LA FIRMA DIGITAL: UNA TECNOLOGÍA PARA LA INTERCOMUNICACIÓN EN LA SOCIEDAD-RED

Ignacio Salvador Ayestarán*

Resumen: Se lleva a cabo un análisis de las tecnologías de firma electrónica, en el contexto de la Unión Europea, desde una triple perspectiva: técnica, normativa y de soporte I+D. Para ello se realiza una descripción de la naturaleza y funcionamiento de la firma digital, los certificados y las autoridades de certificación, la gestión de claves y sus problemas legales y regulatorios. Se efectúa un análisis histórico del soporte de investigación y desarrollo de la comunidad europea *(Programa de Servicios Confiables Europeos),* previo a la Directiva del Consejo Europeo sobre Firma Electrónica. Por último, se considera el Intercambio Electrónico de Documentos (EDI), en el marco de las políticas del Programa IDA *(Intercambio de Datos entre Administraciones),* y la proyección de la intercomunicación administrativa europea en el futuro.

Palabras clave: firma electrónica, Unión Europea, autoridades de certificación, investigación y desarrollo, Intercambio Electrónico de Documentos, Intercambio de Datos entre Administraciones.

Abstract: An analysis of the technologies of digital signature is achieved within the European Union from three different angles: technique, official standard and I+D support. Firstly, a description of the nature and the bringing into operation of the digital signature is made, together with certificates,Trusted Third Parties, key management and its legal problems. Secondly, a historical analysis of the research support and the development of the European Community is also provided (European Trustworthy Services Programme), previous to the European Council directive about digital signature. Finally, the Electronic Data Interchange (EDI) is considered within the policies of IDA Programme (Interchange Data Administration) and the projection of the future European administrative intercommunication.

Keywords: digital signature, European Union, Trusted Third Parties, Research and Development, Electronic Data Interchange, Interchange Data Administration

1 Introducción

El desarrollo de las tecnologías de firma electrónica para redes abiertas es una necesidad cada vez más sentida por los actores empresariales y privados que realizan interacciones informativas y transacciones comerciales en redes tipo Internet o en redes cerradas, pero abiertas a un público numeroso —redes de la Administración Pública - que necesita interactuar con otros agentes informativos para realizar diversas activi-

* Departamento de Información y Documentación, Universidad de Murcia.
Recibido: 19-10-2000. Segunda versión: 22-2-2001.

dades. En este contexto, la firma digital se presenta como una solución para las políticas de seguridad en las redes, específicamente en lo que se refiere a la autenticación. El mecanismo más utilizado hoy en día en Internet —por su simplicidad— es el de nombre de usuario + contraseña - password—. Mucho más segura es una combinación de esto con el uso de una firma digital, por lo que a corto plazo las firmas digitales y los servicios de certificación se generalizarán con rapidez.

En este contexto, nuestro trabajo (1) es una revisión de las tecnologías de firma digital, desde la perspectiva del soporte técnico, normativo, de regulación y desarrollo que sustenta la **«Directiva del Parlamento Europeo y del Consejo por la que se establece un marco comunitario para la firma electrónica».** Hemos determinado el campo de nuestro estudio en el marco comunitario de la UE, si bien ocasionalmente hemos hecho referencias puntuales a aspectos concretos relacionados con España.

2 La firma digital: una tecnología para las políticas de seguridad electrónica en la red

2.1 Consideraciones previas

Actualmente se está incrementando el uso de redes abiertas, tipo Internet, como plataforma para la comunicación en nuestra sociedad. Redes abiertas y accesibles, que permitan rápidos y eficientes intercambios a nivel mundial, a bajo coste. Esto, sin duda, es una revolución en el mundo de los negocios y de la Administración —empresas «virtuales», trabajo cooperativo universal, en el primer caso; declaración fiscal electrónica y comunicaciones de los ciudadanos con las administraciones, en el segundo.

Sin embargo, es un hecho que la realización de tales desarrollos presenta también los inconvenientes propios de los mismos, que inciden de lleno en el campo de la seguridad informativa: los mensajes pueden ser interceptados y manipulados, la validez de los documentos puede negarse, los datos personales pueden obtenerse ilícitamente, etc. De tal modo que, hoy, los documentos importantes suelen intercambiarse sólo a través de redes cerradas, en donde las relaciones contractuales y la confianza mutua entre los usuarios existen siempre.

Para hacer factible estos intercambios en redes abiertas, las tecnologías criptográficas están ampliamente reconocidas como herramientas esenciales para la seguridad y la confianza en las comunicaciones electrónicas.

Basaremos lo que sigue en la Comunicación (2) de la Comisión al Parlamento, al Consejo, al Comité Económico y Social y al Comité de las Regiones, que sirvió como marco de referencia doctrinal para la posterior elaboración de la Directiva sobre Firma Digital.

2.2 La firma digital: qué es y cómo trabaja

Dos aplicaciones fundamentales de la criptografía son las firmas digitales y la encriptación. Las primeras permiten probar la fuente original de los datos —autenticación —y verificar después que éstos no han sido alterados —integridad. La segunda proporciona la confidencialidad necesaria para la transmisión de datos y la comunicación.

En la UE (3) se distingue claramente entre estas cuestiones: servicios de autenticación e integridad —firmas digitales— y servicios de confidencialidad —encriptación. Esta distinción también se hace claramente en las políticas de la OCDE sobre criptografía (4).

Existen muchos métodos para firmar documentos electrónicos, variando desde métodos simples —insertar una imagen escaneada o una firma manuscrita en un documento hecho con procesador de texto— a otros más avanzados y complejos —uso de criptografía. Las firmas electrónicas basadas en «criptografía de clave pública» son denominadas «firmas digitales» (5).

Un sistema de firma digital segura consta de dos partes: 1) un método para firmar un documento de modo «infalsificable»; y 2) otro para verificar que la firma ha sido generada por la persona a quien representa. Los protocolos de auntenticación pueden estar basados en sistemas de encriptación de tipo simétrico o asimétrico. La autenticación y la integridad se salvaguardan con sistemas asimétricos —de dos claves— denominados generalmente «sistemas de clave pública».

