornos o redes abiertas de comunicación.

Al abordar el estudio del sistema de certificación pusimos en relieve la importancia de establecer un sistema de responsabilidad civil adecuado, y por sobre todo claro, a fin de que

la certificación sea viable pudiendo atraer a empresas que estén dispuestas a prestar este servicio a precios relativamente accesibles a sus clientes.

Consideramos que el régimen de responsabilidad civil del PSC establecido en la LFE cumple con los requerimientos mínimos para considerarse óptimo. No obstante, estimamos que presenta falencias que son de importancia para configurar un régimen de responsabilidad más integral que el actualmente contemplado, como por ejemplo, la omisión a las responsabilidades que devienen para el Firmante y/o el Usuario por su actuación negligente, cuando fruto de ello se generan daños y perjuicios.

XXVII.-

La doctrina a momento de clasificar las distintas clases de comercio electrónico (CE), de manera prácticamente uniforme, reconoce las siguientes categorías de acuerdo con el contenido de la transacción electrónica de información: CE en sentido amplio y CE en sentido estricto. A su vez, el CE “*en sentido estricto*” admite las siguientes variantes: i) De acuerdo con el canal por el que se entrega el bien o servicio: CE directo y CE indirecto; ii) De acuerdo con la red/medio de información empleado: CE cerrado y CE abierto; iii) De acuerdo con la forma de pago por el bien o servicio: CE completo y CE incompleto.

Ahora bien, es necesario hacer notar que la doctrina a momento de referirse al comercio electrónico en sentido estricto que involucra una contratación (*es decir, dejando de lado las actividades de comercio electrónico que no implican una contratación, como por ejemplo: los pagos electrónicos*) cualquiera sea la modalidad (directo, indirecto, cerrado, abierto, completo o incompleto), dan por supuesta o implícita la existencia de una contratación en línea “*on line*”, vale decir, que los elementos determinantes a momento de clasificar las distintas categorías de comercio electrónico, no se encuentran en el modo de contratación (*que como se tiene dicho, se da por sobreentendido que es una contratación electrónica*), sino que acuden a elementos externos al modo de contratación, para categorizar el fenómeno.

Nuestra investigación permite identificar una clasificación adicional del CE en sentido estricto. Para ello, debemos analizar la temática partiendo del razonamiento inverso, es decir, del estudio de la forma de contratación dejando de lado los otros factores (*canal por el que se entrega el bien o servicio, el medio de información empleado o la forma de pago*).

Desde ese punto de vista, el contrato de prestación de servicios de certificación de firma electrónica, como se tiene estudiado, es un contrato que habitualmente se perfecciona con la presencia física de las partes (*por un lado el Solicitante, que pasa a denominarse Firmante/Suscriptor y por otro, el PSC o la Entidad de Registro delegada que actúa en nombre y por cuenta del PSC*), de modo que no se origina propiamente una contratación electrónica, aunque evidentemente la prestación de los servicios (*envío del certificado electrónico al Firmante/Suscriptor y demás servicios complementarios vinculados con la administración de una infraestructura de clave pública, por ejemplo: suspensión o revocación de certificados, consulta del directorio, etc.*) se efectúan por medios electrónicos.

De todo lo anotado hasta acá, es posible afirmar en consecuencia la existencia de una categoría de comercio electrónico en sentido estricto, en el cual no existe contratación electrónica, pero la prestación del servicio se efectúa por medios electrónicos,

independientemente de: el canal, el medio o la forma de pago. Razón por la cual es posible incorporar una clasificación de comercio electrónico adicional, del modo siguiente:

- **CE perfecto:** Referido al CE en el que la contratación del bien o servicio se efectúa en línea “on line”, independientemente del modo en que se articulan los demás factores.
- **CE imperfecto:** Referido al CE en el que la contratación es fuera de línea “off line”, pero la prestación del servicio se efectúa por medios electrónicos, independientemente de la forma de pago (medios electrónicos o tradicionales) e independientemente de si se efectúa en entornos abiertos o cerrados de comunicación.

En otras palabras, la contratación no es electrónica sino que se lleva a cabo por medios tradicionales, en presencia de las partes de modo simultáneo, aplicándose a dicha contratación todas las reglas tradicionales de los contratos. Pero a la ulterior prestación del o los servicios, que constituye en realidad la ejecución de acuerdo de voluntades plasmadas en el contrato, se aplicarían las reglas jurídicas de la prestación de servicios de la Sociedad de la Información, puesto que el servicio o servicios, efectivamente son prestados por medios electrónicos.

El ejemplo y paradigma del supuesto anterior, constituye precisamente la prestación de servicios de certificación de firma electrónica reconocida, toda vez que se instrumentaliza por medios tradicionales. Pero a la ulterior prestación del o los servicios asociados a la certificación reconocida (v.gr. emisión del certificado reconocido, administración del sistema de certificados, mediante la suspensión o revocación, servicios de consulta y validación de certificados, etc.) que constituyen en realidad la ejecución de acuerdo de voluntades plasmadas en el contrato de certificación reconocida, se aplicarían las reglas jurídicas de las prestación de servicios de la Sociedad de la Información, entre las que se encuentran la LSSI, DCE, LFE y DFE, puesto que el servicio o servicios, efectivamente son prestados por medios electrónicos.

Bibliografía

Obras físicas consultadas

- Albaladejo García, Manuel, *Compendio de Derecho Civil*, Barcelona, 3ª ed., 1976.
- Albaladejo García, Manuel, *Derecho Civil*, Barcelona, 7ª ed., 1982.
- Albaladejo García, Manuel, *Derecho Civil*, t.II, *Derecho de obligaciones*, v.II, *Los contratos en particular y las obligaciones no contractuales*, 9ª ed., Barcelona, 1994.
- Alfaro Aguilera-Real J., *Las condiciones generales de la contratación*, Madrid, Civitas, 1991.
- Almagro Nosete, José, “Comentarios al art. 1255 C.c.”, en Ignacio Sierra Gil de la Cuesta, comp., *Comentario del Código Civil*, T.6, Barcelona, Bosch, 2006.
- Alonso Olea, Manuel y Casas Baamonde, Marfa Emilia, *Derecho del trabajo*, 12ª ed., Madrid, 1991.
- Alpa, Guido, Corsaro, Luigi y otros, *Estudios sobre la Responsabilidad Civil*, Lima, ARA Editores, 2001.
- American Bar Association (ABA), *ABA Guidelines*, 1996.
- Andorno, Luis O., *La informática y el Derecho a la Intimidad*, LL 1985-A.Sec. Doctrina.
- Aparicio, Juan Manuel, *Contratos*, vol. I y II, Buenos Aires, Hammurabi SRL, 1997.
- Banedas Carpio, J.M. y otros, *Comercio electrónico y protección de los consumidores*, Madrid, La Ley, 2001.
- Barreiros Fernández, Francisco Javier, “El papel del notariado en el uso de la firma digital”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.
- Barriuso Ruiz, Carlos, *La contratación electrónica*, Madrid, Dykinson, 1998.
- Bauzá, Marcelo, “Firma electrónica y entidades certificadoras”, en Julio César Faira, comp., *Comercio electrónico. Análisis jurídico multidisciplinario*, Montevideo-Buenos Aires, B de F - Euros Editores SRL, 2003.
- Beltrán Sánchez, Emilio, *La unificación del derecho privado*, Madrid, Consejo General del Notariado, 1995.
- Bercovitz Rodríguez-Cano, Rodrigo, “La transposición de la Directiva Comunitaria al derecho español”, en Ubaldo Nieto Caro, comp., *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000.
- Bergel, Salvador Darío, “Informática y responsabilidad civil”, en Daniel R. Altmark, comp., *Informática y derecho. Aportes de doctrina internacional*, vol. II, Buenos Aires, Desalma, 1996.
- Berman, J. Harold, *La Formación de la tradición jurídica de Occidente*, México, Editorial Fondo de Cultura Económica, 1993.
- Betti, E., *Teoría general de las obligaciones*, Milano, Giuffrè, 1995.
- Blanch Domeque, Ma. Rosa, “La fe pública judicial en el sistema de firma electrónica. Autoridades de certificación”, en María del Carmen Bernal López, comp., *Jornadas sobre Actos de comunicación: Nuevas Tecnologías*, Madrid, 2001; en Estudios Jurídicos. Secretarios Judiciales, VI-2001, Madrid, S.A. de Fotocomposición, 2001.
- Bolás Alfonso, Juan, “Firma electrónica, comercio electrónico y fe pública Notarial”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.

- Bonardell Lenzano, Rafael, “La firma electrónica. Especial consideración de sus efectos jurídicos”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.
- Bonardell Lenzano, Rafael, “Los certificados de firma electrónica. Los prestadores de servicios de certificación”, en Susana García Santa Cecilia, comp., *Firma Electrónica*, Madrid, 2000; en Estudios Jurídicos. Secretarios Judiciales, IV-2000, Madrid, Solana e Hijos A.G., S.A., 2000.
- Bullard González, Alfredo, “La Asimetría de Información en la Contratación a propósito del Dolo Omisivo”, en Atilio Anibal Alterini; José Luís De Los Mozos; Carlos Alberto Soto, comp., *Contratación Contemporánea, Teoría General y principios*, Bogotá, Editorial Temis S.A., 2000.
- Calvo Caravaca, Alfonso Luís y Carrascosa González, Javier, “Problemas de extraterritorialidad en la contratación electrónica”, en A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001.
- Carbone Oyarzun, Carlos, *Contratos de adhesión*, Ed. Librería Jurídica, Buenos Aires, 1922.
- Carrascosa López, V. y otros, *La contratación informática: el nuevo horizonte contractual. Los contratos electrónicos e informáticos*, Granada, Comares, 1997.
- Casas Vallés, Ramón y otros, *Legislación de Internet y comercio electrónico*, Madrid, Tecnos, 2ª ed., 2003.
- Cebollero Valera, “Algunos aspectos del contrato de arquitecto. Los honorarios”, en *Revista de Derecho Privado*, 1985.
- Cervilla Garzón, María Dolores, *La Prestación de servicios profesionales*, Valencia, Tirant Lo Blanch, 2001.
- Clavería Gosálbez, L.H., *La causa del contrato*, Bolonia, 1998.
- Clemente Meoro, Mario E., “Responsabilidad de los prestadores de servicios de la sociedad de la información”, en M. Jesús Moro Almaraz, comp., *Autores, consumidores y comercio electrónico*, Madrid, Colex, 2004.
- Clemente Meoro, Mario E., “La protección del consumidor en los contratos electrónicos”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Comisión de las Comunidades Europeas, *Presentación del EDI (Electronic data Interchange) EUR 11883 ES.*, 1989.
- Corral García, Eduardo, “La buena fe en la formación y determinación del contenido del contrato: la oferta y la promesa al público”, en Santiago Espiau Espiau y Antoni Vaquer Aloy, comp., *Bases de un derecho contractual europeo. Bases of a european contract law*, Valencia, Tirant Lo Blanch, 2003.
- Correa, Carlos M. y otros, *Derecho Informático*, 1ª reimp., Buenos Aires, Depalma, 1994.
- Davara Rodríguez, Ángel, “Firma electrónica y autoridades de certificación: el notario electrónico”, en Juan José Martín-Casallo López, comp., *Problemática jurídica en torno al fenómeno de Internet*, Madrid, Consejo General del Poder Judicial, 2000.
- Davara Rodríguez, Miguel Ángel, *Comercio Electrónico*, Navarra, Aranzadi, 2004, 3º ed..
- Dávila Muro, Jorge y Morant Ramón, José Luís, “Servicios básicos de seguridad en la contratación electrónica”, en *Encuentros sobre Informática y Derecho. 1994-95*, Pamplona, Aranzadi, 1995.
- De Castro y Bravo, Federico, *El negocio jurídico*, Madrid, INEJ, 1967.
- De Castro y Bravo, Federico, *Las Condiciones Generales de los Contratos y la Eficacia de las Leyes*, Reimpresión de la 2da. Ed., Civitas, Madrid, 1987.
- De Castro y Bravo, Federico, *El negocio jurídico*, Madrid, 1985.

- De Cossío, A., *Instituciones de Derecho Civil*, Madrid, 1977.
- De Cuevillas Matozzi, Ignacio, “La perfección de la oferta en el comercio internacional (Principios de Unidroit: un análisis desde la órbita del derecho privado español)”, en Santiago Espiau Espiau y Antoni Vaquer Aloy, comp., *Bases de un derecho contractual europeo. Bases of a european contract law*, Valencia, Tirant Lo Blanch, 2003.
- De la Puente y Lavalle, Manuel, *El Contrato en General*, vol I, Palestra Editores, Lima, 2001.
- De la Puente y Lavalle, Manuel, “Las cláusulas generales de contratación y la protección al consumidor”, en Carlos Alberto Soto Coaguila y Roxana Jiménez Vargas-Machuca, comp., *Contratación Privada*, Lima, Jurista, 2002.
- De la Torre Saavedra, Enrique, García Villaverde, Rafael, y otros, *Contratos Bancarios*, Madrid, Civitas, 1992.
- De Los Mozos, José Luís, *El Principio de la buena fe (sus aplicaciones prácticas en el Derecho Civil Español)*, Barcelona, Bosch, 1965.
- De Prada Guaita, Vicente, “Nuevos campos que abre la informática a la función notarial”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.
- De Quinto Zumárraga, Francisco, *La firma electrónica. Marco legal y aplicaciones prácticas*, Barcelona, Grupo Difusión, 2004.
- Del Toro Huerta, Mauricio Iván, “El fenómeno del *soft law* y las nuevas perspectivas del Derecho Internacional”, *Anuario Mexicano de Derecho Internacional*, vol. VI, México, UNAM, 2006.
- Desantes Real, Manuel, “La Directiva sobre el Comercio Electrónico. Mercado interior y servicios financieros de la sociedad de la información”, en Rafael Mateu de Ros y Juan Manuel Cendoya Méndez de Vigo, comp., *Derecho de Internet. Contratación electrónica y firma digital*, Navarra, Aranzadi, 2001.
- Devoto, Mauricio, *Comercio electrónico y firma digital. La regulación del ciberespacio y las estrategias globales*, Buenos Aires, La Ley, 2001.
- Díaz Fraile, Juan María, “Aspectos jurídicos más relevantes de la Directiva y del proyecto de Ley español de Comercio Electrónico”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Díez-Picazo, Luis y Gullón Ballesteros, Antonio, *Sistema de Derecho Civil*, vol. II, Madrid, Tecnos, 7ª ed., 1995.
- Díez-Picazo, Luís, “Prólogo” en: Franz Wieacker, *El Principio General de Buena Fe*, (trad. De José Luís Carro), Madrid, Civitas, 1982.
- Díez-Picazo, Luís, *Fundamentos del Derecho Civil Patrimonial*, vol. I y II, Madrid, Civitas, 1996, 5ª ed..
- Domínguez Gragera, María Luisa, “Normativa aplicable a la firma electrónica (Directiva 99/93/CE y Real Decreto-Ley 14/1999)”, en Javier Cremades y otros, comp., *Régimen Jurídico de Internet*, Madrid, La Ley, 2002.
- Domínguez Luelmo, Andrés, “La contratación electrónica y la defensa del consumidor”, en Joseba A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001.
- Dotzauer Strampfer, Erwin, *Aspectos Jurídicos y Tecnológicos del Comercio, Firmas y Documentos Electrónicos. Estudio del Proyecto de Ley boliviano*; Santa Cruz, El País, 2009.
- Duque Domínguez, Justino F., “Las cláusulas abusivas en contratos de consumo”, en Ubaldo Nieto Caro, comp., *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000.

- Eckl, Christian, “Algunas observaciones alemanas acerca de la buena fe en el derecho contractual español: el principio general del derecho a cláusula general”, en Santiago Espiau Espiau y Antoni Vaquer Aloy, comp., *Bases de un derecho contractual europeo. Bases of a european contract law*, Valencia, Tirant Lo Blanch, 2003.
- Echebarría Sáenz, Joseba Aitor, “El comercio electrónico entre empresarios”, en Josefa A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001.
- Ennecerus, L., *Tratado de Derecho Civil*, vol. II, Barcelona, 2ª ed., 1959.
- Espín Canovas, D., *Manual de Derecho Civil Español*, Madrid, Revista de Derecho Privado, 5ª ed., 1978.
- Fajardo Fernández, J., *Derecho privado Europeo*, S. Cámara Lapuente (coord.), AAVV, Madrid, 2003.
- Fernández Costales, *El contrato del arquitecto en la edificación*, Madrid, 1977.
- Fernández Delpech, Horacio, *Internet: su problemática jurídica*, Buenos Aires, Abeledo Perrot, 2000.
- Fernández Domingo, Jesús Ignacio, “Algunas notas acerca de la contratación y el comercio electrónico”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Fernández Fernández, Ma. Cristina, “La firma electrónica avanzada en el derecho europeo”, en Santiago Espiau Espiau y Antoni Vaquer Aloy, comp., *Bases de un derecho contractual europeo. Bases of a european contract law*, Valencia, Tirant Lo Blanch, 2003.
- Ferrer Gomila, Josep Lluís, “Aspectos científicos de la firma digital”, en Susana García Santa Cecilia, comp., *Firma Electrónica*, Madrid, 2000; en Estudios Jurídicos. Secretarios Judiciales, IV-2000, Madrid, Solana e Hijos A.G., S.A., 2000.
- Fortunato Garrido, Roque y Sago, Jorge Alberto, *Contratos civiles y comerciales*, vol. I y II, Buenos Aires, Editorial Universidad, 2ª ed., 1998.
- Franzoni, Massimo, “La responsabilidad en las obligaciones de medios y en las obligaciones de resultado”, en Guido Alpa y otros, comp., *Estudios sobre la Responsabilidad Civil*, Lima, ARA Editores, 2001.
- Frossard, “La distinction des obligations de moyens et des obligations de résultat”, París, 1965, citado por Belén Trigo García, *Contrato de servicios. Perspectiva jurídica actual*, Granada, COMARES, 1999.
- Gaete González, Eugenio Alberto, *Instrumento Público Electrónico*, Barcelona, Bosch, 2000.
- Galgano, Francesco, *El negocio Jurídico*, Trad. Española F. Blasco Gasco y Lorenzo Prats Albentosa, Valencia, 1992.
- Galvez Montes, J., “Colegios profesionales y tarifas de honorarios de ingenieros”, en *Revista de Administración Pública*, 1983.
- Gallardo Ortiz, Miguel Ángel, “Garantías criptológicas de las firmas electrónicas”, en *Actualidad Informática Arazandi*, N° 6, 1993.
- García Amigo M., *Teoría general de las obligaciones y contratos, Lecciones de Derecho civil II*, Madrid, 1995.
- García Cantero, Gabriel, *La Traducción Española de la Parte General del Código Europeo de Contratos*, Bogotá, Ediciones Academia Colombiana de Jurisprudencia, 1ª ed., 2004.
- García-Cruces, J.A., *El contrato de factoring*, Madrid, Tecnos, 1990.
- García de Haro de Coytisolo, Ramón, en Ludovico Barassi, *Instituciones de derecho civil*, vol. II, Traducción y notas de comparación al derecho español por Ramón García de Haro de Coytisolo con la colaboración de Mario Falcón Carreras, Barcelona, 1955.

