Alcatraz® News
El Boletín de los Expertos en Cumplimiento Normativo
Nº. 8. Noviembre 2010

El Cumplimiento de la LOPD en el Sector Sanitario

Alcatraz

La amplia experiencia en Derecho Tecnológico y nuestra Comunidad con más de 400 Partners, nos sitúan como referente en el ámbito de la Protección de Datos de Carácter Personal con más de 60.000 Adaptaciones realizadas, un 25% de Cuota de Mercado.

LOPDGEST nace de la experiencia de Davara&Davara Asesores Jurídicos, despacho especializado en Derecho Tecnológico con mayor prestigio del país, cuyo presidente D. Miguel Angel Davara está considerado como uno de los "padres de la ley" y de nuestro empeño como desarrollador tecnológico de herramientas especializadas en el cumplimiento de normativas. Con Sedes en Madrid y La Coruña nuestro equipo humano está integrado por más de 40 profesionales, Expertos en Cumplimiento Normativo y especialmente en LOPD.

Sumario

La Ley de Protección de Datos

Al igual que a muchos padres no les satisface que sus hijos les traigan a casa un *cinco*, a pesar de tratarse de un aprobado; la Agencia Española de Protección de Datos reconoce el esfuerzo realizado por el Sector Sanitario en el cumplimiento de la Ley Orgánica de Protección de Datos, pero considera que todavía hay mucho por hacer.

No puede negarse el hecho de que en el ámbito de la Salud, las distintas Entidades, cada vez son más conscientes de la importancia de cumplir con la Normativa en Materia de Protección de Datos. Es verdad. Pero precisamente la mayor concienciación de los empleados que manejan información crítica es uno de los aspectos que todavía pueden y deben mejorarse. Ya sea por tratarse de datos de gran sensibilidad, como son los relativos a la salud de las personas, o por las importantes sanciones que puede acarrear su mala gestión; resulta absolutamente imprescindible que los Centros Sanitarios, Hospitales, Clínicas Privadas o Laboratorios implanten las medidas oportunas que impidan a cualquiera saltarse la Normativa.

En ocasiones los Hospitales, por ejemplo, pueden llegar a incumplir la LOPD sin ni siquiera saberlo. Por ejemplo, que personas no autorizadas lleguen a visualizar contenidos protegidos o confidenciales o la filtración de datos, pueden llegar a meter a más de un Centro en un serio problema, entre otras cosas, por verse en la tesitura de tener que resolver un problema que ni conocen.

Y es que a la falta de concienciación que existe en torno a este asunto, se unen la necesidad de aprender conocimientos técnicos y jurídicos o la creencia de que la seguridad no es un asunto prioritario. Sin ir más lejos, estos pueden ser algunos

"necesita un Reconocimiento Médico"

de los motivos que han llevado a la Sanidad Pública Española a no cumplir con la Ley Orgánica de Protección de Datos. O lo que es lo mismo: a que uno de cada tres Hospitales de nuestro país no estén capacitados para salvaguardar la información de sus pacientes.

El de ahora es un buen momento para que nuestros Sanitarios se paren a reflexionar sobre la política de actuación que están adoptando en lo relativo a este tema. A estas alturas se ha producido un incremento de las inspecciones en diferentes sectores, algo por otro lado normal si se tiene en cuenta que de todas las sanciones impuestas por la AEPD en el 2008, un 75% fueron de carácter muy grave. Pero no sólo es eso, al contrario de lo que puede parecer, a tenor de los datos, en los Centros y Clínicas de Salud; los Ciudadanos cada vez están más concienciados con la Protección de sus Datos, de hecho un total de 1.107 denuncias han sido promovidas por particulares. Esta preocupación de los Pacientes y/o de sus familiares por su información debería mantener a todas Entidades Sanitarias en alerta.