Las firmas digitales con criptografía de clave pública tienen una amplia variedad de aplicaciones:

— firmas digitales usadas para comunicaciones oficiales entre instituciones públicas (documentos de identidad, declaraciones fiscales, transmisión de documentos legales, etc.)
— firmas digitales usadas para relaciones contractuales en redes abiertas (compraventa electrónica, transacciones financieras).
— firmas digitales usadas para identificar o autorizar propósitos (tener certeza de la identidad de una persona autorizada o de sus atributos específicos, p. ej. una autorización para acceder a un sistema informático, identificación de servidores web, etc.).
— firmas digitales usadas en sistemas cerrados (p. ej. intranet corporativa).
— firmas digitales usadas para propósitos personales.

En la comunicación electrónica, el concepto de firmas digitales está unido a la noción de transmisión de datos, usando una clase de precinto electrónico fijado a los datos y que permite al receptor:

a) verificar el origen de los datos: el uso de una clave asignada a cierto remitente (autenticación de la fuente de datos);
b) chequear que los datos están completos, no modificados y por ello salvaguardan su integridad (integridad de los datos).

Técnicamente hablando, las firmas digitales son generalmente creadas y verificadas por técnicas de criptografía asimétrica similares a las usadas para encriptación. Se generan dos claves complementarias y se asignan al usuario. Una de ellas —una clave de firma— es guardada en privado —clave privada— mientras que la otra —una clave de verificación de firma— es publicada - clave pública. Por supuesto, es crucial que la clave privada no pueda ser computada a partir de la clave pública.

Al contrario que la criptografía usada para propósitos de confidencialidad, las firmas digitales están anexionadas a los datos y dejan el contenido del documento electrónico firmado o de la transacción electrónica, intacto. Por supuesto, si se desea, el

contenido de los datos puede ser encriptado adicionalmente para propósitos de confidencialidad.

Con la ayuda de la clave pública del remitente, el receptor puede averiguar si cualquier dato del mensaje firmado ha sido alterado y chequear que la clave pública y la clave privada del remitente son un par de claves complementarias —coincidentes

Pero la verificación de la autenticidad y la integridad de los datos no es necesariamente prueba de la identidad del propietario de la clave pública. ¿Cómo puede el receptor del mensaje conocer que el remitente es realmente quien dice ser? La clave pública puede estar vinculada al mensaje o ser publicada en un directorio, pero ¿qué grado de confidencialidad puede tener el receptor? El receptor puede desear obtener más información confiable sobre la identidad del propietario de la clave. Tal información puede ser proporcionada por el mismo propietario de la clave. Otra forma para ello es tener la confirmación por una tercera parte —una persona o institución mutuamente acordada por ambas partes.

En el contexto de las firmas digitales, a estas terceras partes se las denomina generalmente «autoridades de certificación» (6).

2.3 Las autoridades de certificación (CA)

La provisión de servicios de certificación públicos es un sector completamente nuevo. Este sector, hasta la existencia de la Directiva europea de firma electrónica, estaba dominado por instituciones externas a Europa. A partir de la directiva, han surgido diversas compañías europeas. Centran su actuación básicamente en sus propios mercados nacionales. No tienen, inicialmente, objetivos de mercado en otros estados miembros de la UE. Esta vacilación está también unida a incertidumbres de tipo legal.

Las CA son cruciales para el desarrollo e implementación de las firmas digitales y su completa aceptación dentro de los sistemas legales nacionales, para asegurar el reconocimiento legal y la indisputabilidad de una firma en el comercio electrónico.

2.4. Los contenidos de un certificado

Algunos ejemplos de contenidos de un certificado:.

— nombre o seudónimo del signatario;
— nombre de la autoridad de certificación;
— clave pública del signatario o remitente;
— algoritmo;
— tipo de clave;
— profesión;
— posición dentro de una organización;
— cualificación, licencias (abogado, doctor, empresa de transporte);
— conformidad oficial (permiso de catering, licencia de conducción);
— límites de responsabilidad (límites legales, representación limitada o límites voluntarios);

— cobertura de límites (seguro, depósito);
— confirmación de que, en caso de litigio, los seudónimos serán revelados;
— fecha de extinción del certificado.

2.5 La gestión de claves

La gestión de claves implica un amplio conjunto de tareas que pueden comprender: 1) generación y asignación de pares de claves: 2) identificación del propietario; 3) creación de un directorio de clave pública; 4) datación.

1 y 2) Creación de claves e identificación del propietario

Las claves necesitan ser únicas y profesionalmente estampadas —elección de la longitud y del procedimiento de generación apropiados.

Las claves pueden ser asignadas a personas físicas, personas jurídicas —una compañía S.L.— o a entidades sin personalidad jurídica —departamento de empresa, grupo de trabajo. También pueden asignarse a entidades funcionales, tales como servidores o PC.

3) Directorio de claves

También denominado «repositorio», tiene que estar permanentemente actualizado. Las listas de revocación de certificados permitirán determinar cuándo un certificado ha sido revocado, suspendido o reactivado. La efectividad de estas facilidades dependerá de la velocidad y la responsabilidad del procedimiento de cancelación, que podría usarse en casos de invalidez del certificado o de robo o pérdida de la clave privada.

4) Datación

En muchas situaciones de relación legal, el tiempo exacto de una cierta actuación es crucial. Los servicios de sellado digital permitirán confirmar el tiempo exacto de las actuaciones que sean necesarias. Es también una cuestión crucial en temas de derechos de Propiedad Intelectual.

2.6 Problemática legal

Mientras que las firmas digitales como productos comerciales están permanentemente disponibles en el mercado, sólo algunas compañías en Europa han recorrido los pasos necesarios para ofrecer servicios con esta tecnología, en diferentes áreas -banca, transacciones de comercio electrónico, administración pública, etc. Una de las principales razones es la falta de demanda, resultado particularmente debido a la ausencia, todavía, de reconocimiento legal de las firmas digitales en diversos países. En España, la legislación fue temprana (7). Fue uno de los primeros países europeos que legisló sobre la materia, incluso antes de que la Directiva Europea sobre Firma Digital fuese oficialmente publicada.

2.7 Reconocimiento legal de las firmas digitales

En cada jurisdicción de los estados miembros, los conceptos legales referentes a las firmas y los requisitos sobre forma y procedimientos son diferentes.

La directiva europea (art. 5) regula la armonización de los efectos jurídicos de la firma electrónica. No de modo imperativo, sino indicativo («... los estados miembros *procurarán* que la firma electrónica...) establece los requisitos legales del efecto jurídico. Básicamente debe ser una firma «avanzada» de criptografía de clave pública, basada en un certificado reconocido y creada por un dispositivo seguro de creación de firma.