- García Del Poyo, Rafael, “Aspectos mercantiles y fiscales del e-business”, en Joseba A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001.
- García Iglesias, Demetrio, “El contrato de obra: concepto y contenido. Los riesgos y la responsabilidad según la doctrina del Tribunal Supremo”, *La Ley*, 1993-4.
- García Más, Francisco Javier, “Análisis de la proposición de Directiva del Parlamento Europeo y del Consejo 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 Comercio Electrónico)”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.
- García Más, Francisco Javier, “La contratación electrónica: la firma y el documento electrónico”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.
- García Más, Francisco Javier, “La contratación electrónica: la firma y el documento electrónico”, en *RCDI*, N° 65, 1999.
- García Más, Francisco Javier, “La firma electrónica: Directiva 1999/93/CE, de 13 de diciembre de 1999 y Real Decreto-Ley 14/1999 de 17 de septiembre”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.
- García Rubio, María Paz, “Bases de datos y confidencialidad en Internet”, en Joseba A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001.
- García Valdecasas, Guillermo, “La esencia del mandato”, en *Revista de Derecho Privado*, 1944.
- García Villaverde, Rafael y otros, *El contrato de factoring*, Madrid, McGraw Hill, 1999.
- Garrigues Díaz-Cañabate, J., *Contratos bancarios*, Madrid, 2ª ed., 1975.
- Garrigues, Joaquín, *Curso de Derecho Mercantil*, vol. II, Imprenta Silverio Aguirre Torre, Madrid, 1962.
- Garrigues, Joaquín., *Curso de Derecho Mercantil (revisión de Sánchez Calero)*, Madrid, 8ª ed., 1983.
- Gete-Alonso y Calera, Mª. C., *Estructura y función del tipo contractual*, Barcelona, 1979.
- Giannantonio, Ettore, *Valor jurídico del documento electrónico; Informática y Derecho. Aportes de la Doctrina Internacional*, t. I, Buenos Aires, Depalma, 1987.
- Giner Parreño, César A., *El contrato de inspección en el comercio internacional*, Valencia, Tirant Lo Blanch, 1998.
- Gómez Díez, José Luís, “Contratación electrónica”, en Cuerpo de Secretarios Judiciales, comp., *Derecho e Informática*, Madrid, 2001; en Estudios Jurídicos, V-2001, Madrid, Imprenta Nacional del Boletín Oficial del Estado, 2001.
- González Aguilar, Audilio y otros, *Los contratos en la sociedad de la información*, Madrid, COMARES, 2004.
- González-Echenique, Leopoldo, “Estudio de la Directiva y del Real Decreto-ley de 17 de septiembre de 1999 sobre firma electrónica”, en Rafael Mateu de Ros y Juan Manuel Cendoya Méndez de Vigo, comp., *Derecho de Internet. Contratación electrónica y firma digital*, Navarra, Aranzadi, 2001.
- Gracia Santiago, Héctor José, “Seguridad en el Comercio Electrónico”, Tesis de Grado, Álvaro Andrés Motta, dir., Bogotá, Pontificia Universidad Javeriana - Facultad de Derecho, 2004.
- Grimalt Servera, Pedro, “La contratación en masa en Internet: el consentimiento de los consumidores para el tratamiento de sus datos en una condición general”, en M. Jesús Moro Almaraz, comp., *Autores, consumidores y comercio electrónico*, Madrid, Colex, 2004.

- Gullón Ballesteros, Antonio, *Curso de derecho civil. Contratos en especial. Responsabilidad extracontractual*, Madrid, 1972.
- Gutiérrez Camacho, Walter, “Los contratos atípicos”, en Atilio Anibal Alterini y otros, comp., *Contratación Contemporánea. Contratación electrónica y tutela del consumidor*, Lima-Bogotá, Palestra-Temis, 2001.
- Hance, Olivier, *Leyes y negocios en Internet*, México, McGraw-Hill, 1996.
- Herrera Millar, Karina M., “Comunicación y Desarrollo en la Sociedad de la Información, Contextos discursivos neodesarrollistas y tecnoinformacionales”, en Erick R. Torrico, comp., *Comunicación, Nuevos Escenarios y Conflictos Sociales*, La Paz, EDOBOL, 2005.
- Huerta Viesca, Ma. Isabel y Rodríguez Ruiz de Villa, Daniel, *Los prestadores de servicios de certificación en la contratación electrónica*, Navarra, Aranzadi, 2001.
- Illescas Ortiz, Rafael, *Derecho de la contratación electrónica*, Madrid, Civitas, 2001.
- Instituto Internacional para la Unificación del Derecho Privado (UNIDROIT), *Principios sobre los Contratos Comerciales internacionales*, Roma, 2004.
- Ihering, R., *El fin en el derecho*, T. I, 3ª Ed., 1893, p.VIII.
- Jordano Barea, J., *Los contratos atípicos*, RGLJ, 1953.
- Josserand, *Derecho Civil*, vol. I, Buenos Aires, 1950.
- Julià Barceló, Rosa, *Comercio electrónico entre empresarios. La formación y prueba del contrato electrónico (EDI)*, Valencia, Tirant Lo Blanch, 2000.
- Kaune Arteaga, Walter, *Teoría general de los contratos*, 4ª ed., La Paz, Temis, 1996.
- Lacruz Berdejo, J.L., *Elementos de Derecho Civil*, vol. II, Barcelona, 2ª ed., 1987.
- Lacruz Berdejo, J.L. y otros, *Elementos de derecho Civil II. Derecho de obligaciones. Vol. I. Parte general. Teoría general del contrato*, (revisada y puesta al día por F. Rivero Hernández), Madrid, 2000.
- Lalaguna Domínguez, Enrique, *El contrato. Estructura, formación y eficacia*, Valencia, Tirant Lo Blanch, 1997.
- Larenz, K., *Derecho de obligaciones*, vol. II, versión española y notas de J. Santos Briz, Madrid, 1959.
- Larroumet, Christian, *Responsabilidad Civil Contractual*, Santiago, Jurídica de Chile, 1998.
- Lasarte Álvarez, Carlos, *Principios de Derecho Civil, vol. III, Contratos*, 3ª ed., Madrid, 1995.
- Llaneza González, P., “LSSI: día cero”, *Noticias Jurídicas*, Madrid, Bosch, oct.-nov./2002.
- López Martínez de Septién, Óscar, “Aspectos jurídicos de la firma electrónica: anteproyecto del real Decreto-ley sobre firma electrónica”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.
- López Santamaría, Jorge, *Los Contratos, parte general*, vol. I, 3ª ed., Santiago, Editorial Jurídica de Chile, 1998.
- López y López, Ángel y otros, *Derecho Civil. Derecho de obligaciones y contratos*, Valencia, Tirant Lo Blanch, 4ª ed., 2001.
- López y López, Ángel M., “Conversaciones con difuntos. Luigi Caiani: analogía”, *Quaderni Fiorentini per la storia del pensiero giuridico moderno*, XXIX, 2000.

- López y López, Ángel M., “Comentarios al Código Civil y Compilaciones forales. Tomo XVII. Volumen 2º. Artículos 1281 a 1314”, Madrid, Editoriales de Derecho Reunidas, 1981.
- Lorenzetti, Ricardo L., *Comercio electrónico*, Buenos Aires, Abeledo Perrot, 2001.
- Lorenzetti, Ricardo Luís, *Esquema de una teoría Sistemática del Contrato*, en Atilio Anibal Alterini; José Luís De Los Mozos; Carlos Alberto Soto, comp., *Contratación Contemporánea, Teoría General y principios, La Convención de las Naciones Unidas Sobre los Contratos de Compraventa Internacional de Mercaderías*, Bogotá, Editorial Temis S.A., 2000.
- Llodrà Grimalt, Francisca, *El contrato celebrado bajo condiciones generales*, Valencia, Tirant Lo Blanch, 2002.
- Madrid Parra, Agustín, “Seguridad en el comercio electrónico”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Madrid Parra, Agustín, “Tramitación y contenido de la Ley Modelo de la CNUDMI/UNCITRAL sobre las firmas electrónicas”, en Universidad Externado de Colombia, comp., Departamento de Derecho de los Negocios, *El contrato por medios electrónicos*, Bogotá, Universidad Externado de Colombia, 2003.
- Maestre, Javier A., “Análisis de la Directiva de comercio electrónico y del anteproyecto español de Ley de servicios de la sociedad de la información (LSSI)”, en Javier Cremades y otros, comp., *Régimen Jurídico de Internet*, Madrid, La Ley, 2002.
- Maluquer De Motes Bernet, Carlos J., “Los códigos de conducta como fuente del Derecho”, *Derecho Privado y Constitución*, nº17, enero-diciembre 2003.
- Marín López, Juan José, “El ámbito de aplicación de la ley sobre Condiciones Generales de la Contratación”, en Ubaldo Nieto Caro, comp., *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000.
- Martín-Ballester, L., “De la causa en los negocios jurídicos contractuales”, RGLJ, 1956.
- Martín Pérez, José Antonio, “El ámbito de aplicación subjetivo del régimen de las condiciones generales (Sobre la necesidad de protección de los adherentes-profesionales)”, en Santiago Espiau Espiau y Antoni Vaquer Aloy, comp., *Bases de un derecho contractual europeo. Bases of a european contract law*, Valencia, Tirant Lo Blanch, 2003.
- Martín-Casallo López, Juan José, “La protección de los datos personales: aspectos penales de la cesión de datos”, en Juan José Martín-Casallo López, comp., *Problemática jurídica en torno al fenómeno de Internet*, Madrid, Consejo General del Poder Judicial, 2000.
- Martínez Nadal, Apol-Lònia, “Las fuentes normativas de la firma electrónica”, en Susana García Santa Cecilia, comp., *Firma Electrónica*, Madrid, 2000; en Estudios Jurídicos. Secretarios Judiciales, IV-2000, Madrid, Solana e Hijos A.G., S.A., 2000.
- Martínez Nadal, Apol-Lònia, “Problemática jurídica de los certificados de atributos en el comercio electrónico. En especial, su discordancia con el registro mercantil. Propuestas de solución”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Martínez Nadal, Apol-Lònia, *Comentarios a la Ley 59/2003 de firma electrónica*, Madrid, Civitas, 2004.
- Martínez Nadal, Apol-Lònia, *Comercio electrónico, firma digital y autoridades de certificación*, Madrid, 3ª ed., Civitas, 2001.
- Martínez Nadal, Apol-Lònia, *Comercio electrónico, firma digital y autoridades de certificación*, Estudios de Derecho Mercantil, Madrid, Civitas, 2ª ed., 2000.
- Martínez Nadal, Apol-Lònia, *La ley de firma electrónica*, Madrid, Civitas, 2000.

- Masuda., Yoneji, *La Sociedad Informatizada como Sociedad Post-Industrial*, Madrid, Fundesco Tecnos, 1984.
- Mata Martín, Ricardo, “Algunos aspectos de la delincuencia patrimonial en el comercio electrónico”, en Joseba A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001.
- Méndez, Rosa M., y Vilalta, A. Esther, *Obligaciones y responsabilidades de los prestadores de servicios de la sociedad de la información*, Barcelona, Bosch, 2003.
- Menéndez, Aurelio, Díez-Picazo, Luis y otros, *Comentarios a la Ley sobre Condiciones Generales de la Contratación*, Madrid, Civitas, 2002.
- Messineo, Francesco, *Doctrina General del Contrato*, vol. I, Buenos Aires, Ediciones jurídicas Europa-América, 1986.
- Miranda Serrano, Luis María , *La aplicación en el derecho español no uniforme de la noción de oferta de contrato de la Convención de las Naciones Unidas sobre la Compra Venta Internacional de Mercaderías: en torno a las ofertas a personas indeterminadas*, Proyecto de Investigación Veinticinco años de Derecho de los consumidores: análisis legal y propuestas de modernización (referencia DER 2010-16204), financiado por el Ministerio de Ciencia e Innovación (IP: Prof. Dr. Luis María Miranda Serrano), Madrid, 2010.
- Molina Mateos, José María, “Libertad informática y criptología”, en *Informática y Derecho*, N° 12-15, 2000.
- Monateri Giuseppe, Pier, “Hipótesis sobre la responsabilidad civil de nuestro tiempo”, en Guido Alpa y otros, comp., *Estudios sobre la Responsabilidad Civil*, Lima, ARA Editores, 2001.
- Moro Almaraz, M. Jesús, “Servicios de la sociedad de la información y sujetos intervinientes”, en M. Jesús Moro Almaraz, comp., *Autores, consumidores y comercio electrónico*, Madrid, Colex, 2004.
- Moro Almaraz, M. Jesús, “Servicios de la sociedad de la información y sujetos intervinientes”, en M. Jesús Moro Almaraz, comp., *Autores, consumidores y comercio electrónico*, Madrid, Colex, 2004.
- Nieto Carol, Ubaldo, y otros, *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000.
- O’Callaghan Muñoz, Xavier y otros, *Contratos de adhesión y derechos de los consumidores*, Madrid, Consejo General del Poder Judicial, 1993.
- O’Callaghan Muñoz, Xavier, *Código Civil comentado y con jurisprudencia*, Madrid, 2ª ed., La Ley, 2001.
- O’Callaghan Muñoz, Xavier, y otros, *Contratos de adhesión y derechos de los consumidores*, Madrid, Mateu Cromo S.A., 1993.
- Oliver Cuello, Rafael, *Tributación del comercio electrónico*, Valencia, Tirant Lo Blanch , 1999.
- Orduña Moreno, Francisco Javier, “Derecho de la contratación y condiciones generales”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Orduña Moreno, Francisco Javier, Tomillo Urbina, Jorge L., y otros, *Contratación Bancaria*, vol. I, Valencia, Tirant Lo Blanch, 2001.
- Ortega Díaz, Juan Francisco, “Firma digital y tráfico económico. La Importancia del contrato de certificación digital”, en M. Jesús Moro Almaraz, comp., *Autores, consumidores y comercio electrónico*, Madrid, Colex, 2004.
- Ortega Díaz, Juan Francisco, *La Firma y el Contrato de Certificación Electrónicos*, Navarra, Aranzadi, 2008.
- Oviedo Albán, Jorge, *Consideraciones Sobre la Formación del Contrato en el Código de Comercio Colombiano*, Lima, Publicado en: Revista Jurídica del Perú, Año LIII, N° 50, Septiembre de 2003.

- Pachionni, Giovanni, *Los contratos a favor de tercero. Estudio de Derecho romano, civil y mercantil*, Traducción de la última edición italiana por Francisco Javier Osset, Madrid, Editorial Revista de Derecho Privado, 1948.
- Pagador López, Javier, “Requisitos de incorporación de las Condiciones Generales y consecuencias negociales”, en Ubaldo Nieto Caro, comp., *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000.
- Palacios González, Ma. Dolores, “El deber de información en los contratos con consumidores”, en Santiago Espiau Espiau y Antoni Vaquer Aloy, comp., *Bases de un derecho contractual europeo. Bases of a european contract law*, Valencia, Tirant Lo Blanch, 2003.
- Palao Moreno, Guillermo, Prats Albentosa, Lorenzo y otros, *Derecho patrimonial europeo*, Navarra, Aranzadi, 2003.
- Pardini, Anibal A., *Derecho de Internet*, Buenos Aires, La Roca, 2002.
- Peña Valenzuela, Daniel, “Responsabilidad y comercio electrónico. Notas sobre el daños y el riesgo en la sociedad de la información”, en Universidad Externado de Colombia, comp., Departamento de Derecho de los Negocios, *El contrato por medios electrónicos*, Bogotá, Universidad Externado de Colombia, 2003.
- Peña, Puig, *Compendio de derecho civil español*, t. IV, vol. II, 3ª ed., Madrid, 1976.
- Perales Viscasillas, P., *La formación del contrato de compraventa internacional de mercaderías*, Valencia, Tirant Lo Blanch, 1996.
- Pérez Gil, Julio, “Documento informático y firma electrónica: aspectos probatorios”, en Josefa A. Echebarría Sáenz, comp., *El comercio electrónico*, Madrid, Edisofer S.L., 2001.
- Pérez Luño, Antonio Enrique, *Manual de Informática y Derecho*, Barcelona, Ariel, 1996.
- Pérez Pereira, María, “Régimen jurídico del prestador de servicios de certificación”, en Javier Cremares y otros, comp., *Régimen jurídico de Internet*, Madrid, La Ley, 2002, 1ª ed..
- Pérez Pereira, María, *Firma electrónica: Contratos y Responsabilidad Civil*, Navarra, Aranzadi, 2009.
- Plaza Penadés, Javier, “Contratación electrónica y pago electrónico (En el Derecho nacional e internacional)”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Plaza Penadés, Javier, “La firma electrónica y su regulación en el derecho español”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Plaza Penadés, Javier, “La firma electrónica y su regulación en la Directiva 1999/93 de la Unión Europea”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Plaza Penadés, Javier, “La responsabilidad civil de los intermediarios en Internet y otras redes (Su regulación en el Derecho comunitario y en la LSSICE)”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Plaza Penadés, Javier, “Los principales aspectos de la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Prats Albentosa, Lorenzo, *Préstamo de consumo, Crédito al consumo*, Valencia, Tirant Lo Blanch, 2001.
- Puig Brutau, José, *Fundamentos de Derecho Civil*, t.II, vol.II, *Contratos en particular*, Barcelona, 1982.

