¿LAS EMPRESAS GALLEGAS INCORPORAN EN SU GESTIÓN EL CUMPLIMIENTO DE LA PROTECCIÓN DE DATOS?

Manuel Martínez Carballo (mmarcar@uvigo.es)
Mª Cruz del Río Rama (delrio@uvigo.es)
Dpto. de Organización de Empresas y Marketing
Universidade de Vigo

Eduardo Guillén Solórzano (edugs@udc.es)
Susana Barbeito Roibal (sbar@cdf.udc.es)
Dpto. de Análisis Económico y Administración de Empresas
Universidade da Coruña

RESUMEN

En este artículo lo que pretendemos es dar respuesta al título planteado para el trabajo, analizando el grado o nivel de cumplimiento por parte de las empresas gallegas de la legislación en materia de protección de datos, ya que, aunque realmente parece un tema de actualidad, la verdad es que ya aparece como una exigencia en nuestra Constitución Española de 1978 que posteriormente se regula específicamente por primera vez en nuestro país en la década de los noventa y más concretamente a finales del año 1992, a través de la Ley Orgánica 5/1992 derogada actualmente por la Ley 15/1999.

La seguridad de la información es algo que cada vez comprobamos que es más importante y que su necesidad crece de forma exponencial. Si queremos que la sociedad de la información sea una realidad la seguridad quizá sea una de las bazas más importantes que hay que solucionar.

INTRODUCCIÓN

En la actualidad, todavía nos encontramos en pleno proceso de globalización de la economía en la que no debemos olvidarnos de la evolución que han tenido en los últimos años las Tecnologías de la Información y de la Comunicación (TIC).

Cada vez un mayor número de organizaciones considera que la información y la tecnología asociada a ella representan sus activos más importantes que significan su principal ventaja estratégica y, de igual modo que se exige para los otros activos de la empresa, los requerimientos de calidad y seguridad, en este caso son indispensables.

En este sentido, la informática produce grandes beneficios a las empresas pero también puede causar importantes problemas, ya que, es posible que los datos de carácter personal de sus empleados, clientes, proveedores, … estén informatizados sin el consentimiento de los mismos, o bien que sean erróneos o estén sin actualizar. Por otro lado, puede suceder que accedan a estos datos personas no autorizadas, por lo tanto, su intimidad o su vida privada pueden verse afectadas.

Por ello, ante el peligro que suponen los hechos anteriores se hace necesario para garantizar el equilibrio entre modernización (desarrollo y aplicación de nuevas tecnologías en el intercambio de datos) y garantía de los derechos de los ciudadanos, la normalización de la protección de datos de carácter personal, derecho fundamental recogido en la Constitución que atribuye a los ciudadanos la facultad de controlar sus datos personales y decidir sobre los mismos.

De los preceptos recogidos en la Constitución Española, el artículo 10 en el que "*se reconoce el derecho a la dignidad de la persona"* y el artículo 18.4 que dispone que "*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*", se deriva el derecho fundamental a la protección de datos de carácter personal recogido por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). En este sentido, la LOPD garantiza y protege, lo referente al tratamiento de datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.

Por otro lado, la Constitución Europea ha recogido expresamente el derecho fundamental a la protección de datos en dos ocasiones, y exige que en todos los Estados miembros exista una autoridad independiente que controle y garantice el derecho fundamental a la protección de datos.

La protección de datos está regulada actualmente en España por una Ley Orgánica del año 1999, según la cual todos los datos referidos a clientes que estén en posesión de una empresa pasan a ser confidenciales y no pueden ser utilizados sin consentimiento; además, las compañías deben

establecer mecanismos de seguridad que garanticen que estos ficheros están fuera del alcance de terceros. Sin embargo, un informe de año 2004 publicado por dos consultoras revelaba que el 47% de las empresas españolas reconocen que sus bases de datos son ilegales y muchas de las que afirman cumplir la ley siguen prácticas no autorizadas.

En España, el ente público que vela por el cumplimiento de la normativa es La Agencia Española de Protección de Datos[1], actuando para ello con plena independencia de las Administraciones Públicas. En este sentido, con el propósito de proteger de los derechos del ciudadano se encarga de *informar* sobre el contenido, los principios y las garantías del derecho fundamental a la protección de datos regulado en la LOPD; *ayuda* al ciudadano a ejercitar sus derechos y a los responsables y encargados de tratamientos a cumplir las obligaciones que establece la ley; *tutela* al ciudadano en el ejercicio de los derechos de acceso, rectificación, cancelación y oposición cuando no han sido adecuadamente atendidos por los responsables de los ficheros; y por último, *garantiza* el derecho a la protección de datos investigando aquellas actuaciones de los responsables o encargados de ficheros que puedan ser contrarias a los principios y garantías contenidos en la LOPD, e impone, en su caso la correspondiente sanción.