En nuestro país, en la legislación mencionada anteriormente, se establecen requisitos para la validez jurídica de las firmas digitales, como prueba en caso de litigio.

Éste es un campo de técnica jurídica en el que no entraremos a profundizar. En él se deberían tratar cuestiones como: declaración de intenciones, no repudiación, tratamiento legal de referencias, efectos legales (reconocimiento como prueba en proceso legal, reconocimiento de equivalencia a firma manuscrita, etc).

2. 8 Consideraciones sobre la regulación

Las firmas digitales son actualmente una respuesta reconocida y validada para cuestiones de autenticación e integridad. No obstante, el mercado puede ofrecer otras soluciones tecnológicas. Por tanto, la regulación tiene que crear, por un lado, un marco de trabajo claro para la confianza en el negocio con firmas digitales, pero también debe ser lo bastante flexible para reaccionar a los nuevos desarrollos tecnológicos.

Cualquier regulación no debería restringir, ni de jure ni de facto, la libertad contractual de las partes. Por tanto, debería ser adecuada para los posibles usos diferentes de las firmas digitales. El uso privado de firmas digitales o dentro de grupos cerrados de usuarios, por ejemplo, podría tener una regulación completamente específica. Casos bien identificados podrían ser objeto de regulación general, por ejemplo en las comunicaciones oficiales. En todo caso, es necesario asegurar que los dos esquemas de firma digital, regulado y no regulado, puedan coexistir y ser interoperables.

Algunos estados miembros han introducido esquemas voluntarios y otros, esquemas de tipo licenciatario, para el negocio con CA confiables, respecto al reconocimiento legal de las firmas digitales. Sin embargo, el sistema de licencias es sólo uno de los posibles métodos que los estados miembros pueden aplicar a la promoción del uso de firmas digitales válidas. Otras organizaciones, privadas o públicas, podrían del mismo modo ser consideradas como entidades de certificación.

En un contexto de licencias, es importante distinguir claramente por un lado, los procedimientos y las condiciones para supervisar el establecimiento de una autoridad de certificación y, por otro, las condiciones impuestas sobre los diferentes servicios proporcionados por la CA.

Prácticas restrictivas respecto al establecimiento de CA, los servicios que proporcionan y el uso de herramientas criptográficas irán en detrimento de la libre circulación de bienes y servicios dentro del mercado interior. Podrían dificultar la libertad de establecimiento empresarial, por ejemplo, por discriminar sin motivo sobre la base de una nacionalidad determinada, o restringir injustificadamente el número de estos proveedores de servicios de certificación.

La Directiva para la Firma Electrónica (8) establece un marco regulador que ar-

moniza todas estas cuestiones, si bien deja expresamente fuera de su propósito la prestación de servicios, por lo que respecta a la confidencialidad informativa, cuando éstos sean objeto de disposiciones nacionales en materia de orden y seguridad pública.

Nuestro estudio se centra fundamentalmente en el análisis de las bases de investigación europea —que dieron soporte de I+D a la Directiva— y del Proyecto IDA, extrayendo aquellos aspectos que tocan explícita o implícitamente el tema objeto de nuestro trabajo —la firma digital.

Realizaremos a continuación unas consideraciones analíticas sobre «The European Trusted Services-ETS Programme» (Programa de Servicios Confiables europeos - ETS), que constituye la base investigadora imprescindible para el desarrollo legislativo y la implantación de las tecnologías de firma digital en Europa.

3 El soporte europeo de I + D para la firma digital: el Programa de Servicios Confiables Europeos (ETS)

3.1 Génesis y desarrollo

La Directiva europea requirió un trabajo de campo exploratorio y de preparación previa, en el que se investigaron cuestiones técnicas, de infraestructura, de modelado, especificaciones, estándares, etc, etc. Todo ese trabajo, con independencia de algunas otras iniciativas individualizadas, fue centralizado a través de la Dirección General XIII de la Comisión Europea.

En 1992, la Dirección General XIII de la Comisión Europea comenzó a dirigir las cuestiones sobre Servicios Confiables, a través de su Iniciativa sobre Firmas Electrónicas (ES) y Servicios de Terceras Partes Confiables (TTP).

En 1996, y como preparación para una Decisión del Consejo que permitiría mostrar un Programa de Acción completamente centrado en esta área, se decidió lanzar un programa preparatorio limitado denominado «The European Trusted Services-ETS Programme». El Programa ETS estaba caracterizado por estudios cortos, de un año o menos de duración y recursos limitados (inferiores a 3 millones de euros). Sin embargo, el amplio marco de trabajo del Programa de Acción se aprovechó para establecer un alcance ambicioso de estos proyectos, aunque era obvio que el tiempo existente y las obligaciones contraídas no permitirían la realización de demandas objetivas.

El objetivo principal de ETS ha sido profundizar, para lograr la máxima extensión posible, desde un punto de vista técnico y económico, en los aspectos legales y regulatorios que gobiernan el uso de la criptografía para la autenticación, confidencialidad y no repudiación, y resolver el dilema planteado por el importante incremento de encriptación en la sociedad de la información.

El Programa ETS ha sido realizado en tres fases:

Fase Inicial

Con una duración de 6 meses, durante los cuales se encargaron cinco estudios específicos a organizaciones seleccionadas y a expertos en campos relevantes:

— Servicios Europeos Confiables- Resultados de proyectos INFOSEC de TTP para 1995.

— Cuestiones Legales y Regulatorias concernientes a TTP y Firmas Digitales.
— Guías para el uso de nombres y claves en una infraestructura global de TTP.
— Cuestiones sobre Normalización para Servicios Europeos Confiables.
— Revisión y evaluación de técnicas biométricas.

