Aspectos prácticos en el cumplimiento de la LOPD

EU Ingeniería Técnica Informática de Oviedo
Universidad de Oviedo
Alejandro Secades Gómez

Aspectos prácticos de la LOPD

- Objetivos:
  - Repasar lo estudiado referente a la aplicación de la LOPD
  - Conocer las prácticas habituales y trucos para facilitar su cumplimiento
  - Profundizar en el papel del Ingeniero (Técnico) Informático a la hora de abordar aspectos de la LOPD
  - Conocer los peligros y situaciones reales de no cumplimiento de la LOPD

1- Identificar ficheros DCP

- Fichero LOPD ≠ Archivo de un FS
- Fichero LOPD ≠ Tabla de BBDD
- Fichero LOPD ≠ Instancia o esquema de BBDD
- ¿Qué es un fichero LOPD?
  - Un conjunto lógico de datos
  - La estructura interna, e incluso la relaci´no entre datos no es determinante → lo único importante es que contenga DCP
  - Podemos identificar un fichero como queramos

1- Identificar ficheros DCP

- ¿Qué podemos hacer en la práctica para facilitarnos el trabajo?
  - Agrupar varios o todos los sistemas de la empresa en un solo fichero con DCP
    - Evitamos repetir trámites, documetnación y burocracia
  - Partir un sistema en varios ficheros DCP
    - Puede servir para aislar DCP de nivel alto → así sólo habrá que cumplir las medidas de nivel alto en parte del sistema → ahorro de esfuerzo, tiempo y dinero, especialmetne cuando hay que adecuar un sistema existente a la LOPD

2- Identificar el nivel de los DCP

- No siempre es evidente a qué nivel asignar ciertos DCP
  - La AEPD tiene un servicio de consulta gratuito
  - Funciona mejor por correo postal que por email
  - Veremos algunos casos concretos
- Personas jurídicas: ¿Afectadas por la LOPD?
  - La LOPD sólo afecta a personas físicas, no jurídicas (empresas)
  - Sin embargo, cualquier fichero con personas jurídicas podría contener autónomos → Son también personas físicas
  - Conclusión: como norma general, un registro de empresas (proveedores, clientes, etc.), se ve afectado por la LOPD

2- Identificar el nivel de los DCP

- Caso real: listas de correo en una web, para dar noticias (lista de suscripción)
  - ¿Una dirección email es un DCP? → aparentemente una cuenta de correo no dice nada de la persona que la posee, si es una persona (p.e. aabbzz88@hotmail.com, o info@miempresa.es)
  - Dictamen de la AEPD:
    - Una dirección de email puede aportar información identificativa sobre una persona (p.e., alex.secades@uniovi.es da el nombre de una persona y su vinculación a uniovi)
    - Si puede haber información personal, entonces estará afectada por la LOPD, como mínimo con nivel básico de datos
    - Conclusión: si montamos una web que incluya listas de distribución, hay que declarar un fichero de nivel básico a la AEPD (igual conviene más olvidarnos de la lista de distribución…)

2- Identificar el nivel de los DCP

- Aplicaciones de nómina
  - Información identificativa de personas: nombre, apellidos → nivel básico
  - Información financiera: sueldo, retenciones de un juzgado, etc. → nivel medio
  - Problemas:
    - La nómina recoge información de cuotas sindicales (se descuentan de la paga)
    - La nómina recoge informacio´n sobre si un trabajador es minusválido (cálculo de retenciones, subvenciones a la empresa…)
  - Conclusión: una nómina tiene DCP de nivel alto
    - Problema: aplicar el reglamento de medidas a datos de nivel alto es costoso, sobre todo si es un sistema ya construido
    - Posible solución: declarar dos ficheros, uno de nivel medio y el otro sólo con la información de nivel alto → se aplican las medidas sólo a la parte del sistema correspondiente