No deja de ser curioso que todavía andemos a vueltas con el cumplimiento de la LOPD cuando ésta no deja lugar a dudas. Existe una Obligación de implantar Medidas de Seguridad, Controles y Procedimientos sobre la Confidencialidad de la Información

Editorial

Sanitaria y las Historias Clínicas de los Pacientes. Entonces, ¿por qué seguir retrasando algo que más tarde o más temprano va a haber que hacer?, ¿Por qué arriesgarse a pagar importantes sanciones por no cumplir con la obligación dictada?

Desde Alcatraz Solutions podemos contribuir a disminuir la elevada cifra de Hospitales que no cumplen lo dictado en la Normativa. Tenemos ante nosotros el reto de ayudar a todos y cada uno de estos Centros a adaptarse a la LOPD y que nuestros Partners aprovechen, así, una magnífica oportunidad de negocio. Nuestro modelo de negocio, consolidado a lo largo de todos estos años, hará posible que nuestros más de 400 Socios de Negocio aumenten la cifra de Organizaciones Sanitarias que cumple con la Ley. Animamos a todos nuestros Partners a trabajar, codo a codo, para hacer posible que ese alto porcentaje de Centros que todavía no se han *enganchado* a la LOPD, se unan a ella de nuestra mano.

Leopoldo Mallo
Director General

· Importantes Deficiencias en el Cumplimiento de la LOPD por parte del Sector Sanitario

Alcatraz News.- La Agencia Española de Protección de Datos ha hecho público el *"Informe de Cumplimiento de la LOPD en Hospitales"*, un documento que recoge el nivel de cumplimiento de las garantías de protección de datos en Centros Sanitarios Públicos y Privados de toda España.

Las principales conclusiones del Informe no dan lugar a dudas: los Centros Sanitarios Privados cumplen en mayor medida con la normativa que los Públicos, en todos y cada uno de los conceptos clave analizados:

- Inscripción de Ficheros.
- Inclusión de Cláusulas Informativas en los Formularios de Recogida de Datos.
- Disponibilidad de Procedimientos para atender el ejercicio de los Derechos de los Ciudadanos.
- Implantación de Medidas de Seguridad y su Auditoría de Seguridad periódica.

El hecho de que sean los Centros Sanitarios Privados aquellos en los que más se lleve a cabo lo dictado en la LOPD, convierte a los Hospitales Públicos en los centros en donde se producen las más importantes deficiencias en la implantación de medidas que hagan posible una adecuada custodia de los Datos Personales e Información Sanitaria de los Pacientes.

Importantes Deficiencias en el Cumplimiento de la LOPD por parte del Sector Sanitario

Para llevar a cabo este Informe en el mes de marzo, la Agencia requirió información a 605 Hospitales, a excepción de los públicos y privados ubicados en Cataluña, así como los públicos de Madrid y País Vasco; por encontrarse sometidos al control de sus respectivas Agencias Autonómicas de Protección de Datos. Del total de centros requeridos, el 92% de los mismos atendió la solicitud de la AEPD. El 8% restante, tendrá que hacer frente a un expediente sancionador por incurrir en una infracción considerada grave, lo que puede acarrearle una multa de entre 60.000 y 300.000 €.

Analizando por Comunidades, se comprueba que los Centros Sanitarios de Murcia y La Rioja son los que presentan mayores niveles de cumplimiento. En el extremo opuesto, se encuentran los Hospitales de Cantabria, Canarias, Valencia y Aragón.

En líneas generales, los principales incumplimientos de los Hospitales se encuentran a la hora de llevar a cabo:

1. La Implantación de Medidas de Seguridad y Custodia de la Información

A pesar del alto número de Hospitales que han elaborado el Documento de Seguridad previsto en la Ley (98% de los Centros Privados y 83% de los Públicos), todavía hay mucho que mejorar y corregir en la operativa establecida para que toda la información y datos concernientes a los pacientes sean adecuadamente custodiados y no reconocidos por terceros no autorizados.

2. La Inclusión de Cláusulas informativas en la Recogida de Datos

Mientras que un 94,5% de los Centros Privados manifiestan haber incluido Cláusulas Informativas en los distintos Formularios, la cifra cae hasta el 55% cuando de los Hospitales de los que se habla son Públicos.