ETS Fase 1

Con una duración de 1 año, en julio de 1996 se invitó a presentar «trabajos preparatorios relativos al desarrollo de un marco de trabajo, de alcance europeo, de Servicios de Terceras Partes Confiables». Los siguientes ocho proyectos fueron recomendados para su financiación, por un panel de expertos independientes y comenzaron en Enero de 1997:

— OPARATE (Operational and Architectural Aspects of TTP for Europe): Arquitectura Operativa de TTP para Europa.
— EUROTRUST: Euroconfianza. Proyecto piloto para un Servicio de Infraestructura de Clave Pública.
— OSCAR (Open Digital Signature Certification Architecture): Arquitectura abierta para Certificación de Firma Digital.
— KRISIS (Key Recovery in Secure Information Systems): Clave de Recuperación en Sistemas de Información Seguros.
— MANDATE II: Infraestructura de Clave Pública para el uso paneuropeo del cheque electrónico, en las transacciones b2b (business-to-business),
— AEQUITAS (La admisión como prueba, en juicios de carácter penal, de documentos electrónicos, firmados digitalmente) (9).
— EUROMED-ETS (TTP Services for Health Care in Europe): Servicios de TTP para servicios de salud en Europa.
— EAGLE (Key Management Systems for European Users using TTP): Sistemas de Gestión de Clave para Usuarios Europeos, mediante TTP.

ETS Fase 2

Con una duración, así mismo, de 1 año, se invitó a presentar «acciones preparatorias en el área de Servicios Europeos Confiables». Los siguientes siete proyectos fueron recomendados para su financiación, por un panel de expertos independientes y comenzaron en enero de 1998:

— KEYSTONE (European crross-domain PKI Architecture): Arquitectura europea PKI de dominio cruzado.
— SEDUCER (Service Evaluation Definition for User Confidence and ETS Recognition): Definición de Servicio de Evaluación para Confidencialidad de Usuario y Reconocimiento ETS.
— LEGAL (Legal issues of evidence and liability in the provision of Trusted Services): Cuestiones legales sobre evidencia y responsabilidad en la provisión de Servicios Confiables.
— COMETS (Cost Model for the European Trusted Services): Modelo de coste para Servicios Europeos Confiables.
— BESTS (Business Environment Study of Trusted Services): Estudio del entorno de negocio para Servicios Confiables.

— PKITS (Public Key Infraestructure with Time Stamping): Infraestructura de Clave Pública con Datación.
— TRUSTWEB (Assessment of new technologies and mutual impact of ETS and WWW): Valoración de nuevas tecnologías y mutuo impacto de ETS y WWW.

El Programa ETS concluyó con estos siete proyectos, a fines de 1998.

Los 20 proyectos diferentes del programa fueron evaluados por un equipo de expertos independientes —Alemania, Suecia, Francia—, que realizaron un control en profundidad de los trabajos de los mismos, a fin de identificar áreas con necesidades ulteriores. El informe de evaluación (10) del Programa ETS es completo y muy interesante.

3.2. Las conclusiones de evaluación

Leyendo las conclusiones del informe de evaluación del desarrollo del Programa ETS, se observa que, a pesar de la valiosa experiencia obtenida de los diferentes proyectos, el diseño de una «arquitectura PKI europea» permanece sin resolver.

Los beneficios de los proyectos ETS tienen una escala más pequeña. Han resuelto muchas cuestiones detalladas o explorado diversas opciones. Tal vez, el efecto principal del Programa ETS haya sido dar soporte investigador para el desarrollo de las políticas futuras sobre las firmas digitales y la infraestructura de PKI a nivel europeo o pan-europeo. Lo segundo no parece, a la vista de los planteamientos de la Directiva europea —que plantea un marco armonizador, pero deja el desarrollo regulador a las decisiones políticas de los estados miembros— un objetivo fácilmente alcanzable. Las políticas comunes sobre aspectos de justicia y seguridad en los estados miembros, facilitarán el camino para logra esa infraestructura pan-europea que las instituciones europeas desean.

El Programa ETS, así mismo, ha aumentado la experiencia y competencia de todas las organizaciones participantes. Sin embargo, no parece claro que ese valor añadido que las empresas participantes han obtenido en las investigaciones, revierta en forma de aplicaciones o servicios gratuitos para la creación de infraestructura de mercado en Europa.

En algunos casos, han surgido ciertas implementaciones industriales o valiosos beneficios de pequeños proyectos piloto. Es el caso particular de los proyectos OSCAR y EUROTRUST. En el caso de AEQUITAS, el proyecto - como ya hemos dicho - proporcionó un input sustancial al proceso de legislación nacional y para iniciar una infraestructura operativa en nuestro país, pero sin embargo no tuvo mucha relación con el objetivo principal del Programa ETS.

Algunos proyectos han establecido relaciones con organizaciones no participantes. Los proyectos que han sido mejor valorados por las organizaciones participantes, han sido aquéllos que contenían en sus informes análisis o perspectivas, tales como «Cuestiones legales y regulatorias concernientes a TTP y firmas digitales» (ETS Fase Inicial), sin duda uno de los más importantes de todos los que hemos conocido.

Poca gente —según los evaluadores— fuera de los directamente implicados, conoce los proyectos, aunque todos ellos se encuentran en la web de Infosec ETS. Muchos equipos de los proyectos no prestaron bastante atención al significado y repercusión pública de un resumen bien desarrollado de los contenidos del proyecto. Así, incluso la información que se encuentra en la página es difícil de percibir.

4 La Firma Electrónica en la relaciones Administración-ciudadano: el Programa IDA

4.1 El marco relacional de la firma electrónica

La consecución de un mercado interior robusto, con el soporte tecnológico adecuado para operar en redes abiertas tipo Internet —firmas electrónicas para el e-comercio— que permita desarrollar una infraestructura paneuropea es uno de los objetivos fundamentales de la Directiva sobe firma electrónica Pero en los considerandos del apartado expositivo de la misma se afirma:

> «(7) 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;
> (...)
> (19) *la firma electrónica se utilizará en el sector público, en el marco de las administraciones nacionales y comunitaria y en la comunicación de 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» (11).

El siguiente paso importante para la construcción de un mercado interior europeo totalmente integrado es la interconexión de las administraciones públicas nacionales mediante servicios telemáticos comunes. La UE, a través de la Dirección General III de la Comisión Europea, da respuesta a esta exigencia política con el *Programa IDA*.

4.2 El Programa IDA

El programa es la solución europea para el intercambio de datos entre administraciones y constituyó, en su momento, una de las claves de la Iniciativa para la Sociedad de la Información de la UE, según recomendó el «Informe Bangemann» en 1994.

