La LOPD no es una leyenda urbana

Amparo D. Valcárce
Analista Digital, Consejera de Seguridad y CFO Futura Soluciones & Futurapps Mobile Solutions

Rosa F. Fernández
Consultora Senior. COO Futura Soluciones & Futurapps Mobile Solutions
Vocal de Comité de Servicios de la AEC

¿Recuerdan aquella serie de televisión estadounidense, "Baywatch", famosísima aquí como "Los vigilantes de la playa", sobre unos socorristas que vigilaban la playa de Santa Mónica, en la costa de Los Ángeles?

Pues bien, entre todas las tareas que tiene que asumir la dirección, gerencia y personal encargado de gestionar y coordinar recursos, algo más que un buen cuerpo van a necesitar para cumplir como "Datawatch", haciendo un seguimiento, sobre todo en lo relativo a los datos y la información de la empresa y evitando "ahogamientos" por fugas, inseguridades o incidencias.

La Comisión Europea ha puesto en marcha una reforma de la legislación en materia de protección de datos que, en poco tiempo, obligará a las empresas a efectuar cambios significativos.

Actualmente, los cambios en las organizaciones se miden no tanto por el volumen y tráfico de información que se genera: datos de proveedores, de clientes, de trabajadores, de organizaciones e instituciones, de contactos, etc., como —o, sobre todo— por los canales que se utilizan a la hora de gestionarlos (canales de entrada, salida, almacenamiento...).

Aún nos acordamos de los tiempos en que se enviaban cartas a los clientes mecanografiadas (con una copia en papel de calco para el archivo) o en los que se compraban los franqueos pagados para obtener una buena respuesta comercial. ¡Qué tiempos aquellos en los que la historia de cada persona que tenía relación con el cliente vivía y se almacenaba en fichas o tarjetas!

Eran tiempos en los que la información y los datos de la empresa tenían unos procesos cortos y los responsables de dichos datos estaban bien asignados y controlados, no sólo con nombre y apellido, sino con el compromiso directo de que cualquier acción, fuga, filtración o pérdida de datos o de información se asignaba a una persona, cargo o equipo concreto y no salía de la empresa, del departamento o del almacén. Allí vivía y allí moría la información.

Pero este escenario, en el que probablemente, querido lector, querida lectora, usted haya vivido o —al menos— le resulte familiar, se ha terminado. Comienzan nuestros hitos con aquel primer correo electrónico que se envió casi como un experimento científico.

Sabido es que en toda guerra siempre hay daños colaterales y en este escenario empresarial, con vertiginosos cambios de *atrezzo,* muchas han sido las víctimas: el papel de calco, el *tippex,* las máquinas de escribir (no sólo las manuales, también las electrónicas), los *floppy disk,* CD's de días contados, incluso los teléfonos fijos en las oficinas… ¡Quién se lo iba a decir al fax, que murió víctima de las TIC!

¡Socorro… viene la red!

Un abanico de canales se abre a nuestros pies como si de un abismo profundo se tratara:

- Gmail, Yahoo…
- Webs, blogs y hojas de registro en las mismas.
- Skype y telefonía IP.

- Youtube, Vimeo, Vine…
- Pinterest, Flickr y todas las redes que se nutren de imágenes (y por tanto de datos).
- Redes sociales: Tuenti, Facebook.
- Redes profesionales: Linkedin, Xing, Google+.
- Foursquare y otros espacios de geolocalización.
- Aplicaciones de ocio y/o de negocio.

Suponen un mareante número de canales que se viralizan y se multiplican por su propia esencia de red, lo que les hace muy peligrosos para la intimidad, confidencialidad y la quietud del dato o de la información de su empresa.

Todo ello genera nuevos actores en este nuevo escenario: prosumidores, fans, *followers, suscribers,* etc., personas que en su estado natural, y sin ser activados para ser protagonistas, tendrían un entorno seguro pero que en cuanto ven una oportunidad de ser "los protagonistas" se lanzan a la red con la furia de su primer *casting,* teniendo como resultado —en ocasiones— situaciones tan vergonzantes o tan peligrosas como las que demasiado a menudo describe la prensa.

Si además sumamos a todo esto la cantidad de dispositivos que todo el mundo utilizamos, donde guardamos todo tipo de datos, convirtiéndolos en lugares de almacenamiento con una potestad ubicua para tener los datos por el mundo globalizado, con ese formato "internetizado" gracias a la red, la situación se vuelve de riesgo a la hora de delimitar un perímetro de seguridad y tratar de poner los datos a buen recaudo.

A la empresa le han salido un montón de puertas y ventanas, sin control y sin pestillo. Y si "casa de dos puertas mala es de guardar" (que decía el dicho antiguo), imaginemos lo que ocurrirá al no poder ponerle puertas al campo, como es el caso de la red.