3. La Realización de Auditorías de Seguridad

Este es otro de los puntos en donde se constatan importantes diferencias. Y es que la realización de la Auditoría bienal de Seguridad del Fichero de Historias Clínicas (un requisito obligatorio), es cumplido por el 88% de los Hospitales Privados y, únicamente, por el 44% de los Públicos.

No deja de ser curioso el dato referido a los Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición). En este apartado, el 96% de Centros Privados encuestados y el 84% de los Públicos afirman que cuentan con procedimientos para su atención efectiva. Para la AEPD este dato está relacionado con el hecho de que en los dos últimos años se haya constatado un incremento significativo en el número de las Solicitudes de Tutelas de Derecho relacionadas con el Acceso a la Historia Clínica. La espectacular subida se ha producido concretamente en las solicitudes presentadas ante la AEPD para que tutele su Derecho de Acceso, ya sea porque su propia historia clínica se le ha suministrado de forma incompleta o porque se le ha denegado el acceso al historial de un familiar fallecido.

¿Y con estos datos qué? Obviamente resulta cuanto menos preocupante las consecuencias que el incumplimiento de la Ley Orgánica de Protección de Datos por parte de los Hospitales puede tener en los Ciudadanos, puesto que no puede olvidarse que estamos hablando de datos sensibles referidos a la salud de las personas.

Es por eso que la Agencia Española de Protección de Datos lejos de quedarse de brazos cruzados, ha optado por intentar buscar una solución lo más pronto posible. Así, al Catálogo de Recomendaciones y Buenas Prácticas incluido en el Informe y remitido a todos los Centros Sanitarios y Consejerías de Sanidad; se ha sumado el requerimiento

enviado a los más de 200 Centros que incumplen alguna de las normas en materia de protección de datos. Una vez subsanadas las carencias, los Centros deberán comunicar las medidas adoptadas a la Agencia en un plazo máximo de 6 meses.

Si bien la iniciativa de evaluar el nivel de cumplimiento de los Centros Hospitalarios se debe a la constatación de alarmantes casos y procedimientos tramitados por la Agencia relativos principalmente a la vulneración de los Deberes de Seguridad y Secreto por parte del Sector Sanitario, así como al incremento de las Tutelas de Derecho relacionadas con el Acceso a la Historia Clínica planteadas por Ciudadanos en los últimos tiempos; los resultados del Informe no han sorprendido a Artemi Rallo. Para el Director de la Agencia Española de Protección de Datos los resultados conectan "*perfectamente*" con las preocupaciones que promovieron la realización de dicho informe. Rallo, que no hace distinción entre los Centros que han implantado el Historial Clínico Digital y los que no, considera que esta nueva técnica debe suponer una mejora de cara al cumplimiento de la legislación en materia de Protección de Datos.

Examen Médico a la AEPD:

- En 2009 se registraron un total de 123 denuncias y actuaciones previas de investigación en el Sector Sanitario.
- En lo que llevamos de año, se han registrado cerca de 100 reclamaciones.
- Principales motivos de Denuncias:
    - Aparición de distinta Documentación Clínica en la vía pública.
    - Almacenamiento de diversa Documentación Clínica en Áreas no Restringidas al Público y al alcance de cualquiera.
- Reclamaciones tramitadas por la AEPD:
    - Pérdida de Historiales Clínicos de Pacientes como consecuencia

de una automatización no segura.

- Utilización de los Datos Sanitarios para finalidades no autorizadas.
- Comunicación Indebida de Datos.
- Entrega de Certificados Hospitalarios de Ingresos a terceras personas con información excesiva.
- Denuncias relativas a la Cesión de Historias Clínicas a efectos de facturación a terceras entidades.

Todos aquellos Partners que tengáis acceso a Entidades del Sector Sanitario y estéis interesados en presentarles una Propuesta conjunta que les ayude a adecuarse a la Normativa en Materia de Protección de Datos, sólo tenéis que enviar un correo electrónico a la dirección: marketing@lopdgest.com

¿Están sanos nuestros Datos Personales?