- Puig Brutau, José, *Fundamentos de Derecho Civil*, vol. I, Barcelona, Bosch, 1978.
- 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.
- Rene David, *Les Grands Systèmes de Droit Contemporains (Droit compare)*, Paris, Libraire Dalloz, 1964.
- Requejo Isidro, Marta, “Contratación electrónica internacional: Derecho aplicable”, en M. Jesús Moro Almaraz, comp., *Autores, consumidores y comercio electrónico*, Madrid, Colex, 2004.
- Rezzónico, Juan Carlos, *Contratos con Cláusulas Predispuestas. Condiciones Negociales Generales*, Astrea, Buenos Aires, 1991.
- Ribagorda Garnacho, Arturo, “Sistema de certificación: la firma y el certificado digital”, en Javier Cremades y otros, comp., *Régimen Jurídico de Internet*, Madrid, La Ley, 2002.
- Ribas Alejandro, Javier, *Aspectos jurídicos del comercio electrónico en Internet*, Pamplona, Arazandi, 1999.
- Ribas Alejandro, Javier, “Comercio electrónico en Internet”, en Juan José Martín-Casallo López, comp., *Problemática jurídica en torno al fenómeno de Internet*, Madrid, Consejo General del Poder Judicial, 2000.
- Roca Guillamón, Juan, “Reglas de interpretación de las Condiciones Generales de los contratos”, en Ubaldo Nieto Caro, comp., *Condiciones Generales de la Contratación y cláusulas abusivas*, Valladolid, Lex Nova, 2000.
- Roca Trias, Encarna, “Naturaleza de la relación entre el arquitecto y los clientes. Responsabilidad extracontractual de los arquitectos”, en *Revista de Derecho Privado*, 1976.
- Rodríguez Adrados, Antonio, “El documento negocial informático”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.
- Rodríguez Adrados, Antonio, “La firma electrónica”, en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.
- Rodríguez Azuero, Sergio, *Contratos Bancarios, su significación en América latina*, Bogotá, Legis, 5ª ed., 2003.
- Rodríguez Delgado, Martha y otros, Informe sobre el grado de desarrollo de la Sociedad de la Información, Declaración Política y Plan de Acción que integre Sur América, Centro América y el Caribe, en UNESCO, comp., Bogotá, 2003.
- Rodríguez González, José Ignacio, *El Principio de Relatividad de los contratos en el derecho español*, Madrid, Colex, 2000.
- Rollano Burgoa, Marcelo Harold, “Fundamentos para un régimen jurídico especial para las transferencias electrónicas de fondos”, Cochabamba, Universidad Católica Boliviana, 2001.
- Ruiz López, Emilio José, “Contratación bancaria electrónica a través de internet”, en Francisco Javier Orduña Moreno, comp., *Contratación y Comercio Electrónico*, Valencia, Tirant Lo Blanch, 2003.
- Ruiz Muñoz, M., *La nulidad parcial del contrato y la defensa de los consumidores*, Valladolid, Lex Nova, 1993.
- Sancho Rebullida, F., *Notas sobre la causa de la obligación en el Código Civil*, RGLJ, 1971.
- Santamaria, J., *Comentarios al Código Civil*, Madrid, 1958.
- Santos Briz, Jaime, *Los contratos civiles. Nuevas perspectivas*, Granada, COMARES, 1992.

- Santos Briz, Manuel, "El contrato de ejecución de obra y su problemática jurídica" en *Revista de Derecho Privado*, 1972.
- Schneider, Gary P., *Comercio electrónico*, México, Internacional Thomson Editores, 3ª ed., 2003.
- Segaller, Stephen, *Nerds 2.0.1. A Brief History of the Internet*, New Cork, TvBooks Inc., ISBN 9781575000886, 1999.
- Serra Rodríguez, Adela, *Cláusulas abusivas en la contratación*, Navarra, Aranzadi, 2002.
- Silva-Ruiz, Pedro F., "Contratos de adhesión, condiciones contractuales generales. (Condiciones generales de los contratos o de la contratación y las cláusulas abusivas)", en Atilio Aníbal Alterini y otros, comp., *Contratación Contemporánea. Contratación electrónica y tutela del consumidor*, Lima-Bogotá, Palestra-Temis, 2001.
- Silva Ruiz, Pedro F., "Contratos de adhesión, condiciones contractuales generales (condiciones generales de los contratos o de la contratación) y las cláusulas abusivas", en Atilio Aníbal Alterini, José Luis De los Mozos y Carlos Alberto Soto Coaguila, comp., *Instituciones de Derecho Privado. Contratación contemporánea. Teoría General y Principios*, Bogotá, Themis, 2001.
- Silva-Ruiz, Pedro F., "Las condiciones generales y su control en el derecho contractual comparado", en Santiago Espiau Espiau y Antoni Vaquer Aloy, comp., *Bases de un derecho contractual europeo. Bases of a european contract law*, Valencia, Tirant Lo Blanch, 2003.
- Simó Sevilla, Diego, "Las nuevas modalidades de prestación del consentimiento: la función notarial ante las nuevas tecnologías en su valor jurídico", en Consejo General del Notariado, comp., *Notariado y contratación electrónica*, Madrid, Visor Fotocomposición, 2000.
- Sole Resina, Judith, *Arrendamiento de obras o servicios. Perfil evolutivo y jurisprudencial*, Valencia, Tirant Lo Blanch, 1997.
- Soto Coahuila, Carlos Alberto, "Las cláusulas generales de contratación y las cláusulas abusivas en los contratos predispuestos", en *Revista Universitas*, Bogotá, Pontificia Universidad Javeriana, Facultad de Ciencias Jurídicas, N° 106, 2003.
- Study Group on a European Civil Code, y Research Group on EC Private Law (Acquis Group), *Principles, Definitions and Model Rules of European Private Law. Draft Common Frame of Reference (DCFR). Full Edition*, Christian von Bar y Eric Clive (Editores), Sellier - European Law Publishers, Munich, 2009.
- Tapscott, Donald, *Economía Digital. Promessa e Perigo na era da inteligencia em rede*, Sao Paulo, Makron Books do Brasil Editoria Limitada, 1997.
- Thurrow, Lester, *Construir Riqueza*, Vergara Business, Javier Vergara Editor, Grupo Z, Ediciones B Argentina SA, 2000.
- Tintó Gimbernat, Montserrat, "La criptografía asimétrica o de clave pública: la firma digital y el cifrado. Los certificados digitales y las autoridades de certificación. Aspectos técnicos y jurídicos", en *Estudios Jurídicos: Secretarios Judiciales*, No. VI-2001, Madrid, Sociedad Anónima de Fotocomposición, 2001.
- Trigo García, Belén, *Contrato de servicios. Perspectiva jurídica actual*, Granada, COMARES, 1999.
- Tomasello Hart, Leslie, *La Contratación. Contratación Tipo, de Adhesión y Dirigida. Autocontratación y Subcontratación*, Edeval, Valparaíso-Chile, 1984.
- Umaña Chaux, Andrés Felipe, "Entidades de certificación: una aproximación a su régimen de responsabilidad.", en Universidad de los Andes, Grupo de Estudios en Internet, Comercio Electrónico & Telecomunicaciones e Informática, *Derecho de Internet y telecomunicaciones*, Bogotá, Legis, 2003.

- UNIDROIT, *Principios Sobre los Contratos Comerciales Internacionales*, obra publicada por el Ministerio de Justicia y del Derecho, de la República de Colombia, en desarrollo del Plan de Armonización del Derecho Internacional Privado -PADIP-, Bogotá, 1997.
- Valpuesta Frenández, Rosario, “Elementos esenciales del contrato”, en *Derecho Civil. Derecho de Obligaciones y contratos*”, A. López y López, V.L. Montés Penades, E. Roca I Trias (directores), AAVV, Valencia, 2001.
- Vallespinos, Carlos Gustavo, *El Contrato por Adhesión a Cláusulas Generales*, Ed. Universidad, Buenos Aires-Argentina, 1984.
- Vaquero Pinto, María José, *El arrendamiento de servicios. Propuesta de modelo general para la contratación de servicios*, Granada, Comares, 2005.
- Vattier Fuanzalida, Carlos, *Responsabilidad contractual y extracontractual en el comercio electrónico*, RCE, N° 18, Madrid, 2001.
- Vattier Fuenzalida, Carlos, “Responsabilidad contractual y extra contractual en el comercio electrónico”, en Javier Cremares y otros, comp., *Régimen jurídico de Internet*, Madrid, La Ley, 1ª ed., 2002.
- Vázquez Ferreira, Roberto A., “Las obligaciones emergentes del contrato y la tutela del consumidor: las prestaciones propias de cada producto o servicios”, en Atilio Aníbal Alterini y otros, comp., *Contratación Contemporánea. Contratación electrónica y tutela del consumidor*, Lima-Bogotá, Palestra-Temis, 2001.
- Vega Vega, José Antonio, *El contrato de permuta financiera*, Navarra, Arazandi, 2002.
- Viguri Perea, Agustín, “Análisis del derecho comparado de la culpa in contrahendo”, en Santiago Espiau Espiau y Antoni Vaquer Aloy, comp., *Bases de un derecho contractual europeo. Bases of a european contract law*, Valencia, Tirant Lo Blanch, 2003.
- Vilches Trassiera, Antonio José, *Aproximación a la Sociedad de la Información: firma, comercio y banca electrónica*, Mancha Real, 2ª ed., Fundación Beneficentia et Peritia Iuris, 2002.
- Villanueva Lupión, Carmen, *El Servicio como objeto de tráfico jurídico*, Madrid, La Ley, 2009.
- Villanueva Lupión, Carmen, *Los contratos de servicios*, Madrid, La Ley, 2009.
- Villar Uríbarri, José Manuel, “El régimen jurídico de los prestadores de servicios de la sociedad de la información”, en José Manuel Villar Uríbarri, comp., *La nueva regulación de las telecomunicaciones, la televisión e Internet*, Navarra, Aranzadi, 2003.
- Visintini, G., *La reticenza nella formazione dei contratti*, Padova, 1972.
- Weingarten, Celia y otros, *Instituciones de derecho privado*, Buenos Aires, Editorial Universidad, 2003.
- Yzquierdo Tolsada, Mariano, *Sistema de responsabilidad civil, contractual y extracontractual*, Madrid, Dykinson, 2001.
- Zavala Romero, Luis, *Derecho de los Contratos en el Código Civil Peruano de 1984*, Fecal, Lima, 2002.

Normativa española

Código Civil español, aprobado por R.D. del 24 de julio de 1.889

Código de Comercio español, de 1885.

Ley 26/1984, de 19 de julio, general para la defensa de los consumidores y usuarios.

Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Ley 59/2003, de 19 de diciembre, de firma electrónica.

Ley 7/1998, de 13 de abril, sobre condiciones generales de la contratación.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

Normativa comunitaria europea

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.

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 2006/123/CE del Parlamento Europeo y del Consejo de 12 de diciembre de 2006 relativa a los servicios en el mercado interior.

Directiva 93/13/CEE del Consejo de 5 de abril de 1993 sobre las cláusulas abusivas en los contratos celebrados con consumidores.

Directiva 95/46/EC y 97/66/CE del Parlamento y del Consejo 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.

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.

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.

Normativa internacional

Instituto para la Unificación del Derecho Privado, *Principios UNIDROIT sobre Contratos Comerciales Internacionales*, 1994.

Organización de Naciones Unidas, *Convención sobre Compraventa Internacional de Mercaderías*, Viena, 1980.

Organización de Naciones Unidas, *Ley Modelo de la CNUDMI sobre Comercio Electrónico con la Guía para su incorporación al derecho interno*, Nueva York, CNUDMI, 1999.

Organización de Naciones Unidas, *Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno*, Nueva York, CNUDMI, 2002.

Jurisprudencia española

STS de 4 de febrero de 1950 (RAJ 191).

STS de 10 de junio de 1975 (RAJ 3265).

STS de 26 de abril de 2005.

Obras electrónicas consultadas

- Aguirre, Carlos Dionisio, “El Desarrollo desde la perspectiva de la defensa del consumidor electrónico - el papel del conocimiento y la contratación”, en *REDI: Revista Electrónica de Derecho Informático*, No. 87, Argentina, Alfa-Redi, octubre/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=3492>
- Ahón Iriarte, Erick, “Firma Digital y el Certificado Digital. El Proyecto Peruano”, en *REDI: Revista Electrónica de Derecho Informático*, No. 14, Perú, Alfa-Redi, septiembre/1999, disponible en: <http://publicaciones.derecho.org/redi/No. 14 - Septiembre de 1999/9>
- Alamillo, Ignacio, “Confianza digital basada en certificados”, en *REDI: Revista Electrónica de Derecho Informático*, No. 13, España, Alfa-Redi, agosto/1999, disponible en: <http://www.alfa-redi.com/rdi-articulo.shtml?x=315>
- Alcaraz Carsi, Juan Ignacio, “Breve comentario sobre la notificación del acuse de recibo del prestador de servicios de la Sociedad de la Información”, en *REDI: Revista Electrónica de Derecho Informático*, No. 21, España, Alfa-Redi, abril/2000, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=448>
- Barzallo, José Luís, “El gobierno electrónico en el Ecuador”, en *REDI: Revista Electrónica de Derecho Informático*, No. 95, Quito, Alfa-Redi, junio/2006, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=6204>
- CAMERFIRMA S.A., *Declaración de Prácticas y Políticas de Certificación*, Madrid, 2007, disponibles en: <http://policy.camerfirma.com>
- Campillos González, Gema Ma., “*El comercio electrónico en el marco jurídico de la Sociedad de la Información*”, Ministerio de Ciencia y Tecnología, Madrid, disponible en <http://www.ieid.org/congreso/ponencias/Campillos,%20Gema.pdf>
- Canut, Pedro, “El Secreto Profesional del Abogado ante la Ley Orgánica de Protección de Datos de Carácter Personal”, en *REDI: Revista Electrónica de Derecho Informático*, No. 90, España, Alfa-Redi, enero/2006, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=4226>
- Corcobado Cartes, T., “*Donde el aire da la vuelta: Sociedad de la Información y exclusión social. El papel de la educación*”, Universidad de Extremadura., 1998, en <http://www.launion.edu.pe/info99-4.htm>
- Comisión de la Sociedad de la Información del Ministerio de Ciencias de Portugal, *Libro Verde*, Aprobado por el Consejo de Ministros de Portugal, 1997, ubicado en <http://www.missao-si.mct.pt/>.
- Comunicación de 8 de diciembre de 1999, relativa a una iniciativa de la Comisión para el Consejo Europeo extraordinario a efectuarse en Lisboa el 23 y 24 de marzo de 2000: “*eEurope - Una sociedad de la información para todos*” [COM (1999) 687], disponible en: http://eurlex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=es&type_doc=COMfinal&an_doc=1999&nu_doc=687
- Cuervo, José y Lobato de Paiva, Mario Antonio, “A Firma digital e entidades de certificação”, en *REDI: Revista Electrónica de Derecho Informático*, No.46, Brasil, Alfa-Redi, mayo/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1509>
- Del Alamo, Oscar, “Construyendo la Sociedad de la información”, en *REDI: Revista Electrónica de Derecho Informático*, No. 49, Madrid, Alfa-Redi, agosto/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1464>
- Ellison, Carl y Schneier, Bruce, *Diez riesgos de la ICP: lo que a usted no le contaron acerca de la Infraestructura de Clave Pública*; disponible en <http://www.counterpane.com>.
- Fábrica Nacional de Moneda y Timbre - Real casa de la Modena (FNMT-RCM), *Declaración de Prácticas de Certificación*, versión al 4 de enero de 2007, disponible en: www.cert.fnmt.es

- Farinella, Favio, "España y una completa regulación para Internet", en *REDI: Revista Electrónica de Derecho Informático*, No. 47, España, Alfa-Redi, junio/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1494>
- Fdez Parreño, Eduardo, *Extensiones de la V3 del certificado x.509. Seguridad en Redes telemáticas*, disponible en: <http://asignaturas.diatel.upm.es/seguridad/trabajos/trabajos/curso%2001%2002/v3x509.pdf>
- Ferreiros Soto, Carlos y Gonzales Aguilar, Audilio, "Tendencias de las Nuevas Tecnologías de la Información", Montpellier, 2005, en <http://www.ieid.org/congreso/ponencias/Ferreiros%20Soto,%20Carlos%20%20Gonzales%20Aguilar,%20Audilio.pdf>
- Galdos, Jorge Mario, "Responsabilidad Civil e Internet. Algunas Aproximaciones", en *REDI: Revista Electrónica de Derecho Informático*, No. 43, Buenos Aires, Alfa-Redi, febrero/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1574>
- Gimeno Díaz de Atauri, Pablo, *Las Cláusulas Abusivas en las Condiciones Generales de la Contratación, Regulación y Requisitos*, Cuaderno de Derecho Mercantil, Año 2. N° 6, Marzo de 2004, disponible en: <http://www.latinlex.net/cuadernos/mercantil/numero6/cuamerinopi.html>
- Guini, Leonor, "Introducción a la Normativa de firma digital y a su régimen de aplicación", en *REDI: Revista Electrónica de Derecho Informático*, No. 82, Buenos Aires, Alfa-Redi, mayo/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=947>
- Hernández Cortés, Danilo, "Aspectos Legales del Comercio y la Contratación Electrónica en Cuba", en *REDI: Revista Electrónica de Derecho Informático*, No. 95, Cuba, Alfa-Redi, junio/2006, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=6218>
- Hernández Cruz, Francisco, López Cebada, Juan José y Ortega Salamanca, Armando, "Breves Consideraciones sobre las Posibilidades Subyacentes en el uso de la Firma Electrónica Avanzada", en *REDI: Revista Electrónica de Derecho Informático*, No. 18, España, Alfa-Redi, enero/2000, disponible en <http://www.alfa-redi.com/rdi-articulo.shtml?x=399>.
- Hernández Fernández, Lisette, "La oferta y la aceptación. Especial referencia a los contratos celebrados por medios electrónicos", en *REDI: Revista Electrónica de Derecho Informático*, No. 76, Cuba, Alfa-Redi, noviembre/2004, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1037>
- Irabien Chedraui, José Fernando, "La Estandarización Internacional en el Ámbito de la Certificación Digital", en *REDI: Revista Electrónica de Derecho Informático*, No. 64, México, Alfa-Redi, noviembre/2003, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1266>
- Irabien Chedraui, José Fernando, "Key Management y Certificación Digital", en *REDI: Revista Electrónica de Derecho Informático*, No. 52, México, Alfa-Redi, noviembre/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1411>
- Laguna Quiroz, Rosa, "Bolivia: El Gobierno Electrónico: Bases de la Administración Gubernamental en Línea", en *REDI: Revista Electrónica de Derecho Informático*, No. 67, Bolivia, Alfa-Redi, febrero/2004, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1232>
- Laguna Quiroz, Rosa, "El Trabajo en la Era Digital: Análisis de la Relación Contractual", en *REDI: Revista Electrónica de Derecho Informático*, No. 78, Bolivia, Alfa-Redi, enero/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=986>
- Loredo A., Alejandro, "Contratos Informáticos y Telemáticos, Comercio Electrónico, y su regulación en la Ley Mexicana", en *REDI: Revista Electrónica de Derecho Informático*, No. 89, México, Alfa-Redi, diciembre/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=3926>
- Maestre, Javier y Sánchez Almeida, Carlos, "Análisis de la Directiva sobre Comercio Electrónico (Servicios de la Sociedad de la Información)", en *REDI: Revista Electrónica de Derecho Informático*, No. 35, España, Alfa-Redi, junio/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=692>

