

Un repaso a la Ley orgánica de protección de datos (LOPD)

Juan Carlos Rodríguez. | Economista de ECU Asesores y Mercedes Mazo, Empresistas de ECU Asesores.

Aunque se avanza poco a poco en el conocimiento general de la “LOPD” (Ley Orgánica de Protección de Datos), vamos a intentar, aportar algo más de información.

En principio y según el informe estadístico de la Cámara de Comercio de Cantabria, se observa que el número de empresas existentes en la provincia es de alrededor de 47.000. Ahora bien, si atendemos al informe presentado por la Agencia Española de Protección de Datos, hay inscritos ficheros de un total de 4.781 entidades.

Es por lo tanto necesario hacer un paréntesis y analizar si realmente el 90 % de las empresas cántabras no manejan ficheros con datos personales susceptibles de ser inscritos en dicha Agencia o si, por el contrario, desconocen la responsabilidad de su uso.

Diremos que un dato de carácter personal es cualquier información concerniente a persona física identificada o identificable, mientras que se entiende por fichero de datos personales todo conjunto organizado de datos de carácter personal, cualquiera que fuere la norma o modalidad de su creación, almacenamiento, organización y acceso.

El tratamiento de datos consiste en las operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones que resulten de comunicaciones, consultas, interconexiones y transferencias.

La Ley regula el tratamiento de los datos y ficheros de carácter personal, independientemente del soporte en el cual sean tratados los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan.

El principio básico de la LOPD se fundamenta en la obligación por parte de los responsables del fichero a que todas sus bases de datos cumplan con el principio de calidad de los mismos, deber de información en la recogida informando al titular de la existencia del

fichero y de los destinos de la información, la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición y garantizar y proteger el tratamiento de los datos personales.

Del mismo modo, el Reglamento desarrolla las medidas que debemos emplear para su correcta implantación; se establecen las sanciones con las que se nos penalizará en caso de la utilización indebida, e igualmente se establece la cuantificación de dichas sanciones.

El propio Reglamento excluye, además de los tratamientos de datos de las personas jurídicas, datos de las personas físicas que prestan sus servicios en ellas, consistentes únicamente en su nombre, apellidos, funciones o puestos desempeñados, dirección y teléfono. Tampoco incluye los datos relativos a empresarios individuales, cuando hagan referencia a su calidad de comerciantes, industriales o navieros. Sin embargo, sí quedan protegidos los profesionales liberales individuales.

Adaptar una empresa a la LOPD no es solamente un proyecto informático, como algunos creen, sino que la parte más compleja del proyecto se encuentra en la modificación de los procedimientos de trabajo, como veremos más adelante y a los cambios a introducir orientados a garantizar la seguridad legal de la organización, así como la puesta en marcha de las medidas legales. Será necesario aplicar una metodología de análisis, evaluación de la situación y adecuación con respecto a la normativa que nos permitirá establecer los elementos para alcanzar una cultura de la seguridad y una excelencia en el tratamiento de la información en todos los procesos de nuestro despacho.

Hay que recordar que el día 20 de abril de 2008, entró en vigor el Real Decreto 1720/2007 de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999 de 13 de diciembre, de protección de datos de carácter personal (LOPD).

Se establecen tres tipos de ficheros y, en función de los datos y como consecuencia de las

medidas de seguridad a aplicar, serán establecidos los niveles de seguridad:

-Nivel Básico: nombre, apellidos, datos de contacto (dirección, teléfono, e-mail) Cualquier otro dato que no sea de nivel medio o alto.

-Nivel Medio: datos relativos a la comisión de infracciones administrativas o penales. Datos cuyos responsables sean las Agencias tributarias o datos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social. Datos que ofrezcan una definición de las características o personalidad de los ciudadanos y permitan evaluar aspectos de su personalidad o comportamiento. Datos de los que sean responsables las entidades financieras, etc.

-Nivel Alto: ideología. Afiliación sindical. Religión y creencias. Origen racial, Salud y vida sexual. Datos recabados para fines policiales sin consentimiento de las personas afectadas. Datos derivados de la violencia de género, etc.