Unas recomendaciones para nuestros Centros Sanitarios

Cuando enfermamos (toquemos madera para que no sea muy a menudo) y acudimos a un Hospital, vamos bajo la confianza de que garantizarán nuestra salud. ¿Pero ocurre lo mismo respecto de nuestros Datos Personales?, ¿Se garantiza su integridad? y ¿Están sometidos a las correctas Medidas de Seguridad? El Informe de la Agencia Española de Protección de Datos (AEPD) sobre el Cumplimiento de la Ley Orgánica de Protección de Datos (LOPD) en los Hospitales, publicado a mediados de octubre de 2010, ha demostrado que existen importantes deficiencias al respecto. Veamos cuáles han sido sus Recomendaciones.

1. Los Datos de Salud como datos especialmente protegidos

Un Dato Personal es cualquier información relativa a una persona física identificada o identificable. Y cuando esta información hace referencia a nuestras creencias religiosas, políticas, orientación sexual, origen racial o salud, estamos ante los conocidos como "datos especialmente protegidos" o "datos sensibles". Este tipo de datos goza de una mayor protección debido, esencialmente, al gran perjuicio que podría causar a su titular el que se conocieran o utilizaran sin su consentimiento. Por este motivo, requisito indiscutible para su tratamiento será el Consentimiento de su Titular y unas Medidas

de Seguridad calificadas de nivel alto por el Reglamento de Desarrollo de la LOPD (el RD 1720/2007, RLOPD), cuyo incumplimiento conllevará una infracción muy grave con su correspondiente sanción, que si es pecuniaria (para el Sector Privado) puede alcanzar hasta 600.000 €.

No basta que el artículo 43 de nuestra Constitución, ni la Ley 14/1986 General de Sanidad o las más recientes Ley 41/2002, de Información y Documentación Clínica y la Ley 16/2003, de Cohesión y Calidad del Sistema Nacional de Salud, tengan entre sus objetivos garantizar y proteger el Derecho a la Salud de los Ciudadanos y la Confidencialidad de la misma, sino que la LOPD añade algo más: un control de esa información confidencial, que nos permita saber y conocer quién, cómo, cuándo, dónde y para qué será utilizada aquella información relativa a nuestra persona que pertenece a nuestra esfera más íntima.

2. El Cumplimiento de la LOPD por parte de los Hospitales y sus grandes lagunas

En el 2009 fueron 123 las denuncias interpuestas en el Sector Sanitario, alcanzando ya la cifra de 100 en lo que llevamos de 2010. ¿Quién no recuerda noticias como las relativas a la difusión de datos de pacientes abandonados en contenedores de basura, o el haber visto la Documentación Clínica almacenada en áreas no restringidas y a las que podía tener acceso cualquier persona sin muchas dificultades?, ¿Quién no ha sufrido en su propia piel, o en la de un entorno no muy lejano, la pérdida de Historias Clínicas o un acceso incompleto a las mismas? ¿Y quién no ha comprobado perplejo cómo en los Certificados Hospitalarios de Ingreso de algún familiar se incluía una información excesiva que iba a acabar en manos del Departamento de Recursos Humanos de la Empresa?

A estos problemas, entre otros, ha querido hacer frente la AEPD. Pero esto no es algo nuevo. El Sector Sanitario siempre ha generado problemas en relación con la Confidencialidad de la Información de los Pacientes. Así, ya en 1997 la Agencia en colaboración con el INSALUD elaboró un Informe sobre el Cumplimiento de la normativa de Protección de Datos por parte de los Hospitales Públicos, detectándose por ese entonces, como ahora, importantes lagunas en las Medidas de Seguridad.