- Magliona, Claudio, “Marco Jurídico de la Contratación Electrónica con especial referencia al Comercio Electrónico”, en *REDI: Revista Electrónica de Derecho Informático*, No. 34, Santiago, Alfa-Redi, mayo/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=681>
- Martín Reyes, María, “El Ocaso del Papel”, en *REDI: Revista Electrónica de Derecho Informático*, No. 13, España, Alfa-Redi, agosto/1999, disponible en: http://publicaciones.derecho.org/redi/No.13_Agosto_de_1999/papel.
- Martínez Barbieri, Mónica Susana, “Responsabilidad de los Operadores de la Red que en su interacción producen daños”, en *REDI: Revista Electrónica de Derecho Informático*, No. 41, Buenos Aires, Alfa-Redi, diciembre/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1003>
- Merino Gaberías, Catalina, “Perspectivas comunitarias en torno a los servicios de la sociedad de la información”, en *REDI: Revista Electrónica de Derecho Informático*, No. 07, España, Alfa-Redi, febrero/1999, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=227>
- Moro Almaraz, María Jesús, “La contratación en el comercio electrónico: luces y sombras”, en *REDI: Revista Electrónica de Derecho Informático*, No. 80, España, Alfa-Redi, marzo/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=968>
- Núñez Fernández, Fernando, “La Firma Electrónica ya Tiene Respaldo y Regulación Legal en España”, en *REDI: Revista Electrónica de Derecho Informático*, No. 17, España, Alfa-Redi, diciembre/1999, disponible en: http://publicaciones.derecho.org/redi/No.17_Diciembre_de_1999/8
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura: UNESCO (1996): “*Las tecnologías de la información y la comunicación en el desarrollo*. Reflexiones de la UNESCO”, en <http://infolac.ucol.mx/documentos/tecnologia.html>
- Oxford Dictionary, “LOG”; disponible en: http://www.wikilearning.com/monografia/control_administracion_e_integridad_de_logs-que_es_un_log/3485-2
- Palazzi, Pablo y Peña, Julián, “Comercio Electrónico y MERCOSUR”, en *REDI: Revista Electrónica de Derecho Informático*, No. 05, Buenos Aires, Alfa-Redi, diciembre/1998, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=193>
- Peguera Poch, Miquel, “Servicios de la Sociedad de la Información: Su caracterización Legal en Europa”, en *REDI: Revista Electrónica de Derecho Informático*, No. 100, Chile, Alfa-Redi, noviembre/2006, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=7842>
- Pérez Pereira, María, “La Situación de los Proveedores de Servicios de Certificación en el Real Decreto-Ley 14/1999, Sobre Firma Electrónica”, en *REDI: Revista Electrónica de Derecho Informático*, No. 017, España, Alfa-Redi, diciembre/1999, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=384>
- Pérez Pereira, María, “Establecimiento y Ley Aplicable al Prestador de Servicios de Certificación en España”, en *REDI: Revista Electrónica de Derecho Informático*, No. 26, Madrid, Alfa-Redi, septiembre/2000, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=551>
- Petrissans Aguilar, Ricardo, “El Futuro y La Sociedad Tecnológica. La necesidad de una reflexión”, en *REDI: Revista Electrónica de Derecho Informático*, No. 33, Montevideo, Alfa-Redi, abril/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=655>
- Portugal, *Libro Verde*, elaborado por la Comisión de la Sociedad de la Información del Ministerio de Ciencias de Portugal y aprobado por el Consejo de Ministros de Portugal, 1997; disponible en: <http://www.missao-si.mct.pt/>.
- Principles on European Tort Law, elaborados por el European Group on Tort Law, disponibles en <http://www.egtl.org>.
- Ramos Suárez, Fernando, “La Firma Digital”, en *REDI: Revista Electrónica de Derecho Informático*, No. 10, España, Alfa-Redi, abril/1999, disponible en: <http://publicaciones.derecho.org/redi/No.%2009%20-%20Abril%20de%201999/1ramos>

- Ramos Suárez, Fernando, “Como Aplicar la Nueva Normativa sobre Firma Electrónica”, en *REDI: Revista Electrónica de Derecho Informático*, No. 19, España, Alfa-Redi, febrero/2000, ubicado en <http://www.alfa-redi.org/rdi-articulo.shtml?x=421>
- Reusser Monsálvez, Carlos Patricio, “¿Qué es la Sociedad de la Información?”, en *REDI: Revista Electrónica de Derecho Informático*, No. 61, Santiago, Alfa-Redi, agosto/2003, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1307>
- Reyes Krafft, Alfredo, “¿Qué son los algoritmos de encriptación? Estándares y su aplicación”, *Ciber-leyes*, ubicado en <http://www.alambre.info/2003/12/29/que-son-los-algoritmos-de-encripcion/>
- Reyes Krafft, Alfredo, “*Criptografía: ciencia de la seguridad. Sus antecedentes*”, disponible en <http://www.alambre.info/2003/12/22/criptografia-ciencia-de-la-seguridad/>
- Rodríguez, Antonio “La brecha y el “Fatum” de Latinoamérica”, en *REDI: Revista Electrónica de Derecho Informático*, No. 39, Lima, Alfa-Redi, octubre/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=844>
- Rodríguez Caramelo, Luis Miguel y otros, “*Funcionamiento de los certificados digitales: un modelo didáctico*”, disponible en <http://www.ieid.org/congreso/ponencias/Rodr%EDguez%20Caramelo%20y%20otros.pdf>
- Rodríguez Ruiz de Villa, Daniel, “*Dos aspectos de los prestadores de servicios de certificación electrónica: concepto y acceso*”, disponible en <http://www.ieid.org/congreso/ponencias/Rodriguez%20Ruiz.%20Daniel.pdf>
- Santander Rengifo, Antonio José, “La Oferta al Público por Internet: Una visión desde la Doctrina del Derecho Civil”, en *REDI: Revista Electrónica de Derecho Informático*, No. 79, Perú, Alfa-Redi, febrero/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=977>
- Soto Coaguila, Carlos Alberto, “El Comercio Electrónico en el Derecho Peruano”, en *REDI: Revista Electrónica de Derecho Informático*, No. 41, Lima, Alfa-Redi, diciembre/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1015>
- Vallepuga Gonzalez, Paula, “Responsabilidad de los Prestadores de Servicios de la Sociedad de la Información”, en *REDI: Revista Electrónica de Derecho Informático*, No. 30, España, Alfa-Redi, enero/2001, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=615>
- Veà Baró, Andreu, *Historia, Sociedad, Tecnología y Crecimiento de la Red. Una aproximación divulgativa a la realidad más desconocida de Internet*, 2002, disponible en http://www.tdx.cesca.es/TESIS_URL/AVAILABLE/TDX-1104104-101718/Index.htm
- Villahermosa Iglesias, Alfonso, “Luces y sombras de la LSSICE: la regulación de Internet”, en *REDI: Revista Electrónica de Derecho Informático*, No. 52, España, Alfa-Redi, noviembre/2002, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=1413>
- Vittone Davila, Alberto, “Riesgos de la Contratación Bancaria Electrónica en el Derecho Comparado con la legislación colombiana”, en *REDI: Revista Electrónica de Derecho Informático*, No. 82, Colombia, Alfa-Redi, mayo/2005, ubicado en <http://www.alfa-redi.com/rdi-articulo.shtml?x=952>

ANEXOS

Ley 59/2003, de 19 de diciembre, de firma electrónica

(Boletín Oficial del Estado de 20 de diciembre de 2003, n.º 304)

(*) Texto consolidado conforme las disposiciones de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información.

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.

Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

EXPOSICIÓN DE MOTIVOS

I

El 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 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.

II

El desarrollo de la sociedad de la información y la difusión de los efectos positivos que de ella se derivan exige la generalización de la confianza de la ciudadanía en las comunicaciones telemáticas. No obstante, los datos más recientes señalan que aún existe desconfianza por parte de los intervinientes en las transacciones telemáticas y, en general, en las comunicaciones que las nuevas tecnologías permiten a la hora de transmitir información, constituyendo esta falta de confianza un freno para el desarrollo de la sociedad de la información, en particular, la Administración y el comercio electrónicos.

Como respuesta a esta necesidad de conferir seguridad a las comunicaciones por internet surge, entre otros, la firma electrónica. La firma electrónica constituye un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

Los sujetos que hacen posible el empleo de la firma electrónica son los denominados prestadores de servicios de certificación. Para ello expiden certificados electrónicos, que son 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.

La 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. Además, 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.

Asimismo, debe destacarse que 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 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.

Por otra parte, la ley contiene las garantías que deben ser cumplidas por los dispositivos de creación de firma para que puedan ser considerados como dispositivos seguros y conformar así una firma electrónica reconocida.

La certificación técnica de los dispositivos seguros de creación de firma electrónica se basa en el marco establecido por la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo. Para esta certificación se utilizarán las normas técnicas publicadas a tales efectos en el "Diario Oficial de las Comunidades Europeas" o, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología.

Adicionalmente, la ley establece un marco de obligaciones aplicables a los prestadores de servicios de certificación, en función de si éstos emiten certificados reconocidos o no, y determina su régimen de responsabilidad, teniendo en cuenta los deberes de diligencia que incumben a los firmantes y a los terceros destinatarios de documentos firmados electrónicamente.

III

Esta ley se promulga para reforzar el marco jurídico existente incorporando a su texto algunas novedades respecto del Real Decreto Ley 14/1999 que contribuirán a dinamizar el mercado de la prestación de servicios de certificación.

Así, se revisa la terminología, se modifica la sistemática y se simplifica el texto facilitando su comprensión y dotándolo de una estructura más acorde con nuestra técnica legislativa.

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 nuevo 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.

Asimismo, es de destacar de manera particular, la eliminación del registro de prestadores de servicios de certificación, que ha dado paso al establecimiento de un mero servicio de difusión de información sobre los prestadores que operan en el mercado, las certificaciones de calidad y las características de los productos y servicios con que cuentan para el desarrollo de su actividad.

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.

El nuevo régimen nace desde el convencimiento de que los sellos de calidad son un instrumento eficaz para convencer a los usuarios de las ventajas de los productos y servicios de certificación electrónica, resultando imprescindible facilitar y agilizar la obtención de estos símbolos externos para quienes los ofrecen al público.

Si bien se recogen fielmente en la ley los conceptos de "acreditación" de prestadores de servicios de certificación y de "conformidad" de los dispositivos seguros de creación de firma electrónica contenidos en la directiva, la terminología se ha adaptado a la más comúnmente empleada y conocida recogida en la Ley 21/1992, de 16 de julio, de Industria.

Otra modificación relevante es que la ley clarifica la obligación de constitución de una garantía económica por parte de los prestadores de servicios de certificación que emitan certificados reconocidos, estableciendo una cuantía mínima única de tres millones de euros, flexibilizando además la combinación de los diferentes instrumentos para constituir la garantía.

Por otra parte, dado que la prestación de servicios de certificación no está sujeta a autorización previa, resulta importante destacar que la ley refuerza las capacidades de inspección y control del Ministerio de Ciencia y Tecnología, señalando que este departamento podrá ser asistido de entidades independientes y técnicamente cualificadas para efectuar las labores de supervisión y control sobre los prestadores de servicios de certificación.

También ha de destacarse la regulación que la ley contiene respecto del documento nacional de identidad electrónico, que se erige en un certificado electrónico reconocido llamado a generalizar el uso de instrumentos seguros de comunicación electrónica capaces de conferir la misma integridad y autenticidad que la que actualmente rodea las comunicaciones a través de medios físicos. La ley se limita a fijar el marco normativo básico del nuevo DNI electrónico poniendo de manifiesto sus dos notas más características -acredita la identidad de su titular en cualquier procedimiento administrativo y permite la firma electrónica de documentos- remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico.

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.

En todo caso, los certificados electrónicos de personas jurídicas no alteran la legislación civil y mercantil en cuanto a la figura del representante orgánico o voluntario y no sustituyen a los certificados electrónicos que se expidan a personas físicas en los que se reflejen dichas relaciones de representación.

Como resortes de seguridad jurídica, la ley exige, por un lado, una especial legitimación para que las personas físicas soliciten la expedición de certificados ; por otro lado, obliga a los solicitantes a responsabilizarse de la custodia de los datos de creación de firma electrónica asociados a dichos certificados, todo ello sin perjuicio de que puedan ser utilizados por otras personas físicas vinculadas a la entidad. Por último, de cara a terceros, limita el uso de estos certificados a los actos que integren la relación entre la persona jurídica y las Administraciones públicas y a las cosas o servicios que constituyen el giro o tráfico ordinario de la entidad, sin perjuicio de los posibles límites cuantitativos o cualitativos que puedan añadirse. Se trata de conjugar el dinamismo que debe presidir el uso de estos certificados en el tráfico con las necesarias dosis de prudencia y seguridad para evitar que puedan nacer obligaciones incontrolables frente a terceros debido a un uso inadecuado de los datos de creación de firma. El equilibrio entre uno y otro principio se ha establecido sobre las cosas y servicios que constituyen el giro o tráfico ordinario de la empresa de modo paralelo a cómo nuestro más que centenario Código de Comercio regula la vinculación frente a terceros de los actos de comercio realizados por el factor del establecimiento.

Con la expresión "giro o tráfico ordinario" de una entidad se actualiza a un vocabulario más acorde con nuestros días lo que en la legislación mercantil española se denomina "establecimiento fabril o mercantil". Con ello se comprenden las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de actividad de la entidad y las actividades de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares. Por último, debe recalarse que, aunque el "giro o tráfico ordinario" sea un término acuñado por el derecho mercantil, la regulación sobre los certificados de personas jurídicas no sólo se aplica a las sociedades mercantiles, sino a cualquier tipo de persona jurídica que quiera hacer uso de la firma electrónica en su actividad.

Adicionalmente, se añade un régimen especial para la expedición de certificados electrónicos a entidades sin personalidad jurídica a las que se refiere el artículo 33 de la Ley General Tributaria, a los

solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministerio de Hacienda.

Por otra parte, siguiendo la pauta marcada por la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, se incluye dentro de la modalidad de prueba documental el soporte en el que figuran los datos firmados electrónicamente, dando mayor seguridad jurídica al empleo de la firma electrónica al someterla a las reglas de eficacia en juicio de la prueba documental.

Además, debe resaltarse que otro aspecto novedoso de la ley es el acogimiento explícito que se efectúa de las relaciones de representación que pueden subyacer en el empleo de la firma electrónica. No cabe duda que el instituto de la representación está ampliamente generalizado en el tráfico económico, de ahí la conveniencia de dotar de seguridad jurídica la imputación a la esfera jurídica del representado las declaraciones que se cursan por el representante a través de la firma electrónica.

Para ello, se establece como novedad que en la expedición de certificados reconocidos que admitan entre sus atributos relaciones de representación, ésta debe estar amparada en un documento público que acredite fehacientemente dicha relación de representación así como la suficiencia e idoneidad de los poderes conferidos al representante. Asimismo, se prevén mecanismos para asegurar el mantenimiento de las facultades de representación durante toda la vigencia del certificado reconocido.

Por último, debe destacarse que la ley permite que los prestadores de servicios de certificación podrán, con el objetivo de mejorar la confianza en sus servicios, establecer mecanismos de coordinación con los datos que preceptivamente deban obrar en los Registros públicos, en particular, mediante conexiones telemáticas, a los efectos de verificar los datos que figuran en los certificados en el momento de la expedición de éstos.

Dichos mecanismos de coordinación también podrán contemplar la notificación telemática por parte de los registros a los prestadores de servicios de certificación de las variaciones registrales posteriores.

IV

La ley consta de 36 artículos agrupados en seis títulos, 10 disposiciones adicionales, dos disposiciones transitorias, una disposición derogatoria y tres disposiciones finales.

El título I contiene los principios generales que delimitan los ámbitos subjetivo y objetivo de aplicación de la ley, los efectos de la firma electrónica y el régimen de empleo ante las Administraciones públicas y de acceso a la actividad de prestación de servicios de certificación.

El régimen aplicable a los certificados electrónicos se contiene en el título II, que dedica su primer capítulo a determinar quiénes pueden ser sus titulares y a regular las vicisitudes que afectan a su vigencia. El capítulo II regula los certificados reconocidos y el tercero el documento nacional de identidad electrónico.

El título III regula la actividad de prestación de servicios de certificación estableciendo las obligaciones a que están sujetos los prestadores -distinguiendo con nitidez las que solamente afectan a los que expiden certificados reconocidos-, y el régimen de responsabilidad aplicable.

El título IV establece los requisitos que deben reunir los dispositivos de verificación y creación de firma electrónica y el procedimiento que ha de seguirse para obtener sellos de calidad en la actividad de prestación de servicios de certificación.

Los títulos V y VI dedican su contenido, respectivamente, a fijar los regímenes de supervisión y sanción de los prestadores de servicios de certificación.

Por último, cierran el texto las disposiciones adicionales -que aluden a los regímenes especiales que resultan de aplicación preferente-, las disposiciones transitorias -que incorporan seguridad jurídica a la actividad desplegada al amparo de la normativa anterior-, la disposición derogatoria y las disposiciones finales relativas al fundamento constitucional, la habilitación para el desarrollo reglamentario y la entrada en vigor.

