LA LEGISLACIÓN SOBRE SEGURIDAD DE DATOS EN INFORMÁTICA DE GESTIÓN. IDEAS PARA UNA GUÍA PARA LA DOCENCIA.

Juan Vicente Oltra Gutiérrez

Escuela Universitaria de Informática
Universidad Politécnica de Valencia
correo-e: jvoltra@omp.upv.es

RESUMEN: En todas las organizaciones empresariales e instituciones públicas existe información de carácter personal, que reside en los sistemas informáticos y recibe un tratamiento automatizado. Esta información, que puede referirse a clientes, empleados, proveedores y colaboradores, está protegida en la legislación española y esto debe formar parte del bagaje de todo futuro profesional informático que pretenda desarrollar su carrera elaborando aplicaciones que manipulen tales datos. En la presente comunicación se presentan ideas para una guía que acerque al alumno la presente legislación, en un marco temporal breve.

1.- INTRODUCCIÓN.

La protección de datos funde el espíritu de protección de las leyes junto con las medidas técnicas y organizativas. Esta aparente *tierra de nadie*, donde ingenieros de organización, abogados e informáticos parecen tener que pugnar, quien tiene la principal competencia es, como veremos en la presente comunicación, el informático, buscando un fin: la humanización de la Informática, la defensa de *la persona*.

A priori parece que el empleo del sentido común aunado con la más elemental deontología profesional bastaría para lograr este fin. No es así[1], al menos en la totalidad de los casos, por lo que el legislador regula aspecto de la informática, ampliando la protección otorgada por la Constitución[2] con otras leyes que la complementan y refuerzan de forma que es obligación tanto ética como legal el cumplirla y hacerla cumplir.

La evolución de la Informática en los últimos años y su integración con las Telecomunicaciones son uno de los fenómenos que más han influido en el vertiginoso cambio social en el que estamos inmersos, con una globalización propiciada por fenómenos como el de Internet.

---

[1] Aparentemente, con la principal Ley al respecto, la Ley de Protección de Datos de Carácter Personal, nos encontramos con una ley que intenta poner *"puertas al campo"*. La expresión *"si no nos detiene la Etica, si al menos el miedo"* sea tal vez el argumento no escrito más expresivo de la citada ley.

[2] Artículo 18.4: *"la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"*.

El crecimiento tecnológico ha permitido que el tratamiento se realice de forma masiva y a grandes velocidades, desde cualquier lugar del planeta[3].

Al desarrollar las leyes de protección de datos a través de los reglamentos definidos aparecen, claramente especificadas, una serie de medidas a adoptar en las organizaciones, bien sean públicas o privadas. Este tipo de medidas son de carácter tanto técnico como organizativo, y no tienen otra misión que garantizar los derechos de las personas de las cuales se poseen los datos. Estas medidas a adoptar implican un conocimiento de la realidad informática de la organización, conocimientos que pertenecen al informático *de carrera,* apoyado en conocimientos de gestión para lograr que la integración de las medidas resulte poco gravoso para la organización y su contexto.

2.- LEGISLACIÓN VIGENTE MÁS RELEVANTE.

Dando complemento a la Ley de Leyes, y apoyada posteriormente por convenios y directivas de la Unión Europea, se desarrolla por primera vez el concepto de *protección de datos*, en la Ley Orgánica 5/1992, de 29 de octubre, donde además se crea un organismo independiente que velará por la aplicación de la ley. Este organismo será la Agencia de Protección de Datos. No será esta la ley definitiva y aparecerá posteriormente la Ley Orgánica 15/1999, de 13 de diciembre, que mejorará la anterior y ampliará el ámbito de la protección no solamente al honor e intimidad sino que incluirá las libertades públicas y derechos fundamentales, utilizando para ello el término "privacidad".

La actividad moderna se ha creado una dependencia de los sistemas informáticos que la hacen vulnerable, por falta de seguridad física, por falta de seguridad lógica y por falta de seguridad jurídica, muchas veces producida, por insuficiencia de medios, o utilización de recursos no apropiados, y es ahí donde los reglamentos que desarrollan las leyes de protección de datos, hacen especial hincapié.