El estudio comprendería, en un primer lugar, un análisis detallado de los principales aspectos de la legislación en materia de protección de datos. En un segundo punto, se analizaría el cumplimiento de esta materia en el conjunto global de nuestro país para centrarnos más concretamente en nuestra Comunidad Autónoma con un desglose para las cuatro provincias gallegas. Finalmente, el trabajo concluiría con una serie de conclusiones y/o recomendaciones a las empresas del ámbito gallego para motivar o concienciarlas hacia un mayor cumplimiento de la normativa en protección de datos.

MARCO JURÍDICO Y ASPECTOS MÁS RELEVANTES

El escenario normativo con el que opera la Agencia Española de Protección de datos se encuentra definido por la Ley Orgánica 15/1999, de protección de Datos de Carácter Personal, junto con la Directiva 95/46/CE del Parlamento Europeo y del Consejo; relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos. Asimismo, este marco jurídico proporcionado por la Ley Orgánica se ve complementado por diversas normas generales o sectoriales, de diverso rango normativo, que conforman el conjunto legal aplicable (ver tabla 1).

[1] El Capítulo VI, a través de los artículos 35-42, de la Ley Orgánica 15/1999 está dedicado al estudio de la Agencia de Protección de datos.

Tabla 1: Normas Generales o Sectoriales

Las que se refieren a las nuevas competencias
• Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones (art. 58,b) en relación a los arts. 53,z y 54,r. • Ley 59/2003, de 19 de diciembre, de firma Electrónica que, en su disposición adicional octava, modificó el art. 43,1 de la ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y del Comercio Electrónico.
Las que se refiere a la propia Agencia Española de Protección de Datos
Ley 62/2003 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social (artículo82).
Las normas que afectan a sectores concretos, resaltando por su importancia las ss.
• Ley Orgánica 4/2003, de 21 de mayo, que complementa la Ley de prevención y bloqueo de la financiación del terrorismo, que modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, y la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa. • Ley Orgánica 14/2003, de 20 de noviembre, de reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social, modificada por la Ley Orgánica 8/2000, de 22 de diciembre, de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local, de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, y de la Ley 3/1991, de 10 de enero, de Competencia Desleal. • Ley Orgánica 19/2003, de 23 de diciembre, que modifica la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. • Ley 12/2003, de 21 de mayo, de prevención y bloqueo de la financiación del terrorismo. • Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud. • Ley 34/2003, de 4 de noviembre, de modificación y adaptación a la normativa comunitaria de la legislación de seguros privados. • Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias. • Ley 45/2003, de 21 de noviembre, que modifica la Ley 35/1988 sobre técnicas de reproducción asistida. • Ley 57/2003, de 16 de diciembre, sobre medidas para la modernización del gobierno local. • Ley 58/2003, de 17 de diciembre, General Tributaria. • Real Decreto 209/2003, de 21 de febrero, que regula los registros y las notificaciones telemáticas, sí como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos. • El Real Decreto Legislativo 2/2004, de 5 de marzo, por el que se aprueba el texto refundido de la Ley Reguladora de las Haciendas Locales. • El Real Decreto Legislativo 6/2004, de 29 de octubre, por el que se aprueba el texto refundido de la Ley de ordenación y supervisión de los seguros privados. • El Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria privada. • El Real Decreto 2393/2004, de 30 de diciembre, por el que se aprueba el Reglamento de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social.

Fuente: Agencia Española de Protección de datos.

Por lo tanto, vemos que existe una legislación muy reciente elaborada a partir de las bases y preceptos legislativos aparecidos principalmente en los años 1992 (Ley Orgánica 5/1992 derogada por la nueva ley) y 1994 (Real Decreto 1332/1994, desarrollo reglamentario de la Ley Orgánica 1992), en la que el eje central es La Agencia de Protección de Datos que se configura como el órgano de control del cumplimiento de la Ley.

En el presente apartado pretendemos analizar aquellos aspectos más relevantes obtenidos al realizar un estudio más exhaustivo de la normativa vigente.