Esta disposición ha sido sometida al procedimiento de información en materia de normas y reglamentaciones técnicas previsto en la 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 normas y reglamentaciones técnicas, modificada por la Directiva 98/48/CE, del Parlamento Europeo y del Consejo,

de 20 de julio de 1998, y en el Real Decreto 1337/1999, de 31 de julio, por el que se regula la remisión de información en materia de normas y reglamentaciones técnicas y reglamentos relativos a los servicios de la sociedad de la información.

TÍTULO I Disposiciones generales

Artículo 1. Objeto.

1. Esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.
2. Las disposiciones contenidas en esta ley no alteran 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 2. Prestadores de servicios de certificación sujetos a la ley.

1. Esta ley se aplicará a los prestadores de servicios de certificación establecidos en España y a los servicios de certificación que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.
2. Se 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.
3. Se entenderá que un prestador de servicios de certificación está establecido en España cuando su residencia o domicilio social se halle en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.
4. Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en él, de forma continuada o habitual, de instalaciones o lugares de trabajo en los que realice toda o parte de su actividad.
5. Se presumirá que un prestador de servicios de certificación está establecido en España cuando dicho 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 mera utilización de medios tecnológicos situados en España para la prestación o el acceso al servicio no implicará, por sí sola, el establecimiento del prestador en España.

Artículo 3. Firma electrónica, y documentos firmados electrónicamente.

1. 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.
2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
3. Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
4. 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.
5. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

Sin perjuicio de lo dispuesto en el párrafo anterior, para que un documento electrónico tenga la naturaleza de documento público o de documento administrativo deberá cumplirse, respectivamente, con lo dispuesto en las letras a) o b) del apartado siguiente y, en su caso, en la normativa específica aplicable.

6. 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.

c) Documentos privados.

7. Los documentos a que se refiere el apartado anterior tendrán el valor y la eficacia jurídica que corresponda a su respectiva naturaleza, de conformidad con la legislación que les resulte aplicable.

8. El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. 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 se trata de una firma electrónica avanzada basada en un certificado reconocido, 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 seguro de creación de firma electrónica.

La carga de realizar las citadas comprobaciones corresponderá a quien haya presentado el documento electrónico firmado con firma electrónica reconocida. Si dichas comprobaciones obtienen un resultado positivo, se presumirá la autenticidad de la firma electrónica reconocida con la que se haya firmado dicho documento electrónico 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 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.

9. No 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.

10. 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.

Artículo 4. Empleo de la firma electrónica en el ámbito de las Administraciones públicas.

1. Esta ley se aplicará al uso de la firma electrónica en el seno de las Administraciones públicas, sus organismos públicos y las entidades dependientes o vinculadas a las mismas y en las relaciones que mantengan aquéllas y éstos entre sí o con los particulares.

Las Administraciones públicas, con el objeto de salvaguardar las garantías de cada procedimiento, podrán establecer condiciones adicionales a la utilización de la firma electrónica en los procedimientos. Dichas condiciones podrán incluir, entre otras, la imposición de fechas electrónicas sobre los documentos electrónicos integrados en un expediente administrativo. Se entiende por fecha electrónica el conjunto de datos en forma electrónica utilizados como medio para constatar el momento en que se ha efectuado una actuación sobre otros datos electrónicos a los que están asociados.

2. Las condiciones adicionales a las que se refiere el apartado anterior sólo podrán hacer referencia a las características específicas de la aplicación de que se trate y deberán garantizar el cumplimiento de lo previsto en el artículo 45 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. Estas condiciones serán objetivas, proporcionadas, transparentes y no discriminatorias y no deberán obstaculizar la prestación de servicios de certificación al ciudadano cuando intervengan distintas Administraciones públicas nacionales o del Espacio Económico Europeo.

3. Las normas que establezcan condiciones generales adicionales para el uso de la firma electrónica ante la Administración General del Estado, sus organismos públicos y las entidades dependientes o vinculadas a las mismas se dictarán a propuesta conjunta de los Ministerios de Administraciones Públicas

y de Ciencia y Tecnología y previo informe del Consejo Superior de Informática y para el impulso de la Administración Electrónica.

4. La utilización de la firma electrónica en las comunicaciones que afecten a la información clasificada, a la seguridad pública o a la defensa nacional se regirá por su normativa específica.

Artículo 5. Régimen de prestación de los servicios de certificación.

1. La prestación de servicios de certificación no está sujeta a autorización previa y 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.

2. Los órganos de defensa de la competencia velarán por el mantenimiento de condiciones de competencia efectiva en la prestación de servicios de certificación al público mediante el ejercicio de las funciones que tengan legalmente atribuidas.

3. La prestación al público de servicios de certificación por las Administraciones públicas, sus organismos públicos o las entidades dependientes o vinculadas a las mismas se realizará con arreglo a los principios de objetividad, transparencia y no discriminación.

TÍTULO II Certificados electrónicos

CAPÍTULO I Disposiciones generales

Artículo 6. Concepto de certificado electrónico y de firmante.

1. Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

2. El firmante es la persona que posee 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.

Artículo 7. Certificados electrónicos de personas jurídicas.

1. Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos.

Los certificados electrónicos de personas jurídicas no podrán afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

2. La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico.

3. Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.

Asimismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico.

4. Se entenderán hechos por la persona jurídica los actos o contratos en los que su firma se hubiera empleado dentro de los límites previstos en el apartado anterior.

Si la firma se utiliza transgrediendo los límites mencionados, la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios o se hubiesen celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física responsable de la custodia de los datos de creación de firma, quien podrá repetir, en su caso, contra quien los hubiera utilizado.

5. Lo dispuesto en este artículo no será de aplicación a los certificados que sirvan para verificar la firma electrónica del prestador de servicios de certificación con la que firme los certificados electrónicos que expida.

6. Lo dispuesto en este artículo no será de aplicación a los certificados que se expidan a favor de las Administraciones públicas, que estarán sujetos a su normativa específica.

Artículo 8. Extinción de la vigencia de los certificados electrónicos.

1. Son causas de extinción de la vigencia de un certificado electrónico:

- a) Expiración del período de validez que figura en el certificado.
- b) Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
- c) Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.
- d) Resolución judicial o administrativa que lo ordene.
- 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 ; terminación de la representación ; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.
- f) Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.
- g) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
- h) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. El 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 cuatro años.

3. La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Artículo 9. Suspensión de la vigencia de los certificados electrónicos.

1. Los prestadores de servicios de certificación suspenderán la vigencia de los certificados electrónicos expedidos si concurre alguna de las siguientes causas:

- a) Solicitud del firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.
- b) Resolución judicial o administrativa que lo ordene.
- c) La existencia de dudas fundadas acerca de la concurrencia de las causas de extinción de la vigencia de los certificados contempladas en los párrafos c) y g) del artículo 8.1.
- d) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

2. La suspensión de la vigencia de un certificado electrónico surtirá efectos desde que se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación.

Artículo 10. Disposiciones comunes a la extinción y suspensión de la vigencia de certificados electrónicos.

1. El prestador de servicios de certificación hará constar inmediatamente, de manera clara e indubitada, la extinción o suspensión de la vigencia de los certificados electrónicos en el servicio de consulta sobre la vigencia de los certificados en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia.

2. El prestador de servicios de certificación informará al firmante acerca de esta circunstancia de manera previa o simultánea a la extinción o suspensión de la vigencia del certificado electrónico, especificando los motivos y la fecha y la hora en que el certificado quedará sin efecto. En los casos de suspensión, indicará, además, su duración máxima, extinguiéndose la vigencia del certificado si transcurrido dicho plazo no se hubiera levantado la suspensión.

3. La extinción o suspensión de la vigencia de un certificado electrónico no tendrá efectos retroactivos.

4. La extinción o suspensión de la vigencia de un certificado electrónico se mantendrá accesible en el servicio de consulta sobre la vigencia de los certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

CAPÍTULO II Certificados reconocidos

Artículo 11. Concepto y contenido de los certificados reconocidos.

1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

2. Los certificados reconocidos incluirán, al menos, los siguientes datos:

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad 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.

f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

g) El comienzo y el fin del período de validez del certificado.

h) Los límites de uso del certificado, si se establecen.

i) Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

4. Si 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.

Artículo 12. Obligaciones previas a la expedición de certificados reconocidos.

Antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación 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.

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 está en posesión 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.

Artículo 13. Comprobación de la identidad y otras circunstancias personales de los solicitantes de un certificado reconocido.

1. La identificación de la persona física que solicite un certificado reconocido 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 si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial.

El régimen de personación en la solicitud de certificados que se expidan previa identificación del solicitante ante las Administraciones públicas se regirá por lo establecido en la normativa administrativa.

2. En el caso de certificados reconocidos de personas jurídicas, los prestadores de servicios de certificación comprobarán, además, 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. La citada 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.

3. Si los certificados reconocidos reflejan una relación de representación voluntaria, los prestadores de servicios de certificación comprobarán 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. La citada comprobación podrá realizarse, asimismo, mediante consulta en el registro público en el que estén inscritos los mencionados datos, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

Si los certificados reconocidos admiten otros supuestos de representación, los prestadores de servicios de certificación deberán exigir la acreditación de las circunstancias en las que se fundamenten, en la misma forma prevista anteriormente.

Cuando el certificado reconocido 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.

4. 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 certificación 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 al firmante en la forma prescrita en este artículo y le conste al prestador de servicios de certificación que el período de tiempo transcurrido desde la identificación es menor de cinco años.

5. Los prestadores de servicios de certificación podrán realizar las actuaciones de comprobación previstas en este artículo por sí o por medio de otras personas físicas o jurídicas, públicas o privadas, siendo responsable, en todo caso, el prestador de servicios de certificación.

Artículo 14. Equivalencia internacional de certificados reconocidos.

Los certificados electrónicos que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro del Espacio Económico Europeo expidan al público como certificados reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumpla alguna de las siguientes condiciones:

a) Que el prestador de servicios de certificación reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos y haya sido certificado conforme a un sistema voluntario de certificación establecido en un Estado miembro del Espacio Económico Europeo.

b) Que el certificado esté garantizado por un prestador de servicios de certificación establecido en el Espacio Económico Europeo que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos.

c) Que el certificado o el prestador de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

CAPÍTULO III El documento nacional de identidad electrónico

Artículo 15. Documento nacional de identidad electrónico.

1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

2. Todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

Artículo 16. Requisitos y características del documento nacional de identidad electrónico.

1. 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.

2. 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.

TÍTULO III Prestación de servicios de certificación

CAPÍTULO I Obligaciones

Artículo 17. Protección de los datos personales.

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

2. Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos.

Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

3. Los prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deberán constatar su verdadera identidad y conservar la documentación que la acredite.

Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera.

4. En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Artículo 18. Obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos.

Los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones:

a) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.

b) Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

1.º Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido.

2.º Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

3.º El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.

4.º Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

5.º Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.

6.º Las demás informaciones contenidas en la declaración de prácticas de certificación.

La información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos.

c) Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

d) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.

Artículo 19. Declaración de prácticas de certificación.

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta ley 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.

2. La declaración de prácticas de certificación de cada prestador estará disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

3. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de carácter personal y deberá contener todos los requisitos exigidos para dicho documento en la mencionada legislación.

Artículo 20. Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos.

1. Además de las obligaciones establecidas en este capítulo, los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones:

- a) Demostrar la fiabilidad necesaria para prestar servicios de certificación.
- b) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.
- c) Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.
- d) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- e) Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.
- 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.
- g) Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

2. 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.

Artículo 21. Cese de la actividad de un prestador de servicios de certificación.

1. El prestador de servicios de certificación que vaya a cesar en su actividad 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.

2. 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.

3. 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). 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.

CAPÍTULO II Responsabilidad

Artículo 22. Responsabilidad de los prestadores de servicios de certificación.

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone esta ley.

La responsabilidad del prestador de servicios de certificación regulada en esta ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.

2. Si el prestador de servicios de certificación no cumpliera las obligaciones señaladas en los párrafos b) al d) del artículo 12 al garantizar un certificado electrónico expedido por un prestador de servicios de certificación establecido en un Estado no perteneciente al Espacio Económico Europeo, será responsable por los daños y perjuicios causados por el uso de dicho certificado.

3. De manera particular, el prestador de servicios de certificación responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.

4. Los prestadores de servicios de certificación asumirán toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

5. La regulación contenida en esta ley sobre la responsabilidad del prestador de servicios de certificación se entiende sin perjuicio de lo establecido en la legislación sobre cláusulas abusivas en contratos celebrados con consumidores.

Artículo 23. Limitaciones de responsabilidad de los prestadores de servicios de certificación.

1. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe, si el firmante incurre en alguno de los siguientes supuestos:

a) No haber proporcionado al prestador de servicios de certificación 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, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación.

b) La falta de comunicación sin demora al prestador de servicios de certificación de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.

c) Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.

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.

e) Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de certificación le notifique la extinción o suspensión de su vigencia.

f) Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación.

2. En el caso de los certificados electrónicos que recojan un poder de representación del firmante, tanto éste como la persona o entidad representada, cuando ésta tenga conocimiento de la existencia del certificado, están obligados a solicitar la revocación o suspensión de la vigencia del certificado en los términos previstos en esta ley.

3. Cuando el firmante sea una persona jurídica, el solicitante del certificado electrónico asumirá las obligaciones indicadas en el apartado 1.

4. El prestador de servicios de certificación tampoco será responsable por los daños y perjuicios ocasionados al firmante o a terceros de buena fe si el destinatario de los documentos firmados electrónicamente actúa de forma negligente. Se entenderá, en particular, que el destinatario actúa de forma negligente en los siguientes casos:

a) Cuando no compruebe y tenga en cuenta las restricciones que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.

b) Cuando no tenga en cuenta la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o cuando no verifique la firma electrónica.

5. El prestador de servicios de certificación no será responsable de los daños y perjuicios ocasionados al firmante o terceros de buena fe por la inexactitud de los datos que consten en el certificado electrónico si éstos le han sido acreditados mediante documento público, inscrito en un registro público si así resulta exigible. En caso de que dichos datos deban figurar inscritos en un registro público, el prestador de servicios de certificación podrá, en su caso, comprobarlos en el citado registro antes de la expedición del certificado, pudiendo emplear los medios telemáticos facilitados por los citados registros públicos.

6. La exención de responsabilidad frente a terceros obliga al prestador de servicios de certificación a probar que actuó en todo caso con la debida diligencia.

TÍTULO IV

Dispositivos de firma electrónica y sistemas de certificación de prestadores de servicios de certificación y de dispositivos de firma electrónica

CAPÍTULO I

Dispositivos de firma electrónica

Artículo 24. Dispositivos de creación de firma electrónica.

1. Los datos de creación de firma son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

2. Un dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.

3. Un dispositivo seguro de creación de firma es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Artículo 25. Dispositivos de verificación de firma electrónica.

1. Los datos de verificación de firma son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

2. Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.

3. 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 siguientes requisitos:

a) Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.

b) Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.

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.

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.

e) Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.

f) Que pueda detectarse cualquier cambio relativo a su seguridad.

4. Asimismo, 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, podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza.

CAPÍTULO II

Certificación de prestadores de servicios de certificación y de dispositivos de creación de firma electrónica

Artículo 26. Certificación de prestadores de servicios de certificación.

1. La certificación de un prestador de servicios de certificación es el procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público.

2. La certificación de un prestador de servicios de certificación podrá ser solicitada por éste y podrá llevarse a cabo, entre otras, por entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria, y en sus disposiciones de desarrollo.

3. En los procedimientos de certificación podrán utilizarse normas técnicas u otros criterios de certificación adecuados. En caso de utilizarse normas técnicas, se emplearán preferentemente aquellas que gocen de amplio reconocimiento aprobadas por organismos de normalización europeos y, en su defecto, otras normas internacionales o españolas.

4. La certificación de un prestador de servicios de certificación no será necesaria para reconocer eficacia jurídica a una firma electrónica.

Artículo 27. Certificación de dispositivos seguros de creación de firma electrónica.

1. La certificación de dispositivos seguros de creación de firma electrónica es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma.

2. La certificación podrá ser solicitada por los fabricantes o importadores de dispositivos de creación de firma y se llevará a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo.

3. En los procedimientos de certificación se utilizarán las normas técnicas cuyos números de referencia hayan sido publicados en el "Diario Oficial de la Unión Europea" y, excepcionalmente, las aprobadas por el Ministerio de Ciencia y Tecnología que se publicarán en la dirección de Internet de este Ministerio.

4. Los certificados de conformidad de los dispositivos seguros de creación de firma serán modificados o, en su caso, revocados cuando se dejen de cumplir las condiciones establecidas para su obtención.

Los organismos de certificación asegurarán la difusión de las decisiones de revocación de certificados de dispositivos de creación de firma.

Artículo 28. Reconocimiento de la conformidad con la normativa aplicable a los productos de firma electrónica.

1. Se presumirá que los productos de firma electrónica aludidos en el párrafo d) del apartado 1 del artículo 20 y en el apartado 3 del artículo 24 son conformes con los requisitos previstos en dichos artículos si se ajustan a las normas técnicas correspondientes cuyos números de referencia hayan sido publicados en el "Diario Oficial de la Unión Europea".

2. Se 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.

TÍTULO V Supervisión y control

Artículo 29. Supervisión y control.

1. El Ministerio de Ciencia y Tecnología controlará el cumplimiento por los prestadores de servicios de certificación que expidan al público certificados electrónicos de las obligaciones establecidas en esta ley y en sus disposiciones de desarrollo. Asimismo, supervisará el funcionamiento del sistema y de los organismos de certificación de dispositivos seguros de creación de firma electrónica.

2. El Ministerio de Ciencia y Tecnología realizará las actuaciones inspectoras que sean precisas para el ejercicio de su función de control.

Los funcionarios adscritos al Ministerio de Ciencia y Tecnología que realicen la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.

3. El Ministerio de Ciencia y Tecnología podrá acordar las medidas apropiadas para el cumplimiento de esta ley y sus disposiciones de desarrollo.

4. El Ministerio de Ciencia y Tecnología podrá recurrir a entidades independientes y técnicamente calificadas para que le asistan en las labores de supervisión y control sobre los prestadores de servicios de certificación que le asigna esta ley.

Artículo 30. Deber de información y colaboración.

1. Los prestadores de servicios de certificación, la entidad independiente de acreditación y los organismos de certificación tienen la obligación de facilitar al Ministerio de Ciencia y Tecnología toda la información y colaboración precisas para el ejercicio de sus funciones.

