Capítulo 9.
NORMATIVA LEGAL EN MATERIA DE SEGURIDAD INFORMÁTICA

Autor: Jesús Costas Santos

NORMATIVA LEGAL

Índice de contenidos

NORMATIVA LEGAL

9.1. LEY ORGÁNICA DE PROTECCIÓN DE DATOS (LOPD)

- **Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal** (**LOPD**): Proteger el uso de datos de carácter personal por parte de empresas y profesionales.
- Protección de los datos personales: **derecho fundamental de las personas**.
- La **LOPD obligaciones** destinadas a la protección de los datos personales contenidos en:
  - **ficheros automatizados o informatizados,**
  - **no automatizados o en papel**,
  - Empresas y Administraciones Públicas: gestión de personal, proveedores, clientes, campañas de marketing, etc.
- **Dato de carácter personal**: cualquier información concerniente a personas físicas, identificadas o identificables. información numérica, gráfica, fotográfica, acústica o de cualquier otro tipo susceptible de recogida.

NORMATIVA LEGAL

9.1.2. Agencia Española de Protección de Datos

- Determinados los ficheros de datos de carácter personal: notificación a la Agencia Española de Protección de Datos para su inscripción.
- Las comunidades autónomas de Madrid, Cataluña y País Vasco, poseen agencias propias.
- La Agencia Española de Protección de Datos, en web *www.agpd.es:* **formularios** para la notificación de ficheros, modificación y supresión.
- Para estos 2 últimos procedimientos será necesario contar con el **código de inscripción** ya otorgado.

NORMATIVA LEGAL

9.1.3. Tratamiento de los datos

- La LOPD establece una serie de **limitaciones al tratamiento de los datos.**
- **Voluntad se manifiesta a través del consentimiento.** La **recogida de los datos** es una operación previa al tratamiento.
- En la recogida proporcionar informaciones para que el afectado pueda suministrar o no sus datos con el **pleno conocimiento del alcance del tratamiento que se va a realizar:**
  - El titular del fichero.
  - Las finalidades del tratamiento.
  - El carácter obligatorio de las respuestas.
  - Los derechos y la posibilidad de ejercerlos.
  - La dirección y las condiciones para ejercitar tales derechos.
- El interesado siempre podrá ejercer los derechos que le concede la Ley (impugnación de valoraciones, acceso, rectificación, cancelación y oposición) y **podrá revocar el consentimiento dado**

NORMATIVA LEGAL

9.1.4. Niveles de seguridad

- La Ley establece principios específicos para el **tratamiento de los datos** por parte del responsable del fichero, **para garantizar su correcto tratamiento**, **conservación**, **acceso** y **destrucción**.
- Entre estas medidas: elaboración de **Documento de Seguridad** se detallarán los **datos almacenados**, las **medidas de seguridad adoptadas**, así como las **personas que tienen acceso a esos datos**.
- La ley identifica 3 niveles de **medidas de seguridad:**
  - BÁSICO, MEDIO y ALTO.
- Deberán ser adoptados en función de distintos tipos de datos personales (datos de salud, ideología, religión, creencias, infracciones administrativas, de morosidad, etc.).
- Los niveles de seguridad de forma acumulativa; ej: al nivel de seguridad Medio se aplicarán las medidas de seguridad del nivel Básico.

NORMATIVA LEGAL

9.1.4. Niveles de seguridad: NIVEL BÁSICO

TIPO DE DATOS

Nombre
Apellidos
Direcciones de contacto (tanto físicas como electrónicas)
Teléfono (tanto fijo como móvil)
Otros

MEDIDAS DE SEGURIDAD OBLIGATORIAS

Documento de Seguridad con funciones y obligaciones de cada usuario.
Existirá un responsable de los ficheros de datos personales, que mantendrá una lista con otros usuarios autorizados y sus accesos.
Régimen de funciones y obligaciones del personal: mensaje de inicio de sesión de normas a nivel organizativo.
Registro de incidencias: activación de auditorías o archivos log del sistema como inicios de sesión o acceso a
Identificación y autenticación de usuarios: Medidas de seguridad como complejidad y longitud de contraseñas, cambio de contraseñas periódico, no superior a 1 año.
Control de acceso físico
Gestión de soportes de almacenamiento.
Copias de respaldo y recuperación, al menos 1 vez en semana.

NORMATIVA LEGAL

9.1.4. Niveles de seguridad: NIVEL MEDIO

TIPO DE DATOS	MEDIDAS DE SEGURIDAD OBLIGATORIAS
Comisión infracciones penales Comisión infracciones administrativas Información de Hacienda Pública Información de servicios financieros	Medidas de seguridad de nivel básico Responsable de Seguridad Auditoria bianual Medidas adicionales de Identificación y autenticación de usuarios: evitar cuentas compartidas como p.ej. invitado Control de acceso físico: registro de accesos, tarjeta inteligente, biometría.

NORMATIVA LEGAL

9.1.4. Niveles de seguridad: NIVEL ALTO

TIPO DE DATOS	MEDIDAS DE SEGURIDAD OBLIGATORIAS
Ideología Religión Creencias Origen racial Salud Vida	Medidas de seguridad de nivel básico y medio Seguridad en la distribución de soportes: cifrado, protocolos seguros y certificados digitales. Registro de accesos a los datos, mediante auditoría o logs de acceso. Medidas adicionales de copias de respaldo: copias en ubicaciones diferentes.