2- Identificar el nivel de los DCP

- Algunas cosas curiosas
  - Un dictamen judicial que condene a alguien por asesinato es de nivel medio
    - Pagar una cuota sindical o padecer de hipertensión es de nivel alto → ¿no parece incongruente? (las leyes las hacen abogados…☺)
    - Caso real de ejecución de sentencias penales por parte de menores
  - Información aparentemente inconexa que permita hacer un seguimiento de aficiones, compras, etc., es de nivel medio
    - Los accesos a internet de una persona podrían considerarse de nivel medio

2- Identificar el nivel de los DCP

- Páginas amarillas y operadoras de telecomunicaciones
  - Las páginas amarillas contienen DCP de nivel básico
  - Hay filiales de las operadoras de telecomunicaciones que proporcionan información a empresas de publicidad
    - Quiero un listado de personas que vivan en tal zona, con determinado nivel de vida, … → contestan con un "sublistado" de las páginas amarillas ¿QUÉ NIVEL TIENEN LOS DATOS DE ESE LISTADO?
    - Según la AEPD esos datos son de nivel medio, y se entregaban sin consentimiento del usuario → multa a la operadora
      - La operadora ganaba con ese negocio mucho más dinero que lo que suponía la multa, por lo que la pagaba sin más

3- El documento de seguridad

- Aparentemente no sirve para nada, de hecho casi nadie lo lee, y suele ser una plantilla
- Sin embargo es lo primero que se solicita en una auditoría LOPD, y no tener actualizado es una falta
- Por otra parte, lo que exige la LOPD al documento de seguridad es bien sencillo
- ¿Cómo mantener un documento de seguridad para cada fichero con DCP de nuestra empresa?

3- El documento de seguridad

- Prácticas habituales en el mundo real
  - Un documento de seguridad genérico para todos los ficheros de la empresa
    - Al final y como anexos, añadimos los datos específicos de cada fichero (nombre, nivel, descripción…)
    - Hay plantillas disponibles en la web
  - El documento de seguridad no contiene normas técnicas ni organizativas detalladas, sino referencias a dichas normas, mantenidas aparte
    - Así el documento de seguridad no cambia, no hay que actualizarlo cada poco
    - En las normas concretas se incluyen las medidas de nivel básico y medio para todos los sistemas, y cuando sea preciso, las de nivel alto
    - Así el responsable de seguridad se quita el "muerto" de encima → mantener las normas técnicas acordes a la LOPD será tarea del área de Sistemas

4- Normas de seguridad

- Las normas y procedimientos de seguridad deben recoger las medidas del RMS
  - ¿Existen normas y procedimientos de seguridad?
- Las normas deben ser lo menos dependientes posible de la tecnología
- Hay que hacer especial hincapié en las normas no técnicas
  - Registro de E/S de soportes (p.e. CD-ROM, cinta de backup): basta un folio escrito a mano… no hace falta una consultora con una aplicación J2EE ☺
- Mantener un backup en un lugar diferente al CPD
  - Legalmente no se indica a qué distancia debe custodiarse la copia de seguridad
  - Lo razonable es que sea en otro edificio (se suele hablar de varios km)
  - Hay empresas dedicadas a la custodia de soportes magnéticos
- Contraseñas almacenadas de forma ininteligible (art. 11)
  - En muchas aplicaciones modernas, sobre todo web, se almacenan las passwords sin cifrar o con cifrado simple y reversible → incumplimiento

4- Normas de seguridad

- Caducidad de las contraseñas
  - No se especifica cada cuánto, y si debe ser automática o manual → no nos compliquemos
  - Cuentas compartidas
    - Se permiten con DCP de nivel básico, aunque no son recomendables (¿root en UNIX?)
  - Control de intentos fallidos de login
    - ¿Cómo lo controlamos en una aplicación web sin permitir ataques DoS?
  - Bases de Datos de pruebas: lo mejor es no usar datos reales
    - Con datos reales habría que aplicar el reglamento de medidas al entorno de pruebas → costoso
    - Solución: se pueden ofuscar los datos
  - Telecomunicaciones (art. 5 y 26 del RMS) ¿qué son ?
    - Dictamen de la AEPD: cuando impliquen a un operador externo (ADSL, Frame-Relay, ATM…). Una red local no estará afectada