Estos reglamentos desarrollan los documentos de seguridad como la herramienta de trabajo fundamental para la regulación de los sistemas de información y su posterior control como sistemas que cumplen y respetan las leyes y los derechos de las personas a las que pretenden servir, que no controlar. El reglamento por excelencia es el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, del que más adelante nos ocuparemos.

Otra legislación relevante, como apuntábamos, son convenios y directivas de la Unión Europea e instrucciones que ahondan en temas concretos como los servicios de información sobre solvencia patrimonial y crédito, seguros, accesos a edificios... etc.
La que consideramos esencial y que no debe faltar en el bagaje de un Ingeniero Técnico Informático especializado en la creación de aplicaciones de gestión (no olvidemos que la practica mayoría manipulan datos personales) son los apuntados:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Reglamento De Medidas De Seguridad De Los Ficheros Automatizados Que Contengan Datos De Carácter Personal

[3] *"Empieza a no contar el tiempo ni el espacio (...). La Informática (...) puede llegar a convertirse en un instrumento de presión y control de masas"* Manual de Derecho Informático. M.A.Davara Rodriguez. Ed. Aranzadi, 1997, pg.23

3. ASPECTOS BÁSICOS DE LA LEY ORGÁNICA DE PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

Inicialmente se trató de proteger siempre que el tratamiento de los datos fuera susceptible de ser manipulado no solo por personal no autorizado, sino de forma automatizada. Sin embargo, las nuevas Directivas, y en nuestro caso la Ley Orgánica 15/1999 de 13 de diciembre, que sustituye y deroga a la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos de carácter personal) 5/1992 de 29 de octubre, ya hacen hincapié en que no solo se protegerán los ficheros automatizados, sino todos aquellos ficheros con datos de carácter personal y los tratamientos, sean o no automatizados.

Por lo tanto, tenemos por un lado los datos que referencian a personas, por otro lado un tratamiento de dichos datos para generar información que identifique de manera unívoca a las personas, y por último el acceso o utilización fraudulenta de dicha información. Estos elementos son los que nos llevan a la creación del concepto de "protección de datos[4]"

El ámbito de aplicación de la ley son los datos de carácter personal en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado[5].

Hace la Ley especial hincapié, y por tanto es preciso hacer notar esto al alumno, en la seguridad de las instalaciones donde se encuentran los sistemas que almacenan y procesan los datos. Por ello el responsable del fichero y, en su caso, el encargado del tratamiento deberán adoptar las medidas técnicas y organizativas necesarias para[6]:

- garantizar la seguridad de los datos personales
- evitar su alteración, pérdida, tratamiento o acceso no autorizado teniendo en cuenta el estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos.

a) Principios de la protección y momentos del tratamiento de datos.

El discente debe tener presente los principios de la protección de datos, como piedra basal sobre la que asentar el resto de conocimientos. Estos, según el Ministro de Justicia son de tres tipos:

1) principios de carácter general: de proporcionalidad, de vinculación al fin, de exactitud, de transparencia y el secreto del responsable

2) principios singulares: de recogida, de tratamiento y de cesión

---

[4] Se protege a la persona titular y no al dato en sí mismo.

[5] Especialmente se protegen los datos relativos a ideología, religión y creencias, donde nadie puede ser obligado a declarar sobre ello. También se protegen los de afiliación sindical. Todos estos datos se solicitarán con consentimiento expreso y por escrito. Como excepción encontramos los ficheros de partidos políticos, sindicatos, iglesias, asociaciones y fundaciones con finalidad política, filosófica, religiosa o sindical, en cuanto a los datos de sus afiliados o miembros. Los referidos a raza, salud y vida sexual se podrán pedir con consentimiento expreso o si lo marca alguna Ley; y los datos referidos a infracciones solo podrán obtenerse por las Administraciones Públicas competentes ejerciendo sus funciones.

[6] Para ello la Ley se apoya en el Real Decreto 994/1999, sobre medidas de seguridad.

3) principios especiales: afectan a datos sensibles, ideología, religión, creencia, raza, salud y vida sexual.

Estos principios, de cara a articular una docencia coherente, deben completarse con elementos más contrastables dado su perfil, que serían:

Principio de pertinencia de los datos, de acuerdo con el ámbito y la finalidad para las que se hayan obtenido.