En esta ocasión se han analizado tanto Centros Públicos como Privados que caían bajo la competencia de la AEPD [Recordamos aquí que aquellos Centros Públicos que se encuentran en Cataluña, Madrid y País Vasco están bajo la competencia de las respectivas Autoridades de Protección de Datos de las citadas Comunidades Autónomas]: de los 562 Centros que contestaron al requerimiento de la Agencia (se preguntó a 654), 294 eran Privados y 268 Públicos. Esto es, un 93% de los Hospitales requeridos contestaron a la Agencia, y en su conjunto, hay que indicar que los Centros Sanitarios de Murcia y La Rioja son los que han mostrado un mayor nivel de cumplimiento, frente a los Centros ubicados en las Comunidades Autónomas de Cantabria, Canarias, Valencia y Aragón.

El problema sigue estando en las Medidas de Seguridad: se constata al final de la evaluación que, a pesar de que el 98% de los Centros Privados, y el 83% de los Públicos, habían elaborado un Documento de Seguridad, los mayores problemas provenían de las deficiencias a la hora de implantar las Medidas de Seguridad recogidas en los mismos. No basta poner el cartel de “Cuidado con el perro”, sino que hay que tenerlo.

En el estudio que realizó la Agencia se analizó:

a) La situación respecto de la Inscripción de Ficheros. Aquí, aunque hay que destacar que se cumple con esta obligación legal en un alto porcentaje (89% de los Hospitales Públicos y 99% de los Privados), el problema se deriva de la falta de un mantenimiento y actualización posterior de las citadas inscripciones (sólo un 80% de los Centros Públicos actualiza, mientras que los Centros Privados nuevamente elevan este porcentaje al 96%).

b) El Cumplimiento de las Medidas de Seguridad. Según el Informe de la AEPD este es el terreno en el que se comenten mayores infracciones. Debemos recordar aquí que aunque en los Centros Hospitalarios se pueden manejar Ficheros de Datos Personales sujetos a un nivel de Medidas de Seguridad Básicos (como pudieran ser los de los empleados), en lo relativo a las Historias Clínicas de los Pacientes, el nivel de Medidas de Seguridad se eleva al máximo.

c) El Deber de Información y el Procedimiento para ejercitar los Derechos ARCO. Este es otro de los campos en los que se han detectado mayores problemas, especialmente, en el Sector Público: aquí, se incluye la Cláusula Informativa en muy pocos casos (un 45% frente a un 95% de los Privados), a pesar de que sí se establece un procedimiento específico para ejercitar los conocidos Derechos ARCO (Acceso, Rectificación, Cancelación y Oposición).

d) Los casos de Externalización de Servicios prestados por los Hospitales. No es infrecuente que muchos Centros externalicen la realización de ciertas pruebas (análisis, radiografías, escáneres…), con la Comunicación de Datos que ello supone. Aquí, aunque en la mayoría de los casos se ha realizado el correspondiente Contrato de Acceso por cuenta de Terceros previsto legalmente (artículo 12 LOPD), sólo un 34% de los Centros encuestados (44% Públicos y 35% Privados) realiza la recomendada (en tanto que datos sensibles) disociación de los Datos Personales comunicados.

3. Las Recomendaciones de la AEPD

Una vez analizada la situación, la AEPD además de remitir a su Subdirección General de Inspección los datos de los Centros que no contestaron a su requerimiento -en tanto que ello podría suponer el indicio de alguna infracción-, y remitir las conclusiones del estudio realizado a las Consejerías de Sanidad y al Ministerio de Sanidad, Política Social e Igualdad, la AEPD por un lado, requirió a más de 200 Centros la adopción de las medidas correctoras de las deficiencias observadas (que tendrán que implantar en un plazo máximo de seis meses); y, por otro lado, elaboró unas Recomendaciones tendentes a un eficaz Cumplimiento de la LOPD.