NORMATIVA LEGAL

9.1.4. Niveles de seguridad

- El órgano de control del cumplimiento de la normativa: Agencia Española de Protección de Datos (AEPD).
- Las sanciones tienen una elevada cuantía, España el país de UE sanciones más altas.
- Dichas sanciones dependen de la infracción cometida y se dividen en:
  - **Sanciones leves**: **601,01** a **60.101,21 €**
  - **Sanciones graves: 60.101,21** a **300.506,05 €**
  - **Sanciones muy graves: 300.506,05** a **601.012,10 €**

NORMATIVA LEGAL

Índice de contenidos

NORMATIVA LEGAL

9.2. LEY DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN Y DE COMERCIO ELECTRÓNICO (LSSICE)

- **LSSI**, **ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico** (**LSSICE)** objeto: regulación del régimen jurídico de los **servicios de la sociedad de la información y de la contratación por vía electrónica**.
- Entiende por "servicio de la sociedad de la información", toda actividad que:
  - Recibe una contraprestación económica.
  - La actividad se realiza a distancia (no presencial).
  - Por medios electrónicos o telemáticos.
  - A petición individual del destinatario del servicio.
- Siempre que se pueda **percibir un ingreso económico a través de un medio telemático,** como un sitio web, esta actividad entra en ámbito de la Ley.

NORMATIVA LEGAL

9.2.1. Entornos Web

- **Artículo 10.1** de la LSSICE, prestador de servicios estará obligado a disponer de los medios que permitan, tanto a destinatarios como a órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a:
  - **1. Nombre o denominación social; su residencia o domicilio** o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.
  - **2.** Los **datos de su inscripción en el Registro Mercantil**.
  - **3. El número de identificación fiscal** que le corresponda.
  - **4. Precios del servicio**.

NORMATIVA LEGAL

9.2.1. Entornos Web

- Mediante Aviso Legal, Contacto o similar. Proporcionar dicha información en la web.
- Artículo 39, por la comisión de infracciones sanciones:
  - a) Infracciones muy graves:150.001 - 600.000 €.
  - b) Infracciones graves: 30.001 - 150.000€.
  - c) Infracciones leves: hasta 30.000€.

NORMATIVA LEGAL

9.2.2. Comunicaciones comerciales

- Artículos 19 a 22, regula envío de comunicaciones comerciales por vía electrónica:
  - Envío de correos electrónicos
  - Envío SMS-MMS.
- La LSSICE pretende impedir la proliferación del fenómeno conocido como *spam.*
- Para ello exigen requisitos para el envío de comunicaciones comerciales electrónicas y que exista un consentimiento expreso.
- El artículo 21.1 prohíbe el envío de comunicaciones comerciales electrónicas que no hubieran sido previamente solicitadas o autorizadas expresamente por su destinatario (persona física o jurídica).
- Una vez obtenido el consentimiento, el mensaje enviado deberá cumplir:
  - Identificar de forma clara el nombre de la persona física o jurídica en nombre de la que envía el mensaje publicitario.
  - Incluir en el comienzo del mensaje la palabra "*Publicidad*" (en los correos electrónicos) o "*Publi*" (especialmente en los SMS).
  - Facilitar al receptor del mensaje la posibilidad de revocar el consentimiento de una forma sencilla y gratuita.

NORMATIVA LEGAL

9.2.2. Comunicaciones comerciales

- No será necesario el consentimiento previo del receptor del mensaje datos de forma lícita:
  - en el marco de una relación contractual previa
  - comunicaciones sobre productos o servicios similares a los inicialmente adquiridos o contratados
  - propia empresa, organización o profesional.
- La LSSICE artículo 38 infracciones y establece infracción leve: el envío de comunicaciones comerciales sin el cumplimiento de alguno de los requisitos recientemente analizados (sanción hasta 30.000 €).
- 3 o más comunicaciones comerciales a un mismo destinatario en el plazo de un año, sin cumplir con los requisitos establecidos, la infracción pasaría a ser considerada como grave (multa de 30.001 a 150.000 €).

NORMATIVA LEGAL

DIRECCIONES DE INTERÉS

- Sitio web de la agencia española de protección de datos:
  - https://www.agpd.es/
- Web con noticias sobre la LOPD y LSSICE:
  - http://www.leydeprotecciondedatos.com/
- Noticias sobre denuncias de LOPD:
  - http://todonoticiaslopd.com/
- Guía práctica de Microsoft para adaptación a la LOPD:
  - http://www.microsoft.com/business/smb/es-es/guias/lopd/home.mspx
- INTECO – sobre la LSSICE:
  - http://cert.inteco.es/Formacion/Legislacion/Ley_de_Servicios_de_la_Sociedad_de_la_Informacion/
- Página web del Ministerio de Industria, Turismo y Consumo sobre la LSSICE:
  - http://www.mityc.es/dgdsi/lssi/Paginas/Index.aspx
- Preguntas frecuentes o FAQS de la web del Ministerio de Industria, Turismo y Comercio, en relación a la LSSI:
  - http://www.mityc.es/dgdsi/lssi/faqs

NORMATIVA LEGAL

NOTICIAS

- **Muchos bancos incumplen la LOPD en materia de videovigilancia**
  - **Fuente: http://blog.cysia.com/2009/07/la-banca-y-la-lopd/**