Principios de protección de datos. Según la nueva ley el tratamiento de datos de carácter personal ha de realizarse de acuerdo con los principios de información, calidad, finalidad, consentimiento y seguridad, de forma que todo responsable de un fichero o tratamiento de datos personales está obligado a cumplir estos principios recogidos en la LOPD. Siguiendo estos principios, los datos deben tratarse de manera leal y lícita y deben recogerse con fines determinados, explícitos y legítimos. Asimismo, los datos deben ser exactos y mantenerse actualizados de manera que respondan con veracidad a la situación actual de sus titular y serán conservados sólo durante el tiempo necesario para las finalidades para el que han sido recogidos. Y por último, todo responsable o encargado de un tratamiento de datos tienen que adoptar todas las medidas necesarias para garantizar la seguridad de los datos personales e impedir cualquier alteración, perdida, tratamiento o acceso no autorizado.

La empresa que contenga ficheros[2] *de carácter personal ha de inscribir los mismos en el Registro General de Protección de Datos, al mismo tiempo que éste les da publicidad.* Hay que distinguir que existen ficheros de titularidad pública y privada. En ambos casos se debe seguir el proceso de notificación e inscripción en el Registro siguiendo los tramites recogidos en la ley.

Toda empresa que tenga inscrito o no los ficheros podrá ser inspeccionada por la Inspección de Datos, pudiendo en base a esa inspección ser sancionada por el Director de la Agencia o serle inmovilizados los ficheros. Por lo tanto, la empresa puede ser sancionada por infracciones leves[3] cuya sanción va de 600 a 60.000 euros; infracción grave por un importe que oscila entre los 60.000 euros y 300.000 euros; y por una infracción grave cuya sanción será de 300.000 a 600.000 euros.

Medidas de seguridad de los ficheros. Independientemente del cumplimiento por parte de la empresa de la notificación a la Agencia de Protección de Datos de la creación, modificación o supresión de sus ficheros, otro aspecto a tener en cuenta es lo referente a la seguridad de los datos de carácter personal de los ficheros automatizados. El Real Decreto 994/1999, de 11 de junio aprobó el Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal, el cuál tiene por objeto establecer las medidas de índole técnica y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos. Entre estas medidas se encuentra la elaboración y la implantación de la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos de carácter personal. Con el objeto de facilitar a los responsables de ficheros y a los encargados de tratamientos de datos personales la adopción de las disposiciones del Reglamento de Seguridad, la Agencia Española de Protección de

[2] En el caso de ficheros preexistentes, deberán adecuarse a la nueva Ley dentro del plazo de tres años a contar desde su entrada en vigor, es decir, antes del 14 de enero del 2003. En el supuesto de ficheros y tratamientos no automatizados, el plazo de adecuación es antes del 24 de octubre de 2007, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación de los afectados.

[3] Las infracciones pueden consultarse en el texto legal.

Datos pone a su disposición un modelo de "Documento de Seguridad", que pretende servir de guía y facilitar el desarrollo y cumplimiento de la normativa sobre protección de datos. Asimismo, en R.D. 994/1999 se distinguen tres niveles de seguridad, según la naturaleza de la información tratada, en relación con la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información (ver tabla 2).

El derecho a la protección de datos puede considerarse una condición preventiva para la garantía de otras libertades y derechos fundamentales. La LOPD reconoce específicamente los siguientes derechos en materia de protección de datos:

Tabla 3: Derechos del ciudadano recogidos en la LOPD

DERECHOS	
DERECHO DE INFORMACIÓN EN LA RECOGIDA DE DATOS	Cualquier persona tiene derecho a saber si sus datos personales van a ser incluidos en un fichero, y los tratamientos que se realizan con esos datos, ello condiciona el ejercicio de otros derechos tales como el derecho de acceso, rectificación, cancelación y oposición.
DERECHO DE CONSULTA DEL REGISTRO GENERAL DE PROTECCIÓN DE DATOS	Cualquier ciudadano puede dirigirse al Registro General de Protección de Datos con el fin de obtener información sobre la existencia de tratamientos de datos de carácter personal, de sus finalidades y de la identidad del responsable del mismo. La consulta es pública y gratuita, y su objeto es hacer posible a todo ciudadano el ejercicio de los derechos de acceso, rectificación, cancelación y oposición.
DERECHO DE ACCESO	Toda persona tiene derecho a dirigirse al responsable o encargado de un fichero o tratamiento para conocer la totalidad de los datos personales que le afecten y así mismo, recibir una copia inteligible de los mismos, y cualquier información sobre su origen.
DERECHO DE RECTIFICACIÓN	El artículo 16 de la LOPD, reconoce al ciudadano el derecho a dirigirse al responsable de un fichero o tratamiento para que rectifique sus datos personales.
DERECHO DE CANCELACIÓN	Este derecho ofrece al ciudadano la posibilidad de dirigirse al responsable para solicitar la cancelación de sus datos personales. Este derecho puede ejercerse cuando el tratamiento no se ajuste a lo dispuesto en la LOPD y, en particular cuando los datos resulten inexactos o incompletos.
DERECHO DE OPOSICIÓN	Toda persona tiene derecho a oponerse, por un motivo legitimo y fundado, referido a una situación personal concreta, a figurar en un fichero o al tratamiento de sus datos personales, siempre que una ley no disponga lo contrario.