En particular, deberán permitir a sus agentes o al personal inspector el acceso a sus instalaciones y la consulta de cualquier documentación relevante para la inspección de que se trate, siendo de aplicación, en su caso, lo dispuesto en el artículo 8.5 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. En sus inspecciones podrán ir acompañados de expertos o peritos en las materias sobre las que versen aquéllas.

2. Los prestadores de servicios de certificación deberán comunicar al Ministerio de Ciencia y Tecnología 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 deberá ser convenientemente actualizada por los prestadores y será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

3. Cuando, como consecuencia de una actuación inspectora, se tuviera conocimiento de hechos que pudieran ser constitutivos de infracciones tipificadas en otras leyes, se dará cuenta de los mismos a los órganos u organismos competentes para su supervisión y sanción.

TÍTULO VI Infracciones y sanciones

Artículo 31. Infracciones.

1. Las infracciones de los preceptos de esta ley se clasifican en muy graves, graves y leves.

2. Son infracciones muy graves:

a) El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, siempre que se hayan causado daños graves a los usuarios o la seguridad de los servicios de certificación se haya visto gravemente afectada.

Lo dispuesto en este apartado no será de aplicación respecto al incumplimiento de la obligación de constitución de la garantía económica prevista en el apartado 2 del artículo 20.

b) La expedición de certificados reconocidos sin realizar todas las comprobaciones previas señaladas en el artículo 12, cuando ello afecte a la mayoría de los certificados reconocidos expedidos en los tres años anteriores al inicio del procedimiento sancionador o desde el inicio de la actividad del prestador si este período es menor.

3. Son infracciones graves:

a) El incumplimiento de alguna de las obligaciones establecidas en los artículos 18 y 20 en la expedición de certificados reconocidos, excepto de la obligación de constitución de la garantía prevista en el apartado 2 del artículo 20, cuando no constituya infracción muy grave.

b) La falta de constitución por los prestadores que expidan certificados reconocidos de la garantía económica contemplada en el apartado 2 del artículo 20.

c) La expedición de certificados reconocidos sin realizar todas las comprobaciones previas indicadas en el artículo 12, en los casos en que no constituya infracción muy grave.

d) El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones señaladas en el artículo 18, si se hubieran causado daños graves a los usuarios o la seguridad de los servicios de certificación se hubiera visto gravemente afectada.

e) El incumplimiento por los prestadores de servicios de certificación de las obligaciones establecidas en el artículo 21 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 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

f) La resistencia, obstrucción, excusa o negativa injustificada a la actuación inspectora de los órganos facultados para llevarla a cabo con arreglo a esta ley y la falta o deficiente presentación de la información solicitada por parte del Ministerio de Ciencia y Tecnología en su función de inspección y control.

g) El incumplimiento de las resoluciones dictadas por el Ministerio de Ciencia y Tecnología para asegurar que el prestador de servicios de certificación se ajuste a esta ley.

4. Constituyen infracciones leves:

El incumplimiento por los prestadores de servicios de certificación que no expidan certificados reconocidos de las obligaciones establecidas en el artículo 18; y el incumplimiento por los prestadores de servicios de certificación de las restantes obligaciones establecidas en esta Ley, cuando no constituya infracción grave o muy grave, con excepción de las obligaciones contenidas en el apartado 2 del artículo 30.

Artículo 32. Sanciones.

1. Por la comisión de infracciones recogidas en el artículo anterior, se impondrán las siguientes sanciones:

a) Por la comisión de infracciones muy graves, se impondrá al infractor multa de 150.001 a 600.000 euros.

La comisión de dos o más infracciones muy graves en el plazo de tres años, podrá dar lugar, en función de los criterios de graduación del artículo siguiente, a la sanción de prohibición de actuación en España durante un plazo máximo de dos años.

b) Por la comisión de infracciones graves, se impondrá al infractor multa de 30.001 a 150.000 euros.

c) Por la comisión de infracciones leves, se impondrá al infractor una multa por importe de hasta 30.000 euros.

2. Las infracciones graves y muy graves podrán llevar aparejada, a costa del sancionado, la publicación de la resolución sancionadora en el "Boletín Oficial del Estado" y en dos periódicos de difusión nacional o en la página de inicio del sitio de internet del prestador y, en su caso, en el sitio de internet del Ministerio de Ciencia y Tecnología, 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.

Artículo 33. Graduación de la cuantía de las sanciones.

La cuantía de las multas que se impongan, dentro de los límites indicados, se graduará teniendo en cuenta lo siguiente:

a) La existencia de intencionalidad o reiteración.

b) La reincidencia, por comisión de infracciones de la misma naturaleza, sancionadas mediante resolución firme.

c) La naturaleza y cuantía de los perjuicios causados.

d) Plazo de tiempo durante el que se haya venido cometiendo la infracción e) El beneficio que haya reportado al infractor la comisión de la infracción.

f) Volumen de la facturación a que afecte la infracción cometida.

Artículo 34. Medidas provisionales.

1. En los procedimientos sancionadores por infracciones graves o muy graves el Ministerio de Ciencia y Tecnología podrá adoptar, con arreglo a la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y sus normas de desarrollo, las medidas de carácter provisional que se estimen necesarias para asegurar la eficacia de la resolución que definitivamente se dicte, el buen fin del procedimiento, evitar el mantenimiento de los efectos de la infracción y las exigencias de los intereses generales.

En particular, podrán acordarse las siguientes:

a) Suspensión temporal de la actividad del prestador de servicios de certificación y, en su caso, cierre provisional de sus establecimientos.

b) 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.

c) 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 las medidas de restricción a que alude este apartado se respetarán, en todo caso, las garantías, normas y procedimientos previstos en el ordenamiento jurídico para proteger los derechos a la intimidad personal y a la protección de los datos personales, cuando éstos pudieran resultar afectados.

2. En los supuestos de daños de excepcional gravedad en la seguridad de los sistemas empleados por el prestador de servicios de certificación que menoscaben seriamente la confianza de los usuarios en los servicios ofrecidos, el Ministerio de Ciencia y Tecnología podrá acordar la suspensión o pérdida de vigencia de los certificados afectados, incluso con carácter definitivo.

3. En todo caso, se respetará el principio de proporcionalidad de la medida a adoptar con los objetivos que se pretendan alcanzar en cada supuesto.

4. En casos de urgencia y para la inmediata protección de los intereses implicados, las medidas provisionales previstas en este artículo podrán ser acordadas antes de la iniciación del expediente sancionador.

Las medidas deberán ser confirmadas, modificadas o levantadas en el acuerdo de iniciación del procedimiento, que deberá efectuarse dentro de los 15 días siguientes a su adopción, el cual podrá ser objeto del recurso que proceda.

En todo caso, dichas medidas quedarán sin efecto si no se inicia el procedimiento sancionador en dicho plazo o cuando el acuerdo de iniciación no contenga un pronunciamiento expreso acerca de las mismas.

Artículo 35. Multa coercitiva.

El órgano administrativo competente para resolver el procedimiento sancionador podrá imponer multas coercitivas por importe que no exceda de 6.000 euros por cada día que transcurra sin cumplir las medidas provisionales que hubieran sido acordadas.

Artículo 36. Competencia y procedimiento sancionador.

1. La imposición de sanciones por el incumplimiento de lo previsto en esta ley corresponderá, en el caso de infracciones muy graves, al Ministro de Ciencia y Tecnología y en el de infracciones graves y leves, al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

No obstante, el incumplimiento de las obligaciones establecidas en el artículo 17 será sancionado por la Agencia de Protección de Datos con arreglo a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

2. La potestad sancionadora regulada en esta Ley se ejercerá de conformidad con lo establecido al respecto en la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y en sus normas de desarrollo.

Disposición adicional primera. Fe pública y uso de firma electrónica.

1. Lo dispuesto en esta ley no sustituye ni modifica las normas que regulan las funciones que corresponden a los funcionarios que tengan legalmente la facultad de dar fe en documentos en lo que se refiere al ámbito de sus competencias siempre que actúen con los requisitos exigidos en la ley.

2. En el ámbito de la documentación electrónica, corresponderá a las entidades prestadoras de servicios de certificación acreditar la existencia de los servicios prestados en el ejercicio de su actividad de certificación electrónica, a solicitud del usuario, o de una autoridad judicial o administrativa.

Disposición adicional segunda. Ejercicio de la potestad sancionadora sobre la entidad de acreditación y los organismos de certificación de dispositivos de creación de firma electrónica.

1. En el ámbito de la certificación de dispositivos de creación de firma, corresponderá al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología la imposición de sanciones por la comisión, por los organismos de certificación de dispositivos seguros de creación de firma electrónica o por la entidad que los acredite, de las infracciones graves previstas en los párrafos e), f) y g) del apartado segundo del artículo 31 de la Ley 21/1992, de 16 de julio, de Industria, y de las infracciones leves indicadas en el párrafo a) del apartado 3 del artículo 31 de la citada ley que cometan en el ejercicio de actividades relacionadas con la certificación de firma electrónica.

2. Cuando dichas infracciones merezcan la calificación de infracciones muy graves, serán sancionadas por el Ministro de Ciencia y Tecnología.

Disposición adicional tercera. Expedición de certificados electrónicos a entidades sin personalidad jurídica para el cumplimiento de obligaciones tributarias.

Podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 33 de la Ley General Tributaria a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministro de Hacienda.

Disposición adicional cuarta. Prestación de servicios por la Fabrica Nacional de Moneda y Timbre-Real Casa de la Moneda.

Lo dispuesto en esta ley se entiende sin perjuicio de lo establecido en el artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.

Disposición adicional quinta. Modificación del artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social.

Se añaden apartado doce al artículo 81 de la Ley 66/1997, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, con la siguiente redacción.

"Doce. En el ejercicio de las funciones que le atribuye el presente artículo, la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda estará exenta de la constitución de la garantía a la que se refiere el apartado 2 del artículo 20 de la Ley 59/2003, de Firma Electrónica."

Disposición adicional sexta. Régimen jurídico del documento nacional de identidad electrónico.

1. Sin perjuicio de la aplicación de la normativa vigente en materia del documento nacional de identidad en todo aquello que se adecue a sus características particulares, el documento nacional de identidad electrónico se registrará por su normativa específica.

2. El Ministerio de Ciencia y Tecnología podrá dirigirse al Ministerio del Interior para que por parte de éste se adopten las medidas necesarias para asegurar el cumplimiento de las obligaciones que le incumban como prestador de servicios de certificación en relación con el documento nacional de identidad electrónico.

Disposición adicional séptima. Emisión de facturas por vía electrónica.

Lo dispuesto en esta ley se entiende sin perjuicio de las exigencias derivadas de las normas tributarias en materia de emisión de facturas por vía electrónica.

Disposición adicional octava. Modificaciones de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Uno. Adición de un nuevo apartado 3 al artículo 10 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

Se añade un apartado 3 con el siguiente texto:

"3. Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.

A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información:

- a) Las características del servicio que se va a proporcionar.
- b) Las funciones que efectuarán los programas informáticos que se descarguen, 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 que se producirá dicho fin, y
- d) El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.

La información anterior deberá estar disponible de manera claramente visible e identificable.

Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con 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."

Dos. Los apartados 2, 3 y 4 del artículo 38 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico se redactan en los siguientes términos:

"2. Son infracciones muy graves:

- a) El incumplimiento de las órdenes dictadas en virtud del artículo 8 en aquellos supuestos en que hayan sido dictadas por un órgano administrativo.
- b) El 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.
- c) El incumplimiento significativo de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12.
- d) La utilización de los datos retenidos, en cumplimiento del artículo 12, para fines distintos de los señalados en él.

3. Son infracciones graves:

- a) El incumplimiento de la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información, prevista en el artículo 12, salvo que deba ser considerado como infracción muy grave.
- b) El incumplimiento significativo de lo establecido en los párrafos a) y f) del artículo 10.1.
- c) El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21.
- d) El incumplimiento significativo de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios.
- e) No poner a disposición del destinatario del servicio las condiciones generales a que, en su caso, se sujete el contrato, en la forma prevista en el artículo 27.
- f) El incumplimiento habitual de la obligación de confirmar la recepción de una aceptación, cuando no 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 esta ley.
- h) El incumplimiento significativo de lo establecido en el apartado 3 del artículo 10.
- i) El incumplimiento significativo de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22.

4. Son infracciones leves:

- a) La 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.
- b) No informar en la forma prescrita por el artículo 10.1 sobre los aspectos señalados en los párrafos b), c), d), e) y g) del mismo, o en los párrafos a) y f) cuando no constituya infracción grave.
- c) El incumplimiento de lo previsto en el artículo 20 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 y no constituya infracción grave.
- e) No facilitar la información a que se refiere el artículo 27.1, cuando las partes no hayan pactado su exclusión o el destinatario sea un consumidor.
- f) El incumplimiento de la obligación de confirmar la recepción de una petición en los términos establecidos en el artículo 28, cuando no se haya pactado su exclusión o el contrato se haya celebrado con un consumidor, salvo que constituya infracción grave.
- g) El incumplimiento de las obligaciones de información o de establecimiento de un procedimiento de rechazo del tratamiento de datos, establecidas en el apartado 2 del artículo 22, cuando no constituya una infracción grave.
- h) El incumplimiento de la obligación del prestador de servicios establecida en el apartado 1 del artículo 22, en relación con los procedimientos para revocar el consentimiento prestado por los destinatarios cuando no constituya infracción grave.
- i) El incumplimiento de lo establecido en el apartado 3 del artículo 10, cuando no constituya infracción grave."

Tres. Modificación del artículo 43, apartado 1, segundo párrafo de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El segundo párrafo del apartado 1 del artículo 43 queda redactado como sigue:

"No obstante lo anterior, 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 refieren los párrafos a) y b) del artículo 38.2 de esta ley corresponderá al órgano que dictó la resolución incumplida. Igualmente, corresponderá a la Agencia de Protección de Datos la imposición de sanciones por la comisión de las infracciones tipificadas en los artículos 38.3 c), d) e i) y 38.4 d), g) y h) de esta ley."

Cuatro. Modificación del artículo 43, apartado 2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico.

El apartado 2 del artículo 43 queda redactado como sigue:

"2. La potestad sancionadora regulada en esta ley se ejercerá de conformidad con lo establecido al respecto en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y en sus normas de desarrollo. No obstante, el plazo máximo de duración del procedimiento simplificado será de tres meses."

Disposición adicional novena. Garantía de accesibilidad para las personas con discapacidad y de la tercera edad.

Los servicios, procesos, procedimientos y dispositivos de firma electrónica deberán ser plenamente accesibles a las personas con discapacidad y de la tercera edad, las cuales no podrán ser en ningún caso discriminadas en el ejercicio de los derechos y facultades reconocidos en esta ley por causas basadas en razones de discapacidad o edad avanzada.

Disposición adicional décima. Modificación de la Ley de Enjuiciamiento Civil.

Se añade un apartado tres al artículo 326 de la Ley de Enjuiciamiento Civil con el siguiente tenor:

"Cuando 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."

Disposición adicional undécima. Resolución de conflictos.

Los usuarios y prestadores de servicios de certificación podrán someter los conflictos que se susciten en sus relaciones al arbitraje.

Cuando el usuario tenga la condición de consumidor o usuario, en los términos establecidos por la legislación de protección de los consumidores, el prestador y el usuario podrán someter sus conflictos al arbitraje de consumo, mediante la adhesión de aquéllos al Sistema Arbitral de Consumo competente.

Disposición transitoria primera. Validez de los certificados electrónicos expedidos previamente a la entrada en vigor de esta ley.

Los certificados electrónicos que hayan sido expedidos por prestadores de servicios de certificación en el marco del Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica, mantendrán su validez.

Disposición transitoria segunda. Prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta ley.

Los prestadores de servicios de certificación establecidos en España antes de la entrada en vigor de esta ley deberán comunicar al Ministerio de Ciencia y Tecnología su actividad y las características de los servicios que presten en el plazo de un mes desde la referida entrada en vigor. Esta información será objeto de publicación en la dirección de internet del citado ministerio con la finalidad de otorgarle la máxima difusión y conocimiento.

Disposición derogatoria única. Derogación normativa.

Queda derogado el Real Decreto Ley 14/1999, de 17 de septiembre, sobre firma electrónica y cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta ley.

Disposición final primera. Fundamento constitucional.

Esta ley se dicta al amparo del artículo 149.1.8.^a, 18.^a, 21.^a y 29.^a de la Constitución.

Disposición final segunda. Desarrollo reglamentario.

1. El Gobierno adaptará la regulación reglamentaria del documento nacional de identidad a las previsiones de esta ley.

2. Así mismo, se habilita al Gobierno para dictar las demás disposiciones reglamentarias que sean precisas para el desarrollo y aplicación de esta ley.

Disposición final tercera. Entrada en vigor.

La presente ley entrará en vigor a los tres meses de su publicación en el "Boletín Oficial del Estado".

Por tanto, Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta ley.

Madrid, 19 de diciembre de 2003.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ MARÍA AZNAR LÓPEZ

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.-

EL PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado constitutivo de la Comunidad Europea y, en particular, el apartado 2 de su artículo 47 y sus artículos 55 y 95, Vista la propuesta de la Comisión(1), Visto el dictamen del Comité Económico y Social(2), Visto el dictamen del Comité de las Regiones(3), De conformidad con el procedimiento establecido en el artículo 251 del Tratado(4), Considerando lo siguiente:

El 16 de abril de 1997, la Comisión presentó al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones la comunicación "Iniciativa europea de comercio electrónico".

El 8 de octubre de 1997, la Comisión presentó al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones la comunicación "El Fomento de la seguridad y la confianza en la comunicación electrónica: hacia un marco europeo para la firma digital y el cifrado".

El 1 de diciembre de 1997, el Consejo invitó a la Comisión a que presentara lo antes posible una propuesta de directiva del Parlamento Europeo y del Consejo sobre la firma digital.

La comunicación y el comercio electrónicos requieren firmas electrónicas y servicios conexos de autenticación de datos. La heterogeneidad normativa en materia de reconocimiento legal de la firma electrónica y acreditación de los proveedores de servicios de certificación entre los Estados miembros puede entorpecer gravemente el uso de las comunicaciones electrónicas y el comercio electrónico. Por otro lado, un marco claro comunitario sobre las condiciones aplicables a la firma electrónica aumentará la confianza en las nuevas tecnologías y la aceptación general de las mismas. La legislación de los Estados miembros en este ámbito no debería obstaculizar la libre circulación de bienes y servicios en el mercado interior.