IDA es un programa facilitador de las tareas, pero no regulador. La definición concreta del flujo de datos es responsabilidad de cada uno de los grupos de administraciones públicas (seguridad social, fiscalidad, empleo, etc). El programa es, así mismo, el impulsor de la creación de redes transeuropeas.

Lo concerniente a firmas electrónicas debería enmarcarse dentro de una de las acciones horizontales: *Aspectos Legales y de Seguridad* (Responsables la DG3 y la DG15)

4.3 Algunos aspectos de las políticas de IDA en relación con la firma electrónica

En el intercambio informativo en las relaciones con la administración es importante una de las funcionalidades principales de las firmas electrónicas: la autentica-

ción. La seguridad de que el ciudadano que se relaciona con la Administración es quien dice ser, es un aspecto fundamental en ocasión de relaciones transaccionales de servicios —fiscalidad, seguridad social, etc. En otros casos de intercambios administrativos, las firmas desempeñarían solo la función de identificación de parte, en la relación Administración-ciudadano.

4.3.1 El Intercambio Electrónico de Documentos (EDI) y las firmas digitales.

En el «Informe sobre aspectos legales del intercambio de datos entre administraciones» (12) se establecen algunas conclusiones sobre la validez y el valor de las firmas digitales en el intercambio electrónico de documentos:

— Respecto a la identificación del autor y remitente.
— Respecto a la integridad del mensaje.
— Respecto a la confidencialidad.
— Respecto a la sustitución de firmas manuscritas por firmas digitales.
— Respecto a la aceptación legal de firmas digitales.

Las firmas digitales exigen más regulación que las ordinarias manuscritas, porque el uso de medios electrónicos facilita y acelera el envío de mensajes, de tal modo que uno no es consciente de los peligros potenciales y las responsabilidades que encierran.

En ninguno de los estados miembros, la firma digital se acepta siempre legalmente para propósitos generales. Sólo en áreas específicas puede ser usada en lugar de la tradicional firma manuscrita. Por ejemplo, en Suecia, se aprobó en 1987 el posible intercambio de información electrónica entre los usuarios y la Administración.

En nuestro país, hay actuaciones en este sentido. El proyecto «Interfom» del Ministerio de Fomento (13) para el desarrollo de las nuevas tecnologías, dentro del área de actuación de Seguridad en la Red, plantea:

> «1. Promover la utilización de la firma electrónica en España y el desarrollo del sector de prestaciones de servicios de certificación, garantizando el cumplimiento de la normativa recogida en el Real Decreto-Ley 14/1999. Se pondrá en marcha el sistema de acreditación de prestadores de servicios y de certificación de productos de firma electrónica previsto en la norma.
>
> 2. Avanzar en la regulación de los aspectos jurídicos y técnicos del comercio electrónico, así como promover el uso de sistemas de seguridad en la prestación de este servicio.
>
> 3. Se hará un seguimiento estadístico del uso de la firma electrónica y de la actividad de los prestadores de servicios de certificación.

Más específico y adelantado es el proyecto «Ceres», (http://www.cert.fnmt.es/que_es_ceres.ht) liderado por la Fábrica Nacional de Moneda y Timbre, que, en resumen, consiste en establecer una Entidad Pública de Certificación que autentique y garantice la confidencialidad de las comunicaciones entre ciudadano, empresas e instituciones y administraciones públicas, a través de redes abiertas de comunicación. El proyecto cubre todas aquellas relaciones entre las distintas administraciones (central, autonómica y local) y los ciudadanos, que necesiten ser aseguradas en términos de ga-

rantías de identidad, confidencialidad e integridad de los mensajes. Usa sistema PK, y soporte de tarjeta inteligente de conexión. El sistema es completamente transparente para el usuario, es decir, no es necesario conocer ninguna técnica criptográfica para realizar o verificar una firma electrónica o cifrar o descifrar un mensaje. Actualmente se ha implantado experimentalmente en las relaciones fiscales del ciudadano con el Ministerio de Hacienda —Declaración del IRPF. Su posible utilización garantiza la seguridad de certificados diversos (registro civil, seguridad social, etc.), peticiones de renovación del DNI o diversos documentos oficiales, tramitación de subvenciones y, en general, cualquier envío y recepción de documentación oficial.

4.3.2 Conocimiento y difusión de EDI en los estados miembros

En muchos gobiernos se han establecido equipos gubernamentales de trabajo interdisciplinar para facilitar la implementación técnica y legal de EDI, dentro de la Administración y en el sector privado. Limitaremos nuestro análisis a lo realizado en España.

El Consejo Superior de Informática constituyó la Comisión Nacional de Cooperación entre Administraciones Públicas, en el campo de la tecnología de los sistemas de información (COAXI). Esta comisión creó un grupo de estudio (SSITAD), en que representantes de las administraciones central, autonómica y local centraron su trabajo en el campo de la seguridad, respecto al intercambio electrónico de datos entre administraciones.

En 1992, la legislación (14) adoptó el uso de EDI dentro de la administración pública. En el marco del desarrollo reglamentario de esta ley, se tomaron importantes iniciativas en diferentes campos. Los medios electrónicos son admitidos en la legislación hipotecaria, fiscal, etc. (15). Quizá la legislación más importante, en este sentido, se ha producido en el campo de la Seguridad Social (16). Aparte de otras muchas medidas, se creó una tarjeta de identidad de los asegurados, que proporciona una mejora en la rapidez de provisión de los servicios. Se piensa implantar un nuevo formato, convirtiéndola en tarjeta inteligente, a corto plazo.

4.4 Una mirada sobre el futuro de la intercomunicación administrativa en Europa

A fines de 1997, la Comisión Europea presentó una Comunicación (17) al Consejo sobre la evaluación del programa IDA y una segunda fase del mismo.

Después de evaluar el programa en su fase I, en su apartado 4 plantea los objetivos, estrategia y acciones de cara al futuro. Las actividades comunitarias propuestas están orientadas a conseguir resultados concretos en un plazo de 3 años.