Fuente: Agencia Española de Protección de Datos.

Tabla 2: Medidas de seguridad

AGÈNCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

CUADRO RESUMEN MEDIDAS DE SEGURIDAD

Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal (RD 994/1999)

Nivel básico: Ficheros que contengan datos de carácter personal.
Nivel medio: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).
Nivel alto: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los recabados para fines policiales sin consentimiento de las personas afectadas.

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
DOCUMENTO DE SEGURIDAD	- Ámbito de aplicación. - Medidas, normas, procedimientos reglas y estándares de seguridad. - Funciones y obligaciones del personal. - Estructura y descripción de ficheros y sistemas de información. - Procedimiento de notificación, gestión y respuesta ante incidencias. - Proced. realización copias de respaldo y recuperación de datos.	- Identificación del responsable de seguridad. - Control periódico del cumplimiento del documento. - Medidas a adoptar en caso de reutilización o desecho de soportes.	
PERSONAL	- Funciones y obligaciones claramente definidas y documentadas. - Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento.		
INCIDENCIAS	- Registrar tipo de incidencia, momento en que se ha producido, persona que la notificia, persona a la que se comunica y efectos derivados.	- Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente. - Autorización por escrito del responsable del fichero para su recuperación.	
IDENTIFICACIÓN Y AUTENTICACIÓN	- Relación actualizada de usuarios y accesos autorizados. - Procedimientos de identificación y autenticación. - Criterios de accesos. - Procedimientos de asignación y gestión de contraseñas y periodicidad con que se cambian. - Almacenamiento ininteligible de contraseñas activas.	- Se establecerá el mecanismos que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado. - Límite de intentos reiterados de acceso no autorizado.	
CONTROL DE ACCESO	- Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones. - Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. - Concesión de permisos de acceso sólo por personal autorizado.	- Control de acceso físico a los locales donde se encuenetren ubicados los sistemas de información.	
GESTIÓN DE SOPORTES	- Identificar el tipo de información que contienen. - Inventario. - Almacenamiento con acceso restringido. - Salida de soportes autorizada por el responsable del fichero.	- Registro de entrada y salida de soportes. - Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. - Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento.	- Cifrado de datos en la distribución de soportes.
COPIAS DE RESPALDO	- Verificar la definición y aplicación de los procedimientos de copias y recuperación. - Garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción. - Copia de respaldo, al menos semanal.		- Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
RESPONSABLE		- Uno o varios nombrados por el responsable del fichero. - Encargado de coordinar y controlar las medidas del documento. - No supone delegación de responsabilidad del responsable del fichero.	
PRUEBAS		- Solo se realizarán si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado.	
AUDITORIA		- Al menos cada dos años, interna o externa. - Adecuación de las medidas y controles. - Deficiencias y propuestas correctoras. - Análisis del responsable de seguridad y conclusiones al responsable del fichero, - Adopción de las medidas correctoras adecuadas.	
REGISTRO DE ACCESOS			- Registrar usuario, hora, fichero, tipo acceso y registro accedido. - Control del responsable de seguridad. Informe mensual. - Conservación 2 años.
TELECOMUNICACIONES			- Transmisión de datos cifrada.

- Los niveles son acumulativos y tienen la condición de mínimos exigibles.
- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.
- La ejecución de trabajos fuera de los locales de la ubicación del fichero debe ser expresamente autorizada por el responsable del fichero y garantizar el nivel de seguridad.
- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.
- Los ficheros de nivel básico que contengan datos que permitan obtener una evaluación de la personalidad del individuo deberan garantizar, además de las medidas de nivel básico, las de nivel medio relativas a auditoria, identificación y autenticación, control de acceso físico y gestión de soportes.