El proceso de implantación de la normativa sobre protección de datos podríamos resumirla en tres fases:

- Adaptación de ficheros en la cual se identifican los ficheros y se notifican al RCPD.

- Legitimación de datos, que supone la recogida de información, el consentimiento del afectado y el cumplimiento de la normativa referente a los derechos del ciudadano: acceso, rectificación, cancelación, oposición.

- Políticas de seguridad de datos, elaborar el documento de seguridad, nombrar responsable de seguridad, aplicar medidas de seguridad: básico, medio o alto, según proceda.

Las medidas a tomar por los responsables de los ficheros tanto en soporte físico como automatizados son:

- Elaborar el Documento de Seguridad.
- Fijar un responsable de seguridad.
- Divulgar la normativa de seguridad al personal.
- Detallar el procedimiento de notificación gestión y respuesta ante las incidencias.
- Especificar y documentar los procedimientos de control de acceso.
- Establecer mecanismos de identificación y autenticación.
- Concretar el procedimiento y gestión de soportes.
- Disponer de copias de seguridad.
- Delimitar normas de archivo.
- Establecer dispositivos de almacenamiento válidos.
- Guardar los soportes.
- Precisar los procedimientos de copia y reproducción de documentos.
- Cifrar las comunicaciones.
- Establecer mecanismos de control en el traslado de documentación
- Realización de auditorías.

- Inscripción de ficheros en el Registro General de Protección de datos.
- Información y obtención del consentimiento sobre el tratamiento.
- Guardar secreto.
- Redactar Documento de Seguridad

Tengamos en cuenta los plazos para su implantación y adaptación de los ficheros existentes.

Todos los ficheros, tanto automatizados como no automatizados, creados a partir del 20 de abril de 2008, deberán tener implantadas desde el momento de su creación la totalidad de las medidas de seguridad que les correspondan por sus características. Así mismo, antes de crearse de modo efectivo los ficheros, deben comunicarse a la Agencia Española de Protección de datos.

El 20 de abril de 2009, deberán estar adaptados a las medidas de seguridad que les co-

rrespondan, los ficheros tanto automatizados como no automatizados de nivel básico y los ficheros automatizados de nivel medio.

El 20 de octubre de 2009, los no automatizados de nivel alto y los automatizados de nivel medio.

Y el 20 de abril de 2010, los automatizados de nivel alto.

¿Dónde están los peligros?

Una pérdida de datos por cualquier motivo como robo, inundación, incendio, avería informática, puede generar graves pérdidas en nuestra empresa y además estar sujeta a una sanción por parte de La Agencia Española de Protección de Datos dependiendo de los daños causados con dicha pérdida.

¿Qué tipos de datos manejamos y cuál es la forma adecuada de protegerlos?

- Soporte en papel:

La mayoría de las empresas maneja una cantidad importante de papel con información de todo tipo y es por ello muy fácil cometer un error con un papel o documento descuidado, sin archivar o destruir correctamente.

El Reglamento anterior no contemplaba los ficheros en papel y, por tanto, no establecía ninguna medida de seguridad específica, por lo que de algún modo parecía coherente pensar que se debían usar las mismas que en los ficheros informáticos.

Los ficheros en papel debían igualmente inscribirse en el Registro General de Protección de Datos y además debían respetarse los derechos de los interesados.

A estas alturas, todos conocemos el modo en que deben archivar, si debemos tenerlos en sitio cerrado bajo llave y el número de personas que puede acceder a él.

Aún así el hecho frecuente de que cualquier documento quede encima de una mesa a la hora del café o por la noche, que la persona de la limpieza acceda sin ningún problema o quede en la papelera sin destruir, son conductas habituales que implican mucho riesgo.

No conviene olvidar que la inmensa mayoría de las inspecciones de la Agencia de Protección de Datos es por incumplimiento de la ley en cuanto a soportes en papel.



Las medidas de seguridad para este tipo de ficheros hacen referencia al archivo, almacenamiento, custodia de los soportes, acceso a ellos, copia y traslado de los documentos. Los documentos de nivel Medio y Alto requieren de Auditoria cada 2 años.