El foco de las actividades está puesto en la *interoperabilidad* administrativa, en el ámbito europeo:

Objetivos:

— Creación de infraestructuras europeas operativas e interoperables, de comunicación telemática entre las administraciones de los estados miembros y entre éstas y las instituciones europeas, según corresponda, que posibiliten un inter-

cambio eficiente y rentable de la información, como respaldo de la gestión administrativa del mercado interior.
— Utilización de soluciones telemáticas plenamente integradas en la gestión cotidiana de las políticas y las actividades de la UE, así como en el proceso de decisión comunitario.
— Disponibilidad de servicios transeuropeos destinados a redes administrativas, caracterizados por su alto nivel de interoperabilidad, dentro de cada sector administrativo y entres sectores administrativos diferentes, así como entre éstos y el sector privado (...).
— Apertura de un banco internacional actualizado de conocimientos y experiencias en materia de redes telemáticas de fácil consulta por parte de todas las administraciones europeas (18).

La interoperabilidad y su mantenimiento requiere en la práctica mucho más que la necesidad de acordar o armonizar normas y especificaciones que serán luego utilizadas, exige también una aplicación compatible de dichas normas y la coherencia de los sistemas legales y de seguridad, así como la integración del conjunto de los nuevos entornos y procesos electrónicos y de los métodos operativos convencionales.

Se establecen —en la comunicación de la Comisión— medidas para el mantenimiento de la interoperabilidad, y se adopta un conjunto de acciones horizontales (19) para facilitarlas, cuya consideración en detalle desbordaría los límites de este artículo.

5 Los dictámenes institucionales para la Directiva. Valoración técnico-política del Comité Económico y Social y del Comité de las Regiones

La propuesta final del Parlamento Europeo y del Consejo —antes de su publicación en el D.O.— fue en su momento - diciembre/98, enero/99 —analizada y valorada por los órganos institucionales que tienen esa función dictaminadora: Comité Económico y Social (20) y Comité de las Regiones (21). Sus dictámenes son preceptivos, pero no vinculantes para la decisión política. Se realizan de conformidad con los artículos 100 A —dictamen del Comité Económico y Social— y primer párrafo del 198C del tratado constitutivo de la Comunidad Europea —Dictamen del Comité de las Regiones.

En esos dictámenes se realizó una valoración crítica de carácter global y una valoración específica y comentario analítico exhaustivo del articulado completo de la Directiva.

6. Conclusiones

De nuestro estudio hemos obtenido las siguientes conclusiones:

— La firmas electrónicas son tecnologías que darán soporte y permitirán el desarrollo de políticas de seguridad en los intercambios de información y documentos, tanto en el sector privado como en el sector público. Esas políticas dependerán, en buena medida, en lo que a su alcance y contenidos se refiere, del marco regulador de la criptografía en Europa.

— Las firmas electrónicas se utilizarán, a corto plazo, en muy diversas circunstancias y aplicaciones. Darán lugar a una gran variedad de productos y servicios relacionados con ellas o que las utilicen. Todos esos productos contribuirán al crecimiento del sector de Nuevas Tecnologías, en el mercado interior europeo. Serán necesarias políticas decididas de normalización y estándares que satisfagan las necesidades que surjan, si se quiere conseguir un mercado interior europeo sólido.
— Para el desarrollo de un mercado interior europeo de productos y servicios de seguridad para los intercambios de información, son necesarias políticas comerciales de sistemas abiertos no propietarios, que puedan romper el mercado actual, dominado por unos pocos sistemas de procedencia externa a Europa. Esta es la idea que tiene la Comisión Europea (22).
— La directiva reguladora europea tiene un objetivo explícitamente armonizador. Ello es coherente con el objetivo de implantar un marco de referencia para la creación de una infraestructura paneuropea de servicios confiables en el mercado interior. Se podrán presentar problemas muy diversos que hagan tal vez necesario un posterior desarrollo reglamentario de alcance europeo, no ya meramente armonizador, sino normativo. La Comisión plantea la directiva desde un enfoque de liberalización y desregulación de servicios en general, que fomenten la libre competencia en un entorno de economía global. Por ello, limita al máximo los aspectos de detalle, que deja a la libre decisión reguladora de los estados miembros.
— Con el propósito de facilitar el desarrollo económico en el mercado interior europeo, la directiva se centra fundamentalmente en las necesidades del comercio electrónico, mientras que las firmas electrónicas y los servicios de valor añadido que éstas posibilitan - certificación, registros, etc - desempeñan un papel importante para el desarrollo de nuevos servicios públicos de alcance europeo, estatal, regional o local. En este campo, no se va más allá de una declaración de intenciones en el expositivo de la directiva.
— Hacen falta decisiones políticas que implementen servicios añadidos de firma electrónica para la Europa social: necesidades de comunicación administrativa electrónica que faciliten la libre circulación de personas (ciudadanos o residentes) entre estados miembros; soporte de seguridad para redes telemáticas europeas y transeuropeas, etc.
— De la misma manera que se adoptan iniciativas para la **eEuropa** —Iniciativa de la Unión Europea para el Consejo de Lisboa, 23/24 marzo—, son necesarias políticas europeas, rápidas y decididas, para la Administración.
— El soporte de I + D que los programas de investigación europeos han proporcionado —fundamentalmente el Programa ETS—, a pesar de la valiosa experiencia obtenida de los diferentes proyectos, no ha resuelto uno de los objetivos fundamentales. El diseño de una «arquitectura PKI europea» permanece sin resolver. El propósito de una infraestructura paneuropea es muy difícil de resolver con una directiva armonizadora que deja a los estados miembros la regulación y el desarrollo de su propia infraestructura de servicios de firma electrónica. En este sentido, podríamos decir que, entre alguno de los objetivos de los programas de I +D y la regulación europea de las firmas electrónicas en la directiva, existe una cierta incoherencia.

— La directiva europea va dirigida fundamentalmente a regular los intercambios de información producidos en redes abiertas tipo Internet. Tal vez el ámbito de los servicios públicos requeriría una actuación más decidida de la Comisión europea para concretar límites y no dejar al arbitrio de las partes el reconocimiento de las firmas electrónicas en sistemas cerrados. Cada vez más, algunos sistemas cerrados están abiertos a un público numeroso que no siempre está necesariamente informado de las normas de cada sistema. Creemos que sería acertado extender el alcance de la Directiva a los sistemas cerrados abiertos al público, sobre todo a los de carácter administrativo.
— Las firmas digitales tienen como función más importante para las políticas de seguridad, la autenticación. Para esta función existen básicamente tres mecanismos de cumplimentación:

  • Lo que el usuario sabe (por lo general, un nombre y una contraseña -password-).
  • Lo que el usuario tiene (una tarjeta inteligente, un certificado digital, un dispositivo en forma de tarjeta que genera un código de acceso diferente cada 60 segundos).
  • Lo que el usuario es (dispositivos biométricos que registran y validan las huellas dactilares, el iris del ojo, etc).