ANÁLISIS DE DATOS

Analizando la actividad de la Agencia de Protección de Datos, podemos observar en los siguientes gráficos el número de ficheros inscritos en el Registro General de Protección de Datos para los periodos 1994 a 2004, en los que se aprecia un crecimiento en la inscripción de ficheros de titularidad pública y privada, pero más que proporcional en el año 2000 referente a los ficheros de titularidad privada, hecho que coincide con la entrada en vigor de la nueva ley.

Gráfico 1: Evolución de la Inscripción en el RGPD

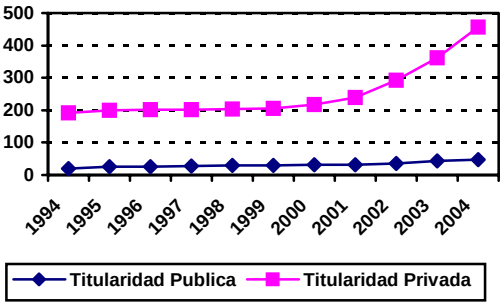
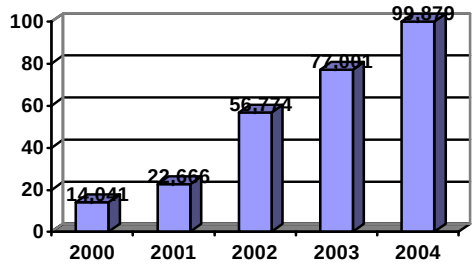


Gráfico 2: Incremento anual de la inscripción



Fuente: Memoria de la Agencia de Protección de Datos año 2004

Sin embargo, aunque el aumento esta siendo espectacular desde la entrada de la nueva ley, tan sólo 394.842 empresas con actividad privada cumplen en algunos aspectos con la normativa que obliga a registrar en la Agencia de Protección de Datos las bases de datos que contengan información de carácter personal, como ficheros de clientes o nóminas de los empleados. Las Pymes son las mayores incumplidoras de la ley, ya que aproximadamente el 10% cumple de alguna forma con esa normativa, y si tenemos en cuenta que la estructura de la industria española se caracteriza por ser un sector con un gran predominio de Pymes (en términos absolutos, la pequeña empresa representa un 85% del total y la mediana un 14%), el número de empresas que no cumplen con la normativa es muy alto.

Por otra parte, si tenemos en cuenta la inscripción en las diferentes Comunidades Autónomas (ver tabla 4), podemos observar que el porcentaje de inscripción es entorno al 4 ó 6% en las diferentes Comunidades Autónomas, lo que representa una cifra muy baja puesto que la normativa es de obligado cumplimiento. Vemos que la Comunidad con un mayor número de empresas inscritas corresponde a Aragón (12.79). En lo referente a Galicia es el 5.97% de empresas se han adaptado a la legislación vigente, y además según un informe elaborado por La Consellería de Industria y Comercio destaca que sólo el 1% cumple correctamente con las exigencias legales, asimismo se aprecia que el desconocimiento de la legislación vigente afecta a más del 66% del entramado empresarial.

Tabla 4: Inscripción de titularidad privada

Comunidad Autónoma	Total responsables	Nº de empresas	%
Comunidad Autónoma de Andalucía	19.368	464.179	4.17
Comunidad Autónoma de Aragón	11.515	90.005	12.79
Comunidad Autónoma del Principado de Asturias	3.580	68.175	5.25
Comunidad Autónoma de Canarias	4.135	128.020	3.22
Comunidad Autónoma de Cantabria	1.240	36.561	3.39
Comunidad Autónoma de Castilla y León	7.031	159.196	4.41
Comunidad Autónoma de Castilla-La Mancha	4.770	118.396	4.02
Comunidad Autónoma de Cataluña	58.505	567.019	10.31
Comunidad de Madrid	29.438	456.175	6.45
Comunidad Valenciana	21.485	329.334	6.52
Comunidad Autónoma de Extremadura	3.623	61.898	5.85
Comunidad Autónoma de Galicia	11.088	185.722	5.97
A CORUÑA	5.516	77.023	7.16
LUGO	1.992	23.122	8.61
OURENSE	909	22.452	4.04
PONTEVEDRA	2.695	63.125	4.26
Comunidad Autónoma de las Illes Balears	2.299	87.024	2.64
Comunidad Foral de Navarra	2.565	40.730	6.29
Comunidad Autónoma del País Vasco	6.706	157.539	4.25
Comunidad Autónoma de la Rioja	2.237	21.598	10.35
Comunidad Autónoma de la Región de Murcia	5.100	85.110	5.99
Ciudad Autónoma de Ceuta	106	7.448	2.10
Ciudad Autónoma de Melilla	51		
TOTAL	394.842	3.064.129	12.88

Fuente: INE (31/12/2004) y Memoria Agencia Española de Protección de Datos (31/12/2004).