Pero no —pensamos—, no es mi caso, esto no me ocurre a mí, yo lo tengo todo controlado, los datos no salen de mi empresa, en mi móvil sólo tengo lo imprescindible. Y en el peor de los casos, si ocurriera algo indeseable, ahí están los de informática que todo lo arreglan, son unos *cracks.* Además, todo este rollo de vida digital a mí no me afecta porque yo pienso en analógico… ¡Fatal error!

Las empresas ya no viven ni pueden vivir al margen de la tecnología que, por cierto, ya no es tan jovencita, también ella se ha hecho mayor.

No existe un mundo real y otro virtual. Ambos son reales, sólo que ocupan distintos espacios.

¡Cómo cambiaron los tiempos…!

Y, sobre todo, el entorno de trabajo. Antes, para tener un entorno seguro bastaba con tener un cajón con llave o una caja fuerte y todo estaba controlado.

Recuerde que siempre es usted, su información o sus datos en otro escenario, tan real como la vida misma y con consecuencias en la vida real, no en la digital

Ahora existe un espacio *off line* (llamémoslo "zona tangible") y un espacio *on line* (la famosa "zona digital"). Aunque ambas pertenecen a la vida real, en espacios diferentes, se han de tomar precauciones de forma diferente, ya que para delimitar el perímetro de seguridad han de estar muy bien definidas todas las medidas para la seguridad y confidencialidad, así como un control permanente y frecuente de ambas.

Dichas "zonas", con las que hay que convivir en la empresa, empiezan también a generar una forma diferente de trabajar, con recursos en otros espacios: Cloud Computing, redes, apps, Dispositivos Mobile y generan, asimismo, otros tipos de funciones y puestos de trabajo, de tal modo que, por ejemplo, tendremos que contar con un *digital manager* en la empresa que controle las respuestas y las interacciones de sus clientes por las redes. Este escenario, que nada tiene que ver con el de hace cinco años, seguramente no tendrá nada que ver con el que vamos a vivir dentro de un año; la era "postPC" ya está llegando a su cénit y las ventas de las tabletas, smartphones y demás dispositivos móviles se disparan.

Las empresas, sin duda, también sacan beneficio de esto. Vean, si no, el último formato de trabajo denominado BYOD (Bring Your Own Device), que en versión española sería algo así como "si quieres trabajar aquí, trae tu propio equipo", lo que a efectos de lo que trata este artículo: dar más pautas para proteger los datos de los que usted o su empresa es responsable y que no le pertenecen, complica aún más la procelosa vida profesional, porque lejos de tener aquella información en un cajón, bajo llave de un solo dueño, ahora los datos y la información viajan por el hiperespacio digital a velocidad de vértigo, de red en red y de dispositivo en dispositivo.

Un momento para la REFLEXIÓN

En nuestra actividad diaria tenemos que proteger, salvaguardar y tutelar la información confidencial estratégica de la empresa o de nuestra actividad, pero también tenemos que proteger información y datos que no nos pertenecen: los de otras personas que, por la relación profesional que establecemos con ellas, nos confían. Es en este punto donde, por imperativo legal, la ley nos obliga a tomar medidas mínimas, definidas a lo largo del articulado de la Ley Orgánica de Protección de Datos (LOPD).

Si además nuestra actividad y gestión trasciende el mundo tangible para trabajar en el mundo digital, entonces también tendremos que observar la LSSI (Ley de Servicios de la Sociedad de la Información).

El incumplimiento de ambas está muy sancionado, pudiendo incurrir en multas de abolengo, además de responsabilidades civiles e incluso penales, y a todo esto se le suma la pérdida de imagen, de prestigio y de la confianza de los clientes y de las personas que tienen relación con su empresa. Un buen *branding* no puede tener falta de confianza y si quiere ganarse el mercado digital tendrá que salir con una zona de confianza y seguridad para el prosumidor multicanal, es decir, para la nueva clientela digital.

Situados, pues, en este escenario vertiginoso, difuso, profuso y, desde luego, confuso, surge la necesidad de una nueva regulación o reglamentación que modifique la protohistórica LOPD de nuestro país, nacida en el siglo XX (diciembre de 1999) y, aunque algo "modernizada" por el RMS (Reglamento de Medidas de Seguridad) aprobado y puesto en vigor en 2007 (justo cuando nace Facebook), desde que surgió este despegue sociotecnológico, la protección y tutela de un derecho constitucional como es la protección de datos de carácter personal, corre más peligro que nunca.

En este escenario de *totum revolutum,* donde ha habido una profusión de canales de entradas y salidas de datos y de plataformas y espacios para su tratamiento y gestión, la Unión Europea ha dicho "basta", y ha comenzado a replantearse una ley en la que, debido a la velocidad vertiginosa que la red impone, la realidad supera la ficción.