  Los más utilizados hoy en día en Internet, por su simplicidad, son los primeros (nombre de usuario y contraseña). Se considera mucho más seguro una combinación de *saber + tener,* por lo que el uso de las firmas digitales y los servicios de certificación se generalizarán con rapidez, a corto plazo. Pero el tercer tipo de autenticación puede aumentar los niveles de seguridad —también los costes de desarrollo e implementación paralelamente—. Por contra, tiene problemas colaterales delicados, que tienen que ver con aspectos como la intimidad y el uso de datos sensibles especialmente protegidos.
— Creemos que el desarrollo de las tecnologías de firma electrónica para redes abiertas no despegará hasta que haya una masa crítica de usuarios en Internet. El desarrollo del comercio electrónico requiere no sólo vendedores —hay muchos ahora y habrá muchos más a muy corto plazo—, sino compradores. Los compradores, en una relación comercial, necesitan confianza: la seguridad de no ser engañados. Y si lo son, mecanismos eficaces de protección y defensa que los amparen. La legislación europea y de los estados miembros va muy por detrás del mercado. Se necesita una rápida adaptación de la que pueda ser válida y nueva legislación que cubra las necesidades de los nuevos intercambios electrónicos de información.
— Todavía hoy, el comercio en Internet no parece ser seguro. La masa crítica necesaria para su expansión vendrá posibilitada por el establecimiento de tarifas planas para el acceso a la red, por parte de los IPS. Las políticas europeas de telecomunicaciones que abrirán de modo inmediato la competencia en el bucle local de la telefonía convencional, las tecnologías de telefonía móvil —WAP y similares— que potenciarán el uso de Internet por el consumidor final y el desarrollo de tecnologías de servicio de Internet-TV harán posible la aparición de esa masa crítica. Entonces comenzará el desarrollo de los servicios de valor añadido para las tecnologías de firma electrónica.

6.1 Efectos en el campo de la Documentación. Unas consideraciones finales

Las firmas digitales, en el momento en que se haya desarrollado un mercado de servicios de información documental, en el cual el valor añadido - seguridad, autenticación, integridad - en las transacciones realizadas en redes telemáticas sea valorado por los usuarios demandantes, ofrecerán sin duda importantes mejoras en la prestación de servicios documentales, para los profesionales de la Documentación.

A título ilustrativo podemos considerar algunas proyecciones:

— Garantizarán las relaciones comerciales realizadas en transacciones de productos y servicios por empresas documentales que podrán usar la firma digital como prueba de la relación contractual con los usuarios, en caso de litigio ante los tribunales.
— Un profesional de la documentación, como empresario que presta servicios de información documental, podrá constituirse, si así lo desea, en proveedor de servicios de certificación, ofreciendo, por tanto, un servicio con importante valor añadido —cualquier persona física o jurídica podrá prestar dichos servicios, según el art. 1, 4 del R.D.L.14/1999 de Firma Electrónica
— Las firmas digitales permitirán incorporar valor añadido a la prestación de servicios de información y documentación al usuario, proporcionando, por tanto, una variedad y ampliación de la oferta en el canal de distribución de este tipo de servicios, en redes telemáticas.
— Según el nivel de calidad, traducido en niveles de seguridad y fiabilidad para el consumidor del producto o servicio que quiera ofrecer, el prestador deberá cumplir unos requisitos generales [art. 11, R.D.L. 14/1999] o específicos [art. 12] de tal manera que podrá hablarse de proveedores que suministren servicios de certificación ordinaria para firmas electrónicas ordinarias y otros que proporcionarán servicios de certificación *reconocida* para firmas digitales. Estos últimos darán servicios documentales de la máxima calidad y garantizarán al usuario que los documentos firmados digitalmente, que cumplan los requisitos exigidos en el mencionado decreto y avalados por un certificado reconocido, tendrán valor probatorio ante los tribunales en caso de litigio entre partes.

Esta tecnología es una puerta abierta al futuro profesional de la Documentación. Aquellos pioneros que se decidan a cruzar esa frontera tecnológica, podrán aprovechar sus potencialidades. Muy probablemente, a muy corto plazo, se producirá en nuestro país el desarrollo legislativo reglamentario del R.D.L. 14/1999, en aquellos aspectos técnicos que posibilitarán el arranque definitivo del comercio electrónico siempre en paralelo a la evolución en el suministro de banda ancha en Internet, para que la masa crítica de usuarios lo haga viable. Ya se está trabajando en la regulación de este mercado (23). Y en ese mercado, las transacciones con productos y servicios documentales ocuparán una parte fundamental.

Por supuesto, en el mercado de actores privados (empresas documentales) habrá que luchar por establecerse frente a la competencia: nichos, productos segmentados, seguridad, confianza. Luego, se tratará de ganar cuota a los competidores mejorando el producto o servicio.

Y, como se sabe, en Internet, el futuro es casi siempre ahora.

Notas

1. Este estudio es síntesis de otro más extenso que, para ulteriores ampliaciones de información, puede consultarse en el sitio web de la Facultad de Ciencias de la Documentación de la Universidad de Murcia: *La Firma digital en el contexto de la Unión Europea: Regulación, Desarrollo e Implementación,* Facultad de Ciencias de la Documentación, Universidad de Murcia, junio, 2000.

2. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social y al Comité de las Regiones, «Hacia un marco de trabajo para Firmas Digitales y Encriptación», COM(97) 503, 8, octubre, 1997.

3. Cfr. *supra* COM (97) 503, p. 2.

4. Cfr. OECDE, *Guidelines for Cryptography Policy,* 23, 3, 97.

5. Las firmas digitales son firmas electrónicas avanzadas que, además de rubricar un documento procesado por ordenador —firma electrónica—, necesitan de tecnología de encriptación de clave asimétrica para asegurar la autenticación del firmante y la integridad del documento. Para su definición y validez legal en nuestro país, cfr. el R.D. Ley 14/1999 de 17 de septiembre, sobre Firma Electrónica.

6. En inglés, TTPs (*Trusted Third Parties,* es decir, Terceras Partes Confiables).

7. Cfr. R.D.Ley 14/1999 de 17 de septiembre, sobre Firma Electrónica (BOE, 18 de septiembre) que plantea el marco legal para el desarrollo de los sistemas de firma electrónica.