Principio de exactitud y actualización, de forma que los datos reflejen con veracidad la situación real del titular, complementados con los principios de congruencia y de racionalidad, en relación a la necesidad de garantizar que los datos no pueden ser tratados, ni utilizado el resultado de su tratamiento en caso de que ya lo hubieran sido, nada más que en aquellos casos en que sea totalmente necesario y adecuado a la finalidad para la que fueron tomados.

Principio de consentimiento[7] del interesado para el tratamiento automatizado.

También resultaría poco coherente no establecer una distinción temporal, según el momento por el que "transitan" esos datos. Los momentos del tratamiento de datos serían:

- La toma de datos
- El tratamiento automatizado de datos, incluyendo el que pueden ser cruzados y relacionados en forma automática junto con otros datos
- La utilización y, si se da el caso, cesión[8] de datos.

b) Derechos de las personas

De igual manera, procede explicar, aun de manera sucinta, al alumno, cuales son los derechos que deben ser respetados:

- Derecho de autodeterminación
- Derecho de información y acceso del titular
- Derechos de rectificación y cancelación
- Derechos de impugnación
- Derecho a exigir responsabilidad por daño
- Otros: consulta al Registro General de protección de datos.

[7] Excepto:
- cuando una Ley lo prevea
- cuando sean datos de fuentes accesibles al público
- cuando exista una libre aceptación de relación jurídica
- cuando los datos se requieran por parte de Fiscales, Tribunales, Defensor del Pueblo, Tribunal de Cuentas y órganos autonómicos con funciones análogas.
- en las actividades propias de las Administraciones Públicas descritas en el artículo 21 de la Ley Orgánica 15/1999.
- en los datos referidos a la salud en caso de urgencias o estudios epidemiológicos.

[8] Las garantías en el caso de cesión, no son necesarias si a los datos se les aplica un proceso de disociación, proceso por el cual los datos no identifican a personas en forma alguna.

Destacando por su singular importancia, los derechos de acceso, rectificación y cancelación.

c) Exclusiones:

Obviamente, interesa delimitar que campo es aquel donde los alumnos tendrán que emplear la legislación, siendo por lo tanto necesario que sepan cuales son las excepciones. Se excluyen del ámbito de aplicación los ficheros personales, de materias clasificadas, sobre investigación del terrorismo y de formas graves de delincuencia organizada -aunque de los cuales se notificará su existencia a la Agencia de Protección de Datos.-

Otros ficheros que se rigen por sus disposiciones específicas son: ficheros electorales, ficheros con fines estadísticos, informes personales de los militares profesionales, el Registro Civil, el Registro Central de Penados y Rebeldes y una novedad con respecto a la anterior Ley, los ficheros de imágenes: la videovigilancia.

4. ASPECTOS BÁSICOS DEL REGLAMENTO DE MEDIDAS DE SEGURIDAD DE LOS FICHEROS AUTOMATIZADOS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL

El cumplimiento del reglamento de seguridad no es tan sólo una obligación legal, sino que, a su vez, redunda en beneficio del informático y de la organización donde desempeña su trabajo, pues genera unas necesidades de organización saludables para la institución en que se aplique.

Los objetivos principales son la confidencialidad de los datos, su integridad y la disponibilidad de los mismos en el ámbito adecuado.

El reglamento de seguridad crea tres niveles de seguridad en función de la información que almacenen los ficheros. Estos tres niveles, denominados básico, medio y alto, podemos desglosarlos de la siguiente manera en una primera aproximación:

- Nivel Básico:
    - Todos los ficheros con datos personales
- Nivel medio:
    - Infracciones Administrativas y Penales
    - Hacienda Pública (Administración Tributaria)
    - Servicios Financieros
    - Evaluación de la personalidad del indivíduo
- Nivel Alto:
    - Ideología[9], Religión y Creencias
    - Origen Racial, Vida Sexual y Salud
    - Policiales

[9] Recordemos que este reglamento apareció para complementar la extinta LORTAD. En ella, los datos sindicales no eran mencionados, no así en la nueva Ley, que los coloca en le rango que merecen, siendo pues de necesaria aplicación en su caso a pesar de no ser expresamente referidos por el reglamento.