Las empresas aparentemente nos preocupamos mucho por el aspecto tecnológico de la protección de datos, pero ¿somos conscientes de la facilidad de transmisión de datos que nos facilitan los equipos informáticos y, sobre todo, por Internet?, ¿qué tenemos en nuestro PC? ¿en nuestro portátil? ¿en nuestra PDA o simplemente en nuestra agenda del teléfono? No todos los usuarios de Internet saben que al navegar en la red se deja un rastro, y menos aún son conscientes del alcance que dicho rastro puede llegar a tener.

El nuevo Reglamento establece el uso de contraseñas individualizadas en los ficheros informáticos, incluso en los de nivel Básico, medidas sobre destrucción o borrado de documentos, pruebas antes de implantar los programas, etc.

Mediante una entrevista realizada en estos días al director de la Agencia Española de Protección de Datos (AEPD), se transmitió que los navegantes saben que pueden encontrarse peligros que conllevan el intercambio de información, sobre todo cuando utilizan las nuevas tecnologías como Internet. Lo que no se conoce es el alcance de esos rastros y el que pueden ejercer determinados derechos para cancelar esa información.

En el procedimiento sancionador PS/00317/2007, instruido por la Agencia Española de Protección de Datos a D. X.X.X., vista la denuncia presentada por el CONCELLO DE OURENSE - POLICIA LOCAL, se repite la historia de los archivos con datos personales que aparecen en las redes P2P como el e-Mule.

En este caso se trata de un abogado al que se le "escapó" un archivo con datos de más de 1500 clientes. Según manifestó "en modo alguno ha existido voluntariedad en cuanto a tal compartición. En efecto, dicha base de datos, -una copia antigua de la que utiliza el despacho-, era utilizada por el personal del despacho como "agenda" para la remisión de la correspondencia usual del despacho y, por error humano, debido a la escasez de conocimientos informáticos del usuario y al parecer en un movimiento de "arrastrar y copiar", fue copiada en una carpeta temporal que se encontraba en otra que a su vez era compartida por el programa P2P. Es de decir que inmediatamente que se tuvo conocimiento de esta circunstancia fue subsanado el error."

El Director de la Agencia Española de Protección de Datos RESUELVE IMPONER a D. X.X.X., por una infracción del artículo 9 de la LOPD, tipificada como grave en el artículo 44.3.h) de dicha norma, una multa de 3.000 (tres mil euros) de conformidad con lo establecido en el artículo 45.2 y 5 de la citada Ley Orgánica.

La Agencia Española de Protección de Datos en los últimos años ha interpuesto un gran

número de sanciones y multas, las cuales han sido muy superiores a las de los países europeos del entorno.

Otro punto importante es la Cesión de Datos para su tratamiento.

En este momento, en el que los profesionales del asesoramiento de empresas nos inclinamos por la colaboración y subcontratación de otros profesionales, no debemos olvidar que esta circunstancia también viene regulada en la LOPD, mediante un contrato de cesión de datos a un Encargado de Tratamiento.

Recordemos que se puede dar el caso de que en nuestros despachos cumplamos perfectamente con los requisitos a los que obliga la ley en cuanto a medidas técnicas, jurídicas y organizativas, pero obviemos el contrato de cesión de datos con aquel que es colaborador del nuestro. El mal uso por parte de este otro despacho hará recaer en nosotros, como Responsables del Fichero, las sanciones que la AGEPD estime oportunas.

Visto lo visto, como es posible que una gran mayoría de los que estén obligados a cumplir esta normativa, no tengan, por lo menos su Documento de Seguridad y los Ficheros inscritos en la AGEPD.

Hagamos un pequeño recordatorio al montante de las sanciones:

No inscribir los ficheros o simplemente por estar en la situación anterior, somos candidatos nosotros mismos, como Responsables del Fichero, a recibir una sanción leve de 6.000 € a 60.000 €.

Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen, se considera infracción grave, que va de 60.000 € a 300.000 €.

Las sanciones correspondientes a faltas muy graves, como puede ser el de comunicar o ceder datos fuera de los casos permitidos, puede llegar a costarnos hasta 601.012 €.



Pregunte al autor:
¿Desea formular alguna pregunta al autor de este artículo? dirijase a: lagaceta@empresistascantabria.es y publicaremos la respuesta en www.empresistascantabria.es