La LOPD, en su Artículo 41, estableció lo siguiente: *"… 2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos…"*. Hasta el año 2003, tan sólo la Comunidad de Madrid y la Generalitat de Cataluña habían creado sus propias agencias de protección de datos. En 2004, se unieron a ésta iniciativa el Gobierno Vasco, la Generalitat Valenciana y la Xunta de Galicia (en proyecto). Al margen de estas cinco comunidades, el resto no cuenta con una agencia regional de protección de datos ni está prevista su creación. Andalucía, Asturias, las Islas Baleares, Canarias, Extremadura y Melilla, no tienen un departamento o servicio de coordinación, control y asesoramiento que vele por el cumplimiento de la LOPD. Por el contrario, Aragón, Castilla y León, Cantabria, Murcia, Navarra, La Rioja y Ceuta sí cuentan con un departamento o servicio que incluye entre sus competencias aquellas relativas a la protección de datos de carácter personal y Castilla-La Mancha está actualmente en fase de cimentación de su futura agencia.

Desde que se aprobara la ley en el año 1999, el número de denuncias ha ido creciendo en progresión geométrica. En 2004 la Agencia Española de Protección de Datos inició 978 inspecciones, lo que supone un aumento del 70% respecto al año anterior. Y entre enero y julio de 2005 ya ha

abierto 660 actuaciones. Por el mismo camino van las multas impuestas, que en 2004 sumaron un total de 16.439.801,58 euros.

En cuanto a las Inspecciones realizadas en el año 2004 por parte de la Agencia, debemos matizar que la provincia con más inspecciones ha sido Madrid y el sector más inspeccionado ha sido el de solvencia patrimonial y crédito casi a la par de las empresas de telecomunicaciones (grafico 3 y 4). Es de resaltar, que la provincia Gallega de A Coruña ocupa el 4 lugar por denuncias iniciadas por provincia del denunciado.

Grafico 4: Iniciadas por provincia del denunciado

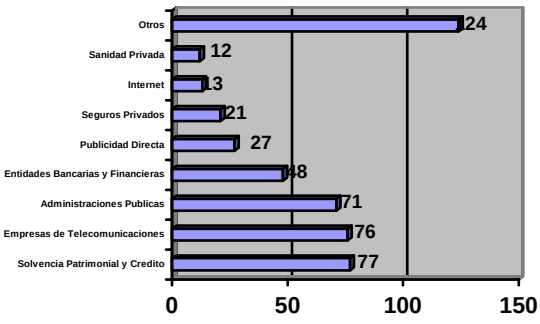
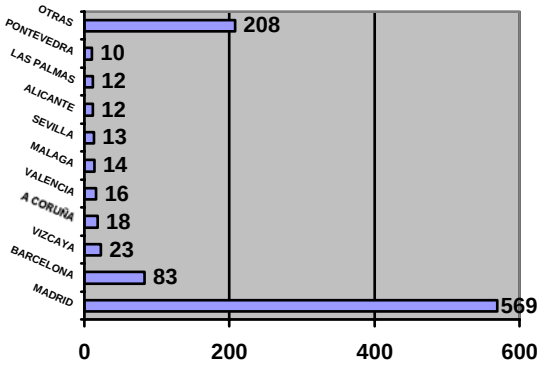


Grafico 3: Iniciados por sectores



Fuente: Memoria de la Agencia de Protección de Datos 2004

Las pymes son el problema, ya que La ley obliga a todas las empresas a inscribirse en el registro de protección de datos. Las grandes, con más medios, están cumpliendo la normativa. El problema son las pequeñas y medianas, que «aún no son conscientes» de la necesidad de proteger las bases de datos que tienen.

Las infracciones más habituales son las relacionadas con el envío no autorizado de correspondencia comercial, aunque algunas de las sanciones se refieren al uso indebido de datos sensibles, como historias clínicas o información bancaria de clientes. En los últimos tiempos, además, se han multiplicado las multas a empresas por el envío de spam (correos electrónicos no solicitados) o el manejo fraudulento de direcciones.