Y como suele ocurrir en Derecho, las leyes van por detrás de las prácticas consuetudinarias: redes sociales, aplicaciones de ocio y de negocio, espacios como Youtube, el *boom* de los dispositivos móviles, la era "postPC" y del auge de las tabletas... han sido y son realidades que han movido, desde enero de 2012, a los sesudos estudiosos de la ley y la protección, después de mil y un debates, a establecer y proponer medidas más restrictivas y sanciones más elevadas para quienes osen ocultarse detrás de un dispositivo móvil o tras una pantalla para evitar cumplir la ley o alegar desconocimiento (nuestro CC lo expresa perfectamente en su Art 6.1: "Ignorantia juris non excusat").

"En este escenario de 'totum revolutum', con profusión de canales de entradas y salidas de datos, de plataformas y espacios para su tratamiento y gestión, la Unión Europea ha dicho "basta". Urge replantearse una ley en la que, la realidad supera la ficción"

Ya, ya... pero ¿todo esto, en qué y cómo nos afecta?

Para empezar, el Reglamento del Parlamento Europeo y del Consejo relativo a la protección de la personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos), de enero 2012, va a sustituir a nuestra LOPD de 1999.

Por tanto, habrá que modificar los Documentos de Seguridad de nuestras empresas y actualizarlos de acuerdo con los cambios que el Reglamento conlleva en esta materia.

Para seguir, habrá que estar más atento que nunca respecto a los registros y las auditorías que haya que realizar, ya que el Reglamento exige responsables dentro de la empresa que asuman la responsabilidad directa del proceso de custodia y tutela de la protección de datos en la organización y habrá que nombrar un DPO (Data Protection Officer) que vele, con luz y taquígrafos, por la tutela efectiva de los datos de terceros (sí, los que no son propiedad de las empresas y que ellas sí manejan) y por la implantación eficaz de las medidas de seguridad contempladas en el Documento de Seguridad. Es decir, el famoso DS tendrá que dejar de ser un "copia, recorta y pega" para convertirse en un documento vivo que realmente responda a las necesidades y obligaciones legales exigidas por la LOPD.

Se amplían los datos protegibles, abriéndose la definición de datos de salud, y estableciendo, por ejemplo, la edad para considerar a un menor de 14 a 13 años, afectando todo ello a protocolos y ficheros y obligando a revisar los consentimientos establecidos.

Se amplía el ámbito y alcance territorial de la ley, lo que supone que todas las empresas que operan en territorio europeo deberán cumplir la normativa, tengan donde tengan su sede, y podrán ser sancionadas, al igual que las empresas europeas.

Modificación y unificación de los plazos para el ejercicio de Derechos ARCO.

Se amplía el ámbito de los derechos, al incluir el Derecho al Olvido, incidiendo en la extensión de los mecanismos para

ejercer el derecho al olvido y portabilidad para todos los ciudadanos europeos, al objeto de facilitar el borrado de sus datos y hacer desaparecer su rastro personal de Internet, con una mayor facilidad.

La Ley va más allá, las empresas deberán tener procedimientos claros e instrucciones adecuadas para que todo el mundo —esté en la parte del proceso que esté—, responda de su área y de las medidas que tiene que aplicar para no conculcar la ley, de forma que se hagan evaluaciones de impacto en la seguridad y en la protección, así como en la gestión adecuada de los incidentes de seguridad.

Por tanto, el responsable deberá tener mayor y/o mejor documentación que acredite la diligencia en el tratamiento de datos y el cumplimiento de la normativa aplicable, debiendo probar siempre, y en todo caso, la existencia de consentimiento.

Incluye sanciones más duras, en el caso de sanciones graves importes de hasta 1.000.000 € o el 2% del volumen de negocio de la empresa responsable.

Con todo ello, pues, se impone necesariamente la implantación de una política sólida, robusta y eficaz de la gestión de la información y del tratamiento de los datos.

¿Sigue pensando, de verdad, que la Ley Orgánica de Protección de Datos es poco más que una leyenda urbana? ■

Bibliografía

Network of Data Protection Officers of the EU institutions and bodies. 14 de octubre de 2010.

"Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working Under Regulation (EC) 45/2001".

Comisión Europea, 25 enero de 2012. "Propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos)".

El encargado independiente. Figura clave para un nuevo Derecho de Protección de Datos (Francisco José Santamaría Ramos, Ed. La Ley).

Actuaciones inspectoras en materia de protección de datos. El protocolo de inspección (J. M. Bosch [ed.]. Libro electrónico).

Ley 2/2011, de 4 de marzo, de Economía Sostenible.

Cómo cumplir la Ley sin aspirinas. Guía en 7 pasos para gestionar los datos de su empresa (Rosa F. Fernández y Amparo D. Valcarce, editorial VISUALGRAF).

Material propio (futura), elaborado para los siguientes cursos:

- "Atrapados en Red". Universidad de Oviedo, Escuela de Magisterio.
- "Gestión de la Seguridad de la Información". Administración Local. Asturias.
- "Pasaporte Tecnológico". Colegio de Agentes Comerciales-Gijón.
- "Marco y cumplimiento legal Ley Orgánica de Protección de Datos" —FEAPS— (Confederación Española de Organizaciones en favor de las Personas con Discapacidad Intelectual).