Es preciso promover la interoperabilidad de los productos de firma electrónica; de conformidad con el artículo 14 del Tratado, el mercado interior implica un espacio sin fronteras interiores en el que está garantizada la libre circulación de mercancías. Deben satisfacerse los requisitos esenciales específicos de los productos de firma electrónica a fin de garantizar la libre circulación en el mercado interior y fomentar la confianza en la firma electrónica, sin perjuicio de lo dispuesto en el Reglamento (CE) n° 3381/94 del Consejo, de 19 de diciembre de 1994, por el que se establece un régimen comunitario de control de las exportaciones de productos de doble uso (5) y en la Decisión 94/942/PESC del Consejo, de 19 de diciembre de 1994, relativa a la Acción común adoptada por el Consejo referente al control de las exportaciones de productos de doble uso (6).

La presente Directiva no armoniza la prestación de servicios por lo que respecta a la confidencialidad de la información cuando sean objeto de disposiciones nacionales en materia de orden público y seguridad pública.

El mercado interior garantiza también la libre circulación de personas, por lo cual es cada vez más frecuente que los ciudadanos y residentes de la Unión Europea tengan que tratar con autoridades de Estados miembros distintos de aquél en el que residen. La disponibilidad de la comunicación electrónica puede ser de gran utilidad a este respecto.

Los rápidos avances tecnológicos y la dimensión mundial de Internet hacen necesario un planteamiento abierto a diferentes tecnologías y servicios de autenticación electrónica de datos.

La firma electrónica se utilizará en muy diversas circunstancias y aplicaciones, dando lugar a una gran variedad de nuevos servicios y productos relacionados con ella o que la utilicen. La definición de dichos productos y servicios no debe limitarse a la expedición y gestión de certificados, sino incluir también cualesquiera otros servicios o productos que utilicen firmas electrónicas o se sirvan de ellas, como los servicios de registro, los servicios de estampación de fecha y hora, los servicios de guías de usuarios, los de cálculo o asesoría relacionados con la firma electrónica.

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.

Los sistemas voluntarios de acreditación destinados a un nivel reforzado de prestación de servicios pueden aportar a los proveedores de servicios de certificación un marco apropiado para aproximarse a los niveles de confianza, seguridad y calidad exigidos por un mercado en evolución. Dichos sistemas deben fomentar la adopción de las mejores prácticas por parte de los proveedores de servicios de certificación; debe darse a los proveedores de servicios de certificación libertad para adherirse a dichos sistemas de acreditación y disfrutar de sus ventajas.

Los servicios de certificación pueden ser prestados tanto por entidades públicas como por personas físicas o jurídicas cuando así se establezca de acuerdo con el Derecho nacional. Los Estados miembros no deben prohibir a los proveedores de servicios de certificación operar al margen de los sistemas de acreditación voluntaria; ha de velarse por que los sistemas de acreditación no supongan mengua de la competencia en el ámbito de los servicios de certificación.

Los Estados miembros pueden decidir cómo llevar a cabo la supervisión del cumplimiento de lo dispuesto en la presente Directiva. La presente Directiva no excluye el establecimiento de sistemas de supervisión basados en el sector privado. La presente Directiva no obliga a los proveedores de servicios de certificación a solicitar ser supervisados con arreglo a cualquier sistema de acreditación aplicable.

Es importante alcanzar un equilibrio entre las necesidades de los consumidores y las de las empresas.

El anexo III abarca los requisitos de los dispositivos seguros de creación de firmas electrónicas para garantizar la funcionalidad de las firmas electrónicas avanzadas; no abarca la totalidad del sistema en cuyo entorno operan dichos dispositivos. El funcionamiento del mercado interior exige que la Comisión y los Estados miembros actúen con celeridad para hacer posible la designación de los organismos encargados de evaluar la conformidad de los dispositivos seguros de firma con el anexo III. Con objeto de subvenir a las necesidades del mercado, la evaluación de la conformidad ha de producirse oportunamente y ser eficaz.

La 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.

La presente Directiva no pretende armonizar las legislaciones nacionales sobre contratos, en particular por lo que respecta al perfeccionamiento y eficacia de los mismos, ni tampoco otras formalidades de naturaleza no contractual relativas a la firma; por dicho motivo, las disposiciones sobre los efectos legales de la firma electrónica deberán entenderse sin perjuicio de los requisitos de forma establecidos por las legislaciones nacionales en materia de celebración de contratos, ni para las normas que determinan el lugar en que se considera celebrado un contrato.

El almacenamiento y la copia de los datos de creación de la firma pueden poner en peligro la validez jurídica de la firma electrónica.

La firma electrónica se utilizará en el sector público en el marco de las administraciones nacionales y comunitarias y en la comunicación entre dichas administraciones y entre éstas y los ciudadanos y agentes económicos, por ejemplo en la contratación pública, la fiscalidad, la seguridad social, la atención sanitaria y el sistema judicial.

Unos criterios armonizados en relación con la eficacia jurídica de la firma electrónica mantendrán un marco jurídico coherente en toda la Comunidad. Las legislaciones nacionales establecen requisitos divergentes con respecto a la validez jurídica de las firmas manuscritas; se pueden utilizar certificados para confirmar la identidad de la persona que firma electrónicamente; las firmas electrónicas avanzadas basadas en un certificado reconocido pretenden lograr un mayor nivel de seguridad. Las firmas electrónicas avanzadas relacionadas con un certificado reconocido y creadas mediante un dispositivo seguro de creación de firma únicamente pueden considerarse jurídicamente equivalentes a las firmas manuscritas si se cumplen los requisitos aplicables a las firmas manuscritas.

Para contribuir a la aceptación general de los métodos de autenticación electrónica, debe garantizarse la admisibilidad de la firma electrónica como prueba en procedimientos judiciales en todos los Estados miembros. El reconocimiento legal de la firma electrónica debe basarse en criterios objetivos y no estar supeditado a la autorización del proveedor de servicios de certificación de que se trate; la legislación nacional rige la determinación de los ámbitos jurídicos en los que pueden usarse los documentos electrónicos y de la firma electrónica. La presente Directiva se entiende sin perjuicio de la facultad de los tribunales nacionales para dictar resoluciones acerca de la conformidad con los requisitos de la presente Directiva y no afecta a las normas nacionales en lo que se refiere a la libertad de la valoración judicial de las pruebas.

Los proveedores de servicios de certificación al público están sujetos a la normativa nacional en materia de responsabilidad.

El desarrollo del comercio electrónico internacional requiere acuerdos transfronterizos que implican a terceros países; para garantizar la interoperabilidad a nivel mundial, podría ser beneficioso celebrar acuerdos con terceros países sobre normas multilaterales en materia de reconocimiento mutuo de servicios de certificación.

Para incrementar la confianza de los usuarios en la comunicación y el comercio electrónicos, los proveedores de servicios de certificación deben observar la normativa sobre protección de datos y el respeto de la intimidad.

Las disposiciones relativas al uso de seudónimos en los certificados no deben impedir a los Estados miembros exigir la identificación de las personas de conformidad con el Derecho comunitario o nacional.

Habida cuenta de que las medidas necesarias para la ejecución de la presente Directiva son medidas de gestión con arreglo al artículo 2 de la Decisión 1999/468/CE del Consejo, de 28 de junio de 1999, por la que se establecen los procedimientos para el ejercicio de las competencias de ejecución atribuidas a la Comisión (7), dichas medidas deben ser aprobadas con arreglo al procedimiento de gestión previsto en el artículo 4 de la citada Decisión.

Transcurridos dos años desde su aplicación, la Comisión procederá a una revisión de la presente Directiva a fin de cerciorarse de que los avances tecnológicos y los cambios del entorno jurídico no han creado obstáculos al logro de los objetivos formulados en la presente Directiva. La Comisión debe estudiar la incidencia de ámbitos técnicos afines y presentar un informe al respecto al Parlamento Europeo y al Consejo.

De conformidad con los principios de subsidiariedad y proporcionalidad recogidos en el artículo 5 del Tratado, el objetivo de crear un marco jurídico armonizado para la prestación del servicio de firma electrónica y de servicios conexos no puede ser alcanzado de manera suficiente por los Estados miembros y, por consiguiente, puede lograrse mejor a nivel comunitario. La presente Directiva no excede de lo necesario para lograr dicho objetivo,

HAN ADOPTADO LA PRESENTE DIRECTIVA:

Artículo 1

Ámbito de aplicación

La presente Directiva tiene por finalidad facilitar el uso de la firma electrónica y contribuir a su reconocimiento jurídico. La presente Directiva crea un marco jurídico para la firma electrónica y para

determinados servicios de certificación con el fin de garantizar el correcto funcionamiento del mercado interior.

La presente Directiva no regula otros aspectos relacionados con la celebración y validez de los contratos u otras obligaciones legales cuando existan requisitos de forma establecidos en las legislaciones nacionales o comunitaria, ni afectan a las normas y límites, contenidos en las legislaciones nacionales o comunitaria, que rigen el uso de documentos.

Artículo 2

Definiciones

A efectos de la presente Directiva, se entenderá por:

- 1) "firma electrónica": los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación;
- 2) "firma electrónica avanzada": la firma electrónica que cumple los requisitos siguientes:
 - a) estar vinculada al firmante de manera única;
 - b) permitir la identificación del firmante;
 - c) haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control;
 - d) estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable;
- 3) "firmante": 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 persona física o jurídica a la que representa;
- 4) "datos de creación de firma": los datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica;
- 5) "dispositivo de creación de firma": un programa informático configurado o un aparato informático configurado que sirve para aplicar los datos de creación de firma;
- 6) "dispositivo seguro de creación de firma": un dispositivo de creación de firma que cumple los requisitos enumerados en el anexo III;
- 7) "datos de verificación de firma": los datos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica;
- 8) "dispositivo de verificación de firma": un programa informático configurado o un aparato informático configurado, que sirve para aplicar los datos de verificación de firma;
- 9) "certificado": la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta;
- 10) "certificado reconocido": el certificado que cumple los requisitos establecidos en el anexo I y es suministrado por un proveedor de servicios de certificación que cumple los requisitos establecidos en el anexo II;
- 11) "proveedor de servicios de certificación": la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica;

12) "producto de firma electrónica": el programa informático o el material informático, o sus componentes específicos, que se destinan a ser utilizados por el proveedor de servicios de certificación para la prestación de servicios de firma electrónica o que se destinan a ser utilizados para la creación o la verificación de firmas electrónicas;

13) "acreditación voluntaria": todo permiso que establezca derechos y obligaciones específicas para la prestación de servicios de certificación, que se concedería, a petición del proveedor de servicios de certificación interesado, por el organismo público o privado encargado del establecimiento y supervisión del cumplimiento de dichos derechos y obligaciones, 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.

Artículo 3

Acceso al mercado

1. Los Estados miembros no condicionarán la prestación de servicios de certificación a la obtención de autorización previa.

2. Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán establecer o mantener sistemas voluntarios de acreditación destinados a mejorar los niveles de provisión de servicios de certificación. Todas las condiciones relativas a tales sistemas deberán ser objetivas, transparentes, proporcionadas y no discriminatorias. Los Estados miembros no podrán limitar el número de proveedores de servicios de certificación acreditados amparándose en la presente Directiva.

3. Los Estados miembros velarán por que se establezca un sistema adecuado que permita la supervisión de los proveedores de servicios de certificación establecidos en su territorio que expiden al público certificados reconocidos.

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.

6. Los Estados miembros y la Comisión cooperarán para promover el desarrollo y la utilización de los dispositivos de creación de firma, a la luz de las recomendaciones para la verificación segura de firma que figuran en el anexo IV y en interés del consumidor.

7. Los Estados miembros podrán supeditar el uso de la firma electrónica en el sector público a posibles prescripciones adicionales. Tales prescripciones serán objetivas, transparentes, proporcionadas y no discriminatorias, y sólo podrán hacer referencia a las características específicas de la aplicación de que se trate.

Estas prescripciones no deberán obstaculizar los servicios transfronterizos al ciudadano.

Artículo 4

Principios del mercado interior

1. Los Estados miembros aplicarán las disposiciones nacionales que adopten en cumplimiento de la presente Directiva a los proveedores de servicios de certificación establecidos en su territorio y a los

servicios prestados por ellos. Los Estados miembros no podrán restringir la prestación de servicios de certificación en los ámbitos regulados por la presente Directiva que procedan de otro Estado miembro.

2. Los Estados miembros velarán por que los productos de firma electrónica que se ajusten a lo dispuesto en la presente Directiva puedan circular libremente en el mercado interior.

Artículo 5

Efectos jurídicos de la firma electrónica

1. Los Estados miembros procurarán que la firma electrónica avanzada basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma 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 sea admisible como prueba en procedimientos judiciales.

2. Los Estados miembros velarán por que no se niegue eficacia jurídica, ni la admisibilidad como prueba en procedimientos judiciales, 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, o
- no esté creada por un dispositivo seguro de creación de firma.

Artículo 6

Responsabilidad

1.- Los Estados miembros garantizarán, como mínimo, que el proveedor de servicios de certificación que expida al público un certificado presentado como certificado reconocido o que garantice al público tal certificado, será responsable por el perjuicio causado a cualquier entidad o persona física o jurídica que confíe razonablemente en el certificado por lo que respecta a:

a) la veracidad, en el momento de su expedición, de toda la información contenida en el certificado reconocido y la inclusión en el certificado de toda la información prescrita para los certificados reconocidos;

b) la garantía de que, en el momento de la expedición del certificado, obraban en poder del firmante identificado en el certificado reconocido los datos de creación de firma correspondientes a los datos de verificación de firma que constan o se identifican en el certificado;

c) la garantía de que los datos de creación y de verificación de firma pueden utilizarse complementariamente, en caso de que el proveedor de servicios de certificación genere ambos; salvo que el proveedor de servicios de certificación demuestre que no ha actuado con negligencia.

2. Los Estados miembros garantizarán como mínimo que el proveedor de servicios de certificación que haya expedido al público un certificado presentado como certificado reconocido será responsable por el perjuicio causado a cualquier entidad o persona física o jurídica que confíe razonablemente en dicho certificado por no haber registrado la revocación del certificado, salvo que el proveedor de servicios de certificación pruebe que no ha actuado con negligencia.

3. Los Estados miembros velarán por que el proveedor de servicios de certificación pueda consignar en un certificado reconocido límites en cuanto a sus posibles usos, siempre y cuando los límites sean reconocibles para terceros. El proveedor de servicios de certificación no deberá responder de los daños y perjuicios causados por el uso de un certificado reconocido que exceda de los límites indicados en el mismo.

4. Los Estados miembros velarán por que el proveedor de servicios de certificación pueda consignar en el certificado reconocido un valor límite de las transacciones que puedan realizarse con el mismo, siempre y cuando los límites sean reconocibles para terceros. El proveedor de servicios de certificación no será responsable por los perjuicios que pudieran derivarse de la superación de este límite máximo.

5. Las disposiciones de los apartados 1 a 4 se aplicarán sin perjuicio de la Directiva 93/13/CEE, del Consejo, de 5 de abril de 1993, sobre las cláusulas abusivas en los contratos celebrados con consumidores(8).

Artículo 7

Aspectos internacionales

1. Los Estados miembros velarán por que los certificados expedidos al público como certificados reconocidos por un proveedor de servicios de certificación establecido en un tercer país, sean reconocidos como jurídicamente equivalentes a los expedidos por un proveedor de servicios de certificación establecido en la Comunidad si se cumple alguna de las condiciones siguientes:

a) que el proveedor de servicios de certificación cumpla los requisitos establecidos en la presente Directiva y haya sido acreditado en el marco de un sistema voluntario de acreditación establecido en un Estado miembro;

b) que un proveedor de servicios de certificación establecido en la Comunidad, que cumpla las prescripciones de la presente Directiva, avale el certificado;

c) que el certificado o el proveedor de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad y terceros países u organizaciones internacionales.

2. Para facilitar tanto la prestación de servicios transfronterizos de certificación con terceros países como el reconocimiento legal de las firmas electrónicas avanzadas originarias de estos últimos, la Comisión presentará, en su caso, propuestas para lograr el efectivo establecimiento de normas y acuerdos internacionales aplicables a los servicios de certificación. En particular, y en caso necesario, solicitará al Consejo mandatos para la negociación de acuerdos bilaterales y multilaterales con terceros países y organizaciones internacionales. El Consejo se pronunciará por mayoría cualificada.

3. Cuando la Comisión sea informada de cualquier dificultad encontrada por las empresas comunitarias en relación con el acceso al mercado en terceros países, podrá, en caso necesario, presentar propuestas al Consejo para obtener un mandato adecuado para la negociación de derechos comparables para las empresas comunitarias en dichos terceros países. El Consejo se pronunciará por mayoría cualificada. Las medidas tomadas en virtud del presente apartado se entenderán sin perjuicio de las obligaciones de la Comunidad y de los Estados miembros con arreglo a los acuerdos internacionales pertinentes.

Artículo 8

Protección de datos

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 (9).

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.

Artículo 9

Comité

1. La Comisión estará asistida por el Comité de firma electrónica (denominado en lo sucesivo "el Comité"), compuesto por representantes de los Estados miembros y presidido por el representante de la Comisión.

2. En los casos en que se haga referencia al presente apartado, se aplicará el procedimiento de gestión previsto en el artículo 4 de la Decisión 1999/468/CE observando lo dispuesto en el artículo 8 de la misma. El plazo previsto en el apartado 3 del artículo 4 de la Decisión 1999/468/CE será de tres meses.

3. El Comité aprobará su Reglamento interno.

Artículo 10

Funciones del Comité

El Comité procederá a la clarificación de los requisitos establecidos en los anexos, los criterios a que se refiere el apartado 4 del artículo 3 y las normas para los productos de firma electrónica que gocen de reconocimiento general establecidas y publicadas con arreglo a lo dispuesto en el apartado 5 del artículo 3, conforme al procedimiento establecido en el apartado 2 del artículo 9.

Artículo 11

Notificación

1. Los Estados miembros interesados notificarán a la Comisión y a los demás Estados miembros lo siguiente:

a) información sobre los sistemas voluntarios de acreditación de ámbito nacional, incluidos cualesquiera requisitos adicionales con arreglo al apartado 7 del artículo 3;

b) el nombre y dirección de los organismos nacionales competentes en materia de acreditación y supervisión, así como de los organismos a que se refiere el apartado 4 del artículo 3; y c) el nombre y dirección de todos los proveedores nacionales de servicios de certificación acreditados.