La O.M. 3514, de 21 de febrero de 2000 (BOE , 22 de febrero), desarrolla reglamentariamente el Real Decreto Ley y aprueba el Reglamento de acreditación de prestadores de servicios de certificación y certificación de determinados productos de firma electrónica.

El R.D. 1908/1999 de 17 de diciembre, por el que se regula la contratación telefónica o electrónica con condiciones generales, en desarrollo del artículo 5.3 de la Ley 7/1998, de 13 de abril, de condiciones generales de la contratación (BOE de 31 de diciembre), es interesante a este propósito. Establece el reconocimiento legal de la firma electrónica avanzada, a efectos probatorios, en caso de litigio (art. 5.2).

8. Directiva 1999/CE del Parlamento Europeo y del Consejo por la que se establece un marco conjunto para la Firma Electrónica.

9. Este proyecto, realizado en julio/1998 por un equipo de la Universidad de Zaragoza, dirigido por Fernando Galindo, ha sido de enorme interés para el desarrollo de la infraestructura de firma digital en nuestro país. Los resultados del proyecto se concretaron en:

- — La aplicación AEQUITAS PROCURADORES, desarrollada como prototipo en la transmisión telemática de documentos electrónicos en la Administración de Justicia.
- — El establecimiento del inicio de una red de fiabilidad: FESTE (Fundación para el Estudio de la Seguridad y las Telecomunicaciones)
- — La elaboración del borrador del proyecto de ley española sobre firma electrónica. Estudios preparatorios fundamentales para la publicación final del Real Decreto-Ley 14/1999 de 17 de septiembre, sobre Firma Electrónica (BOE, 18, septiembre),

10. Cfr. *Evaluation of the European Trusted Services Programme,* abril, 6, 1999. Autores: Franz-Peter Heider, Debis IT Security Services, Alemania; Hans Nilsson, iD2 Tecnhologies, Suecia; y Denis Pinkas, Bull, Francia.

11. Directiva 1999/CE del Parlamento Europeo y del Consejo por la que se estable un marco conjunto para la Firma Electrónica, considerandos 7 y 19 (el subrayado es nuestro).

12. *IDA, Legal Aspects of the interchange of data between administrtions, Final Report,* febrero, 1996.

El informe es amplísimo y exhaustivo (consta de 20 páginas de índice). Contiene:1) Descripción de los proyectos IDA. 2) Análisis de los procedimientos. 3) Cuestiones legales en el intercambio de datos entre administraciones. 4) Instrumentos legales para el intercambio normativo. 5) Recomendaciones. 6) Terminología. 7) Bibliografía. 8) Estudio de casos sobre Protección de Datos.

13. Puede consultarse en el sitio web http://www.sgc.mfom.es/sat/interfom.htp

14. Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común, artículos 45, 46.

15. Ley 37/1992, de 28 de diciembre sobre el Valor Añadido, art. 88.2; y Real Decreto 1624/1992 por el que se aprueba el Reglamento sobre el Impuesto del Valor Añadido, art. 9 bis.

16. Orden de 17 de enero de 1994 sobre presentación de solicitudes, afiliaciones y altas y bajas de los trabajadores de la Seguridad Social (BOE, 24 enero 1994); Orden de 3 de abril de 1995, sobre uso de medios electrónicos e informáticos y telemáticos en relación con la inscripción de empresas, afiliación, altas y bajas de trabajadores, cotización y recaudación en el ámbito de la Seguridad Social (BOE, 7 abril 1995); Resolución de 23 de mayo de 1995 por la que se desarrolla la Orden de 3 de abril sobre uso de medios electrónicos (BOE, 7 junio); Resolución de 17 de enero por la que se establecen nuevas medidas de mejora en la gestión de la Seguridad Social y de la atención e información prestada al ciudadano (BOE, 19 enero 1996); Orden de 17 de enero sobre control de accesos al sistema informático de la Seguridad Social (BOE, 25 enero 1996).

17. COM (97) 661 final, Comunicación de la Comisión sobre la Evaluación del Programa IDA y una segunda fase del mismo

18. Cfr. COM (97) 661 final, p. 13 y s.s.

19. Cfr. *La firma digital en el contexto de la Unión Europea: Regulación, Desarrollo e Implementación.* Facultad de Ciencias de la Documentación, Universidad de Murcia.

Del conjunto de acciones, son especialmente destacables la creación de herramientas y técnicas comunes para las distintas aplicaciones. En esta acción se contemplan referencias muy concretas a cuestiones que suponen implícitamente la aplicación de tecnologías de firma digital al intercambio de información administrativa.

20. Dictamen (1999/C 40/10) del Comité Económico y Social sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica, aprobado en Pleno, el 2 diciembre 1998.

21. Dictamen (1999/C 93/06) del Comité de las Regiones sobre la Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para al firma electrónica, aprobado en Pleno, 14 enero 1999

22. Cfr. Erkki Liikanen, Comisario para las empresas y la sociedad de la infor-

mación. *Trust and Security in electronic communications: the european approach.* Discurso pronunciado en Information Security Solutions Europe (ISSE 99), Berlín, 4 octubre 1999. Se puede consultar en:

http:// europa.eu.int/comm/commissioners/liikanen/speeche/051099_en.htm

23. El R.D.L 14/1999, de Firma Electrónica no ha tenido más desarrollo legislativo específico que la O.M 3514/2000 (Reglamento de acreditación de prestadores de servicios de certificación).

La Secretaría de Estado para las Telecomunicaciones y para la Sociedad de la Información del Ministerio de Ciencia y Tecnología está trabajando, en fase muy avanzada, en un anteproyecto de ley (Anteproyecto de Ley de servicios de la sociedad de la información y de comercio electrónico), mediante el cual se incorporará a nuestro ordenamiento jurídico la Directiva 2000/31/CE, de 8 junio 2000, 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 el comercio electrónico).

El anteproyecto de ley tiene por objeto regular el régimen del establecimiento de los prestadores de servicios, de las comunicaciones comerciales, de la contratación por vía electrónica, de la responsabilidad de los prestadores de servicios, incluidos los intermediarios, de los códigos de conducta, de la resolución judicial y extrajudicial de los conflictos y el de infracciones y sanciones.