Se trata de niveles "envolventes", p.e.: el nivel alto incluye las medidas necesarias para los niveles medio y básico. Dado que las medidas citadas en el nivel básico deberán ser cumplidas siempre, y que estadísticamente, serán estos ficheros los más comunes, parece oportuno centrar la atención del alumno en ellas, sin desdeñar las complementarias para los niveles de seguridad más elevados.

El elemento más importante que aparece es el *documento de seguridad*, que debe mantenerse permanentemente actualizado y revisado siempre y cuando se produzcan cambios relevantes en el sistema de información o en la organización del mismo. En él encontramos información tan significativa como los recursos protegidos, las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido por el reglamento, las funciones y obligaciones del personal, la estructura de los ficheros y la descripción del Sistema de Información, así como los procedimientos de notificación, gestión y respuesta ante las incidencias, y los procedimientos de realización de copias de respaldo[10] y recuperación de los datos.

Como vemos, unos contenidos prolijos[11] que sirven al tiempo de guía para la correcta gestión de los datos.

En el nivel medio resulta destacable la creación de la figura del responsable de seguridad, que por perfil coincide con el responsable de informática o alguien de su equipo. Se hace mención de dos registros: el de incidencias, viejo conocido de los informáticos como cuaderno de bitácora de un S.I. y el novedoso registro de entrada y salida de soportes.

En el nivel alto se observan unas medidas exigidas encaminadas a una intensa actividad controladora de los movimientos de datos.

a) Adaptación al documento de seguridad

Prácticamente todas las medidas que se pueden disponer quedan definidas en el documento de seguridad, sin embargo aparecen al margen de las medidas organizativas y técnicas otras que podríamos denominar *de sentido común*[12] que se solucionan implicandose directamente en la formación de los usuarios.

b) Implantación y su impacto

Se realizará de manera progresiva, yendo del nivel básico a los superiores. De esta manera, los cambios organizativos se verán como algo positivo que no supone apenas esfuerzo llevar a cabo y que sufre evoluciones para mejorar. Se podrían detectar dos niveles de impacto: técnico (donde se precisa el apoyo de los conocimientos de otras asignaturas *tecnológicas*) y personal, donde se puede encontrar ciertas reticencias para colaborar (donde se precisaría ayuda de conocimientos del campo *Comportamiento Organizacional*)

[10] Como dato curioso, el reglamento fija una temporalidad mínima exigible a las copias de seguridad, algo que parece escapar de la *ley* para caer en la *gestión*.
[11] ¡y sólo citamos el nivel básico!
[12] No obtener datos para asuntos particulares, no emplear soportes magnéticos de cuya procedencia no se esté seguro, no hacer mal uso de las aperturas y cierres de sesiones de trabajo...

5. CONCLUSIONES

Hay que tener en cuenta que no sólo los problemas legales y técnicos, sino también organizativos, en cuanto a cambio en la operativa diaria y en la forma de actuar de las organizaciones para cumplir esta legislación.

El alumno no debe infravalorar el impacto de este problema a la hora de establecer prioridades. La realización del diagnóstico de adecuación al mismo conlleva también problemáticas adicionales, con el fin de evitar las sanciones en un entorno tan sujeto a necesidades de gestión de configuración y de gestión del cambio como son los sistemas de información.

6. BIBLIOGRAFÍA

BARRIUSO, C. Interacción del derecho y la informática. Dykinson. Madrid, 1996 ✸ DAVARA, M.A. Manual de derecho informático. Aranzadi. Pamplona, 1997. ✸ GRIMALT, P. La responsabilidad civil en el tratamiento automatizado de datos personales. Comares, Granada, 1999 ✸ Herran, A. La violación de la intimidad en la protección de datos personales. Dykinson. Madrid, 1999 ✸ OLTRA, J.V. Ética e informática, protección de datos y otros aspectos. SPUPV, Valencia 2000; Impacto legal de la informática en las organizaciones. SPUPV, Valencia, 1999 ✸ VVAA. Protección y seguridad de datos (Vol I y II). Cuatrecasas, Madrid 2000