2. Toda la información facilitada en virtud del apartado 1 y cualquier modificación de su contenido serán notificadas por los Estados miembros a la mayor brevedad.

Artículo 12

Revisión

1. La Comisión procederá al examen de la aplicación de la presente Directiva y presentará el oportuno informe al Parlamento Europeo y al Consejo a más tardar el 19 de julio de 2003.

2. Dicho examen permitirá, entre otras cosas, determinar si conviene modificar el ámbito de aplicación de la presente Directiva en vista de la evolución tecnológica y comercial y del contexto jurídico. El informe incluirá, en particular, una valoración de los aspectos de armonización, basada en la experiencia adquirida. El informe irá acompañado, en su caso, de propuestas legislativas.

Artículo 13

Aplicación

1. Los Estados miembros pondrán en vigor las disposiciones legales, reglamentarias y administrativas necesarias para dar cumplimiento a lo establecido en la presente Directiva antes del 19 de julio de 2001. Informarán inmediatamente de ello a la Comisión. Cuando los Estados miembros adopten dichas disposiciones, éstas harán referencia a la presente Directiva o irán acompañadas de dicha referencia en su publicación oficial. Los Estados miembros establecerán las modalidades de la mencionada referencia.

2. Los Estados miembros comunicarán a la Comisión el texto de las principales disposiciones de Derecho interno que adopten en el ámbito regulado por la presente Directiva.

Artículo 14

Entrada en vigor

La presente Directiva entrará en vigor el día de su publicación en el Diario Oficial de las Comunidades Europeas.

Artículo 15

Destinatarios

Los destinatarios de la presente Directiva serán los Estados miembros.

Hecho en Bruselas, el 13 de diciembre de 1999.

Por el Parlamento Europeo

La Presidenta

N. FONTAINE

Por el Consejo

El Presidente

S. HASSI

(1) DO C 325 de 23.10.1998, p. 5.

(2) DO C 40 de 15.2.1999, p. 29.

(3) DO C 93 de 6.4.1999, p. 33.

(4) Dictamen del Parlamento Europeo de 13 de enero de 1999 (DO C 104 de 14.4.1999, p. 49), Posición común del Consejo de 28 de junio de 1999 (DO C 243 de 27.8.1999, p. 83) y Decisión del Parlamento Europeo de 27 de octubre de 1999 (no publicada aún en el Diario Oficial), Decisión del Consejo de 30 de noviembre de 1999.

(5) DO L 367 de 31.12.1994, p. 1; Reglamento modificado por el Reglamento (CE) n° 837/95 (DO L 90 de 21.4.1995, p. 1).

(6) DO L 367 de 31.12.1994, p. 8; Decisión cuya última modificación la constituye la Decisión 1999/193/CE (DO L 73 de 19.3.1999, p. 1).

(7) DO L 184 de 17.7.1999, p. 23.

(8) DO L 95 de 21.4.1993, p. 29.

(9) DO L 281 de 23.11.1995, p. 31.

ANEXO I

Requisitos de los certificados reconocidos

Los certificados reconocidos habrán de contener:

- a) la indicación de que el certificado se expide como certificado reconocido;
- b) la identificación del proveedor de servicios de certificación y el Estado en que está establecido;
- c) el nombre y los apellidos del firmante o un seudónimo que conste como tal;
- d) un atributo específico del firmante, en caso de que fuera significativo en función de la finalidad del certificado;
- e) los datos de verificación de firma que correspondan a los datos de creación de firma bajo control del firmante;
- f) una indicación relativa al comienzo y fin del período de validez del certificado;
- g) el código indentificativo del certificado;
- h) la firma electrónica avanzada del proveedor de servicios de certificación que expide el certificado;
- i) los límites de uso del certificado, si procede; y
- j) los límites del valor de las transacciones para las que puede utilizarse el certificado, si procede.

ANEXO II

Requisitos de los proveedores de servicios de certificación que expiden certificados reconocidos

Los proveedores de servicios de certificación deberán:

- a) demostrar la fiabilidad necesaria para prestar servicios de certificación;
- b) garantizar la utilización de un servicio rápido y seguro de guía de usuarios y de un servicio de revocación seguro e inmediato;
- c) garantizar que pueda determinarse con precisión la fecha y la hora en que se expidió o revocó un certificado;
- d) comprobar debidamente, de conformidad con el Derecho nacional, la identidad y, si procede, cualesquiera atributos específicos de la persona a la que se expide un certificado reconocido;
- e) emplear personal que tenga los conocimientos especializados, la experiencia y las cualificaciones necesarias correspondientes a los servicios prestados, en particular: competencia en materia de gestión, conocimientos técnicos en el ámbito de la firma electrónica y familiaridad con los procedimientos de seguridad adecuados; deben poner asimismo en práctica los procedimientos administrativos y de gestión adecuados y conformes a normas reconocidas;
- f) utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procedimientos con que trabajan;
- g) tomar medidas contra la falsificación de certificados y, en caso de que el proveedor de servicios de certificación genere datos de creación de firma, garantizar la confidencialidad durante el proceso de generación de dichos datos;
- h) disponer de recursos económicos suficientes para operar de conformidad con lo dispuesto en la presente Directiva, en particular para afrontar el riesgo de responsabilidad por daños y perjuicios, por ejemplo contratando un seguro apropiado;
- i) registrar toda la información pertinente relativa a un certificado reconocido durante un período de tiempo adecuado, en particular para aportar pruebas de certificación en procedimientos judiciales. Esta actividad de registro podrá realizarse por medios electrónicos;
- j) no almacenar ni copiar los datos de creación de firma de la persona a la que el proveedor de servicios de certificación ha prestado servicios de gestión de claves;
- k) antes de entrar en una relación contractual con una persona que solicite un certificado para apoyar a partir del mismo su firma electrónica, informar a dicha persona utilizando un medio de comunicación no perecedero de las condiciones precisas de utilización del certificado, incluidos los posibles límites de la utilización del certificado, la existencia de un sistema voluntario de acreditación y los procedimientos de reclamación y solución de litigios. Dicha información deberá hacerse por escrito, pudiendo transmitirse electrónicamente, y deberá estar redactada en un lenguaje fácilmente comprensible. Las partes pertinentes de dicha información estarán también disponibles a instancias de terceros afectados por el certificado;

l) utilizar sistemas fiables para almacenar certificados de forma verificable, de modo que:

- sólo personas autorizadas puedan hacer anotaciones y modificaciones,
- pueda comprobarse la autenticidad de la información,
- los certificados estén a disposición del público para su consulta sólo en los casos en los que se haya obtenido el consentimiento del titular del certificado, y
- el agente pueda detectar todos los cambios técnicos que pongan en entredicho los requisitos de seguridad mencionados.

ANEXO III

Requisitos de los dispositivos seguros de creación de firma electrónica

1. Los dispositivos seguros de creación de firma garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:

- a) los datos utilizados para la generación de firma sólo pueden producirse una vez en la práctica y se garantiza razonablemente su secreto;
- b) existe la seguridad razonable de que los datos utilizados para la generación de firma no pueden ser hallados por deducción y la firma está protegida contra la falsificación mediante la tecnología existente en la actualidad;
- c) los datos utilizados para la generación de firma pueden ser protegidos de forma fiable por el firmante legítimo contra su utilización por otros.

2. Los dispositivos seguros de creación de firma no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes del proceso de firma.

ANEXO IV

Recomendaciones para la verificación segura de firma

Durante el proceso de verificación de firma, deberá garantizarse, con suficiente certeza, que:

- a) los datos utilizados para verificar la firma corresponden a los datos mostrados al verificador;
- b) la firma se verifica de forma fiable y el resultado de esa verificación figura correctamente;
- c) el verificador puede, en caso necesario, establecer de forma fiable el contenido de los datos firmados;
- d) se verifican de forma fiable la autenticidad y la validez del certificado exigido al verificarse la firma;
- e) figuran correctamente el resultado de la verificación y la identidad del firmante;
- f) consta claramente la utilización de un seudónimo; y
- g) puede detectarse cualquier cambio pertinente relativo a la seguridad.

Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) sobre las Firmas Electrónicas (2001)

Artículo 1. Ámbito de aplicación

La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas en el contexto (*) de actividades comerciales (**). No deroga ninguna norma jurídica destinada a la protección del consumidor.

(*) La Comisión propone el texto siguiente para los Estados que deseen ampliar el ámbito de aplicación de la presente Ley: "La presente Ley será aplicable en todos los casos en que se utilicen firmas electrónicas, excepto en las situaciones siguientes: [...]."

(**) El término "comercial" deberá ser interpretado en forma lata de manera que abarque las cuestiones que dimanen de toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, aunque no exclusivamente, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; acuerdos de distribución; representación o mandato comercial; facturaje ("factoring"); arrendamiento con opción de compra ("leasing"); construcción de obras; consultoría; ingeniería; concesión de licencias; inversiones; financiación; banca; seguros; acuerdos o concesiones de explotación; empresas conjuntas y otras formas de cooperación industrial o comercial; transporte de mercancías o de pasajeros por vía aérea, marítima y férrea o por carretera.

Artículo 2. Definiciones

Para los fines de la presente Ley:

- a) Por "firma electrónica" se entenderán los datos en forma electrónica consignados en un mensaje de datos, o adjuntados o lógicamente asociados al mismo, que puedan 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;
- b) Por "certificado" se entenderá todo mensaje de datos u otro registro que confirme el vínculo entre un firmante y los datos de creación de la firma;
- c) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax;
- d) Por "firmante" se entenderá 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;
- e) Por "prestador de servicios de certificación" se entenderá la persona que expide certificados y puede prestar otros servicios relacionados con las firmas electrónicas;
- f) Por "parte que confía" se entenderá la persona que pueda actuar sobre la base de un certificado o de una firma electrónica.

Artículo 3. Igualdad de tratamiento de las tecnologías para la firma

Ninguna de las disposiciones de la presente Ley, con la excepción del artículo 5, será aplicada de modo que excluya, restrinja o prive de efecto jurídico cualquier método para crear una firma electrónica que cumpla los requisitos enunciados en el párrafo 1 del artículo 6 o que cumpla de otro modo los requisitos del derecho aplicable.

Artículo 4. Interpretación

1. En la interpretación de la presente Ley se tendrán en cuenta su origen internacional y la necesidad de promover la uniformidad en su aplicación y de asegurar la observancia de la buena fe.
2. Las cuestiones relativas a las materias que se rigen por la presente Ley que no estén expresamente resueltas en ella se dirimirán de conformidad con los principios generales en los que se basa esta Ley.

Artículo 5. Modificación mediante acuerdo

Las partes podrán establecer excepciones a la presente Ley o modificar sus efectos mediante acuerdo, salvo que ese acuerdo no sea válido o eficaz conforme al derecho aplicable.

Artículo 6. Cumplimiento del requisito de firma

1. Cuando la ley exija la firma de una persona, ese requisito quedará cumplido en relación con un mensaje de datos si se utiliza una firma electrónica que, a la luz de todas las circunstancias del caso, incluido cualquier acuerdo aplicable, sea fiable y resulte igualmente apropiada para los fines con los cuales se generó o comunicó ese mensaje.

2. El párrafo 1 será aplicable tanto si el requisito a que se refiere está expresado en forma de una obligación como si la ley simplemente prevé consecuencias para el caso de que no haya firma.

3. La firma electrónica se considerará fiable a los efectos del cumplimiento del requisito a que se refiere el párrafo 1 si:

- a) los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
- b) los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
- c) es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma; y
- d) cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, es posible detectar cualquier alteración de esa información hecha después del momento de la firma.

4. Lo dispuesto en el párrafo 3 se entenderá sin perjuicio de la posibilidad de que cualquier persona:

- a) demuestre de cualquier otra manera, a los efectos de cumplir el requisito a que se refiere el párrafo 1, la fiabilidad de una firma electrónica; o
- b) aduzca pruebas de que una firma electrónica no es fiable.

5. Lo dispuesto en el presente artículo no será aplicable a: [...].

Artículo 7. Cumplimiento de lo dispuesto en el artículo 6

1. *[La persona, el órgano o la entidad, del sector público o privado, a que el Estado promulgante haya expresamente atribuido competencia]* podrá determinar qué firmas electrónicas cumplen lo dispuesto en el artículo 6 de la presente Ley.

2. La determinación que se haga con arreglo al párrafo 1 deberá ser compatible con las normas o criterios internacionales reconocidos.

3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de la aplicación de las normas del derecho internacional privado.

Artículo 8. Proceder del firmante

1. Cuando puedan utilizarse datos de creación de firmas para crear una firma con efectos jurídicos, cada firmante deberá:

a) actuar con diligencia razonable para evitar la utilización no autorizada de sus datos de creación de la firma;

b) sin dilación indebida, utilizar los medios que le proporcione el prestador de servicios de certificación conforme al artículo 9 de la presente Ley, o en cualquier caso esforzarse razonablemente, para dar aviso a cualquier persona que, según pueda razonablemente prever el firmante, pueda considerar fiable la firma electrónica o prestar servicios que la apoyen si:

i) el firmante sabe que los datos de creación de la firma han quedado en entredicho; o

ii) las circunstancias de que tiene conocimiento el firmante dan lugar a un riesgo considerable de que los datos de creación de la firma hayan quedado en entredicho;

c) cuando se emplee un certificado para refrendar la firma electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el ciclo vital del certificado o que hayan de consignarse en él son exactas y cabales.

2. Serán de cargo del firmante las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1.

Artículo 9. Proceder del prestador de servicios de certificación

1. Cuando un prestador de servicios de certificación preste servicios para apoyar una firma electrónica que pueda utilizarse como firma con efectos jurídicos, ese prestador de servicios de certificación deberá:

a) actuar de conformidad con las declaraciones que haga respecto de sus normas y prácticas;

b) actuar con diligencia razonable para cerciorarse de que todas las declaraciones importantes que haya hecho en relación con el ciclo vital del certificado o que estén consignadas en él son exactas y cabales;

c) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que permitan a ésta determinar mediante el certificado:

i) la identidad del prestador de servicios de certificación;

ii) que el firmante nombrado en el certificado tenía bajo su control los datos de creación de la firma en el momento en que se expidió el certificado;

iii) que los datos de creación de la firma eran válidos en la fecha en que se expidió el certificado o antes de ella;

d) proporcionar a la parte que confía en el certificado medios razonablemente accesibles que, cuando proceda, permitan a ésta determinar mediante el certificado o de otra manera:

i) el método utilizado para comprobar la identidad del firmante;

ii) cualquier limitación de los fines o del valor respecto de los cuales puedan utilizarse los datos de creación de la firma o el certificado;

iii) si los datos de creación de la firma son válidos y no están en entredicho;

iv) cualquier limitación del alcance o del grado de responsabilidad que haya establecido el prestador de servicios de certificación;

v) si existe un medio para que el firmante dé aviso de que los datos de creación de la firma están en entredicho, conforme a lo dispuesto en el apartado b) del párrafo 1 del artículo 8 de la presente Ley;

vi) si se ofrece un servicio para revocar oportunamente el certificado;

e) cuando se ofrezcan servicios conforme al inciso v) del apartado d), proporcionar un medio para que el firmante dé aviso conforme al apartado b) del párrafo 1 del artículo 8 de la presente Ley y, cuando se ofrezcan servicios en virtud del inciso vi) del apartado d), cerciorarse de que existe un servicio para revocar oportunamente el certificado;

f) utilizar, al prestar sus servicios, sistemas, procedimientos y recursos humanos fiables.

2. Serán de cargo del prestador de servicios de certificación las consecuencias jurídicas que entrañe el hecho de no haber cumplido los requisitos enunciados en el párrafo 1.

Artículo 10. Fiabilidad

A los efectos del apartado f) del párrafo 1 del artículo 9, para determinar si los sistemas, procedimientos o recursos humanos utilizados por un prestador de servicios de certificación son fiables, y en qué medida lo son, podrán tenerse en cuenta los factores siguientes:

a) los recursos humanos y financieros, incluida la existencia de activos;

b) la calidad de los sistemas de equipo y programas informáticos;

c) los procedimientos para la tramitación del certificado y las solicitudes de certificados, y la conservación de registros;

- d) la disponibilidad de información para los firmantes nombrados en el certificado y para las partes que confíen en éste;
- e) la periodicidad y el alcance de la auditoría realizada por un órgano independiente;
- f) la existencia de una declaración del Estado, de un órgano de acreditación o del prestador de servicios de certificación respecto del cumplimiento o la existencia de los factores que anteceden; o
- g) cualesquiera otros factores pertinentes.

Artículo 11. Proceder de la parte que confía en el certificado

Serán de cargo de la parte que confía en el certificado las consecuencias jurídicas que entrañe el hecho de que no haya tomado medidas razonables para:

- a) verificar la fiabilidad de la firma electrónica; o
- b) cuando la firma electrónica esté refrendada por un certificado:
 - i) verificar la validez, suspensión o revocación del certificado; y
 - ii) tener en cuenta cualquier limitación en relación con el certificado.

Artículo 12. Reconocimiento de certificados extranjeros y de firmas electrónicas extranjeras

1. Al determinar si un certificado o una firma electrónica producen efectos jurídicos, o en qué medida los producen, no se tomará en consideración:

- a) el lugar en que se haya expedido el certificado o en que se haya creado o utilizado la firma electrónica; ni
- b) el lugar en que se encuentre el establecimiento del expedidor o del firmante.

2. Todo certificado expedido fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que todo certificado expedido en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.

3. Toda firma electrónica creada o utilizada fuera [*del Estado promulgante*] producirá los mismos efectos jurídicos en [*el Estado promulgante*] que toda firma electrónica creada o utilizada en [*el Estado promulgante*] si presenta un grado de fiabilidad sustancialmente equivalente.

4. A efectos de determinar si un certificado o una firma electrónica presentan un grado de fiabilidad sustancialmente equivalente para los fines del párrafo 2, o del párrafo 3, se tomarán en consideración las normas internacionales reconocidas y cualquier otro factor pertinente.

5. Cuando, sin perjuicio de lo dispuesto en los párrafos 2, 3 y 4, las partes acuerden entre sí la utilización de determinados tipos de firmas electrónicas o certificados, se reconocerá que ese acuerdo es suficiente a efectos del reconocimiento transfronterizo, salvo que el acuerdo no sea válido o eficaz conforme al derecho aplicable.