CONCLUSIONES

La Ley Orgánica de Protección de Datos (LOPD) española es considerada una de las más estrictas del mundo, según Jesús Rubí, adjunto al director de la Agencia de Protección de Dato,.pero el cumplimiento de la misma es escaso, ya que el porcentaje de organizaciones que tienen inscritos sus ficheros en la Agencia de Protección de Datos no supera aproximadamente el 12%. Por otro lado ya

hay registradas más de 563.771 bases de datos de empresas (septiembre del 2005) y aunque el porcentaje no se puede calcular, sí se puede afirmar que es muy bajo. En lo que respecta al Reglamento de Medidas de Seguridad su implantación también es muy baja ya que en el caso de ficheros de nivel alto, el proceso es complicado y costoso para las pequeñas empresas.

Aunque hay un conocimiento creciente de la normativa, las grandes empresas, que tienen las bases de datos más grandes y complejas, ya cuentan con políticas al respecto. El problema, hoy en día son la Pymes, siendo la protección de datos esencial para todas las empresas independientemente de su negocio o tamaño. Por los datos reflejados en el apartado anterior podemos afirmar que la mayoría de las empresas, especialmente Pymes no tienen en cuenta la protección y tratamiento de toda la información de carácter personal que van almacenando en sus bases de datos, por dos motivos principalmente; por un lado el desconocimiento de la legislación vigente que regula la protección de datos y por otro lado por la percepción que tienen de que los datos que contienen sus bases de datos son conocidos de antemano y por lo tanto, no le conceden la importancia de salvaguardar la misma.

Según una encuesta realizada entre las 400 compañías españolas de mayor facturación, las empresas españolas desconocen totalmente las normas de protección de datos. Según este estudio, el 75% de las empresas no conocen, ni siquiera superficialmente, la Ley Orgánica de Protección de Datos que entro en vigor en enero de 2000 y sólo el 23% conoce su contenido y, por lo tanto, lo aplica en la empresa. Sin embargo, los encuestados reconocen la importancia del ámbito de aplicación de esta ley, concretamente el 87% considera estas normas muy importantes.

Las principales razones que argumentan los empresarios para no cumplir la normativa son por un lado los elevados costes implantación, la falta de información y desconocimiento sobre las obligaciones que impone la ley. Por otro lado, los sectores más afectados por la normativa se encuentran el sanitario y el farmacéutico, donde las medidas de seguridad serán de especial importancia ya que deben aplicarse en su grado máximo, así como las administraciones públicas.

Por otro lado, descuidar el cumplimiento de la LOPD se paga muy caro (de las cerca de tres millones de empresas que existen en España, un gran número de empresas no tienen el «documento de seguridad», según datos de la Agencia de Protección de Datos). España es uno de los 35 países que cuenta con un organismo oficial destinado a la protección de datos confidenciales, la AEPD, pero el régimen de sanciones es de los más duros desde el punto de vista económico, con sanciones mínimas de 600 euros que pueden llegar a 600.000 para infracciones más graves. Una falta grave, como puede ser la cesión no consentida de un dato protegido, está sancionada con una multa de entre 300.000 y 601.012 euros, independientemente del tamaño de la empresa infractora. Las empresas españolas pagan cada año alrededor de 10 millones de euros a la Agencia Española de Protección de Datos (AEPD) en concepto de multas y sanciones por incumplir la legislación vigente.

Asimismo, las empresas deberían tener en cuenta de que la protección de sus datos es esencial (todos los días se crean y se almacenan grandes volúmenes de datos, el crecimiento de datos es de aproximadamente un 80% cada año en todas las empresas). El tiempo de inactividad debido a la pérdida o a la no disponibilidad de los datos afecta de manera muy significativa en las operaciones empresariales y, por consiguiente, en la rentabilidad de la empresa.

La labor de información a nivel empresarial está siendo llevada, principalmente, por las Cámaras de Comercio y asociaciones empresariales, que realizan periódicamente jornadas informativas, convenios y acuerdos sectoriales y son foco de información y consulta para los empresarios y trabajadores que pretenden adaptar sus empresas a la ley o bien informarse de sus derechos. En la Administración es más complicada de realizar esta función, dado el tamaño y la diversidad de sistemas de información existentes; en algunas de las comunidades españolas, existen servicios de organización o coordinación pero dependientes cada uno de ellos de ramas muy diferentes como Hacienda, Presidencia o Infraestructuras, con lo cual la coordinación o la unificación de criterios llega a ser muy difícil a estos extremos.