5- Derechos y deberes

- Personal que maneja el fichero con DCP
  - Debería firmar una cláusula en su contrato aceptando cumplir el documento de seguridad (cláusula genérica)
  - El documento de seguridad y las normas y procedimientos deben ser conocidas por el personal
    - Si no es así, la empresa sería culpable de un mal uso de los datos por parte de éstos
    - Lo mejor es hacer firmar a la gente un "recibo" de que se le han comunicado sus deberes respecto al uso de DCP

5- Derechos y deberes

- Derechos de los usuarios cutos datos manejamos
  - Importante: hay un plazo para responder a sus peticiones de acceso, rectificación, oposición y cancelación (10 días, art. 16)
    - "Timo" legal: hacer petición de cancelación o rectificación y denunciar a la empresa cuando pase el plazo
  - Hay que informar al usuario cuando se recojan sus datos, sea como sea

6- Responsable de seguridad

- Papel del responsable de seguridad
  - Implantar y vigilar las medidas de seguridad, siguiendo órdenes del responsable de fichero
  - Informar al responsable de fichero de posibles problemas
  - Suele ser el "informático" de la empresa (vosotros) → ¡Pedid aumento de sueldo si os toca ☺!
- ¿Qué responsabilidad real tiene?
  - Ante la LOPD, ninguna en especial → el responsable legal siemrpe es el de fichero
  - Situación habitual: el responsable de fichero "pasa" de la LOPD y le pasa el muerto al de seguridad
  - Es muy importante que le responsable de seguridad documente por escrito cualquier problema y lo notifique con acuse de recibo
    - Esos informes se pasarán a la AEPD si hay problemas
    - Así el responsable de fichero no tendrá excusas
    - El responsable de fichero es quien debe asumir y responder de incumplimientos, nuestro trabajo sería tener informado de qué problemas hay y cómo solucionarlos. Si al final el responsable de fichero no quiere remediar los fallos será problema suto (situación de "asumir" el riesgo)

7- Responsable de fichero

- No tiene por qué ser una persona física
  - Si ponemos a una persona física, cada vez que cambie habrá que declararlo a la AEPD
  - Lo mejor es poner un cargo
  - Realmente le responsable de fichero en una empresa sería el dueño (director general, consejo de administración…)
- Es el verdadero responsable de que se cumpla la LOPD

8- Declaración a la AEPD

- Hay APD automómicas (Madrid, Cataluña, Valencia, País Vasco…)
  - Sólo tienen competencias para ficheros de titularidad pública (CC.AA. O Admon. Local) → hay normas especiales para ficheros de AAPP (p.e. publicar una resolución en el Boletín Oficial para crear un fichero…)
  - Para ficheros de titularidad privada, hay que ir a la AEPD
- En la web de la AEPD hay plantillas en PDF, y una aplicación Access para generar la documentación a enviar
  - Se puede inscribir un fichero por correo postal o vía web

9- Auditorías

- La auditoría LOPD no tiene por qué ser externa
  - Si la hacéis para vuestra empresa, se ahorrará un dinero, basta que quede documentada
- Al final, ¿en qué consiste un auditoría LOPD?
  1. Comprobar si están inscritos correctamente todos los ficheros
  2. Comprobar la documentación LOPD y si es correcta
  3. Comprobar si lo que dice la documentación es cierto
  - En la práctica, cualquier "currito" con una plantilla Word/Excel con preguntas y "huecos" para las respuestas puede hacer auditorías LOPD → muchas veces lo hacen licenciados en derecho o económicas, sin conocimientos técnicos… ☹

10- Cuestiones finales

- Para 2008, se esperan cambios legales que obliguen a aplicar la LOPD a ficheros en "papel", aparte de los informáticos
- Hay mucho trabajo en temas LOPD, perop lo suelen copar licenciados en derecho y consultoras
  - Los Ingenieros (Técnicos) en Informática deberíamos implicarnos más en estos temas → perdamos el miedo a la legislación, en realidad ni los propios abogados la entienden de veras… ☺