Todo esto nos lleva a pensar que sería necesario el que, desde las administraciones locales que aún no lo han hecho, se valorara a corto plazo la creación sucesiva de las Agencias de Protección de Datos Autonómicas u organismos de coordinación similares, que podrían ser destinados en un primer lugar a resolver (de modo vinculante) las dudas y situaciones diversas que pueden producirse en materia de protección de datos, tanto a empresas como a entidades de la administración local u autonómica y, en un segundo paso, a registrar los ficheros de titularidad pública y otro tipo de competencias que cada una en función de su interés o capacitación, decidiese asumir.

Por una parte se reduciría la carga de trabajo de la agencia central y por otra se regularían y optimizarían tanto las inscripciones de ficheros como las respuestas a posibles consultas o reclamaciones de los usuarios de la administración. Todo ello siempre redundará en un mayor aprovechamiento de los beneficios la Sociedad de la Información por parte de la administración ya que, los preceptos que incluye la LOPD y más concretamente en el Reglamento que la desarrolla, son en gran medida pautas de sentido común a seguir a la hora de trabajar con cualquier tipo de fichero de datos, sean personales o no.

La Consellería gallega de Innovación, Industria y Comercio ha puesto a disposición de las pequeñas empresas de la región un programa informático gratuito para facilitar a éstas su adaptación a los requisitos técnicos y legales impuestos por la Ley de Protección de Datos (LOPD). El programa se denomina “Sinxelo LOPD” y este sofware permite la identificación de los ficheros automatizados con datos de carácter personal, así como la notificación de su existencia al Registro General de Protección de Datos. La decisión de ofrecer esta herramienta fue adoptada por la Consellería de Innovación tras

comprobar el escaso conocimiento de las obligaciones legales y el bajo cumplimiento de las mismas que en general presentaban las empresas gallegas. El nuevo programa permite, de forma sintética, evaluar y saber cómo adoptar las medidas exigidas por la legislación en la materia. Se trata, en definitiva, de una guía de adaptación que pretende ser un referente para la empresa, quien decidirá cuáles son las mejores prácticas y correctas políticas de seguridad a implementar. Las beneficiarias de este software serán aquellas empresas gallegas con hasta 10 trabajadores que dispongan de ficheros con datos personales de Nivel Básico.

BIBLIOGRAFÍA

- COLLADO GARCÍA-LAJARA, Enrique. Protección de datos de carácter personal. Legislación, comentarios, concordancias y jurisprudencia. Editorial Comares. Granada, 2000.
- DAVARA RODRÍGUEZ, Miguel Ángel. Guía práctica de protección de datos. Asociación Nacional de Establecimientos Financieros de Crédito. Madrid, 1999.
- DAVARA RODRÍGUEZ, Miguel Ángel. Nueva guía práctica de protección de datos. Asociación Nacional de Establecimientos Financieros de Crédito. Madrid, 2001.
- DEL PESO NAVARRO, Emilio. Ley de protección de datos. La nueva LORTAD. Díaz de Santos. Madrid, 2000.
- DEL PESO NAVARRO, Emilio y PIATTINI VELTHUIS, Mario Gerardo. Auditoría Informática. Un enfoque práctico. 2ª edición. Rama. Madrid, 2000.
- DEL PESO NAVARRO, Emilio y RAMOS GONZÁLEZ, Miguel Ángel. LORTAD: análisis de la Ley. 2ª edición. Díaz de Santos. Madrid, 1998
- DEL PESO NAVARRO, Emilio y RAMOS GONZÁLEZ, Miguel Ángel. LORTAD: Reglamento de seguridad. Díaz de Santos. Madrid, 1999.
- DEL PESO NAVARRO, Emilio. Ley de protección de datos. La nueva LORTAD. Díaz de Santos. Madrid, 2000.
- LAMERE, J. M. La seguridad informática. Metodología. Ediciones Arcadia. Madrid, 1987.
- Memoria 2003. Agencia de Protección de Datos. Madrid, 2003.
- Memoria 2004. Agencia de Protección de Datos. Madrid, 2004.
- http://www.ag-protecciondatos.es/novedad.htm
- Constitución Española de 1978.
- Ley Orgánica 5/1992, de 29 de octubre de 1992, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (BO.E. 31/10/1992).
- Resolución de 22 de junio de 1994, de la Agencia de Protección de Datos, por la que se aprueban los modelos normalizados en soporte papel y magnético a través de los que deben efectuarse las correspondientes inscripciones en el Registro General de Protección de Datos (B.O.E. 23/6/1994).

- Real Decreto 1332/1994, de 29 de junio, por el que se desarrollan algunos aspectos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
- Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal (B.O.E. 25/6/199).
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (B.O.E. 14/12/1999).