Como hemos visto hasta ahora, en el apartado anterior, el problema no deriva tanto de la falta de medidas sino de su eficaz cumplimiento. Hay que ponerse en marcha. En este sentido, las Recomendaciones son sencillas y van orientadas, por un lado, a garantizar una correcta y adecuada información; y, por otro lado, a cumplir con aquellas Medidas de Seguridad que pueden proteger la confidencialidad de los Datos Personales, y por tanto de sus titulares. Entre estas Recomendaciones encontramos:

a) Respecto de la Inscripción de Ficheros: se debe mantener actualizada la Inscripción de los Ficheros declarados. Hay que revisar la situación actual del Centro Sanitario: muchos Ficheros están desactualizados -quedando inutilizables-, o no tienen publicada en el Diario Oficial (en el caso de los Servicios Públicos) la correspondiente Disposición General de Adecuación a la LOPD y al RLOPD, siendo esto contrario a los Principios de la LOPD.

b) Respecto de las Medidas de Seguridad: aquí tenemos todo un campo de trabajo. Se recomiendan entre otras cosas, medidas como la disociación de los Datos de Carácter Personal (especialmente, en los casos en los que el tratamiento de los mismos haya sido externalizado); llevar un Registro de los Accesos a los Historiales Clínicos; Almacenar y Custodiar la Información de forma correcta (en áreas de acceso restringido mediante llave o clave o en archivadores); Adoptar Medidas que eviten la pérdida o sustracción de la Documentación durante su transporte; y realizar las correspondientes Auditorías.

Entre todas estas Recomendaciones destaca ésta última de realizar Auditorías (bienales, de obligada realización conforme a la normativa existente; y aquéllas otras que sirvan de orientación sobre el nivel de cumplimiento por parte del Personal del Centro). Sólo mediante una adecuada Auditoría podremos comprobar el nivel de Cumplimiento efectivo de las Medidas de Seguridad recogidas en el Documento de Seguridad, y evitaremos que éste se convierta en papel mojado. Y aquí queremos destacar que la gran mayoría de los Centros Hospitalarios (un 82%) opta de manera total o parcial por un Auditor externo para la realización de la citada Auditoría.

c) Respecto del Deber de Información y del Procedimiento para ejercitar los Derechos ARCO: la Agencia hace especial hincapié en la fácil y sencilla tarea de incluir las Cláusulas Informativas en los impresos de los Hospitales, colocar Carteles Informativos, e Informar al Personal del Hospital sobre su Deber de Secreto al respecto. Y, de la misma manera, se aconseja establecer un sencillo y eficaz procedimiento para que los Pacientes puedan ejercitar sus Derechos ARCO, lo cual se lograría centralizando el mismo en una Unidad del Hospital que se encargara exclusivamente de dar respuesta a las peticiones recibidas. Debemos recordar la sujeción a unos plazos legales.

Esta labor informativa es realmente importante, en tanto que en los últimos años se ha producido un incremento en las peticiones por parte de los Pacientes de acceder a su Historia Clínica o a la de algún familiar fallecido, siendo por desgracia el resultado el acceso a una historia incompleta o la denegación de la misma en el último caso citado. Consecuencia inmediata: la intervención de la AEPD con la correspondiente sanción al Centro.

d) Respecto de la Externalización de los Servicios del Hospital: teniendo en cuenta que un alto porcentaje de los Hospitales contrata empresas que gestionan la mayoría de sus servicios, se aconseja revisar y actualizar los Contratos entre ambas partes, y controlar que se cumplen las Medidas de Seguridad cuando se produzca una Comunicación de Datos, recomendándose la disociación o encriptación de la Información Clínica.

4. Conclusiones

Probablemente la imposición de multas pecuniarias, frente a las sanciones administrativas de los Centros Públicos, sea lo que mueve a los Centros Privados a cumplir, en un porcentaje mucho más elevado que en el caso de los Hospitales Públicos, con la normativa de Protección de Datos. Pero las infracciones se siguen produciendo tanto en uno como en otro sector.

Debemos destacar que la mera tenencia de un Documento de Seguridad no es suficiente para cumplir con una adecuada y correcta Protección de los Datos Personales. No basta con tener un Documento de Seguridad, sino que hay que seguir las directrices en él detalladas y mantener las Medidas Técnicas y Organizativas. El mantenimiento y actualización en este terreno es indispensable. Por este motivo, una de las mayores deficiencias y respecto de las que la AEPD hace mayor hincapié es la realización de Auditorías de Seguridad. Cumpliendo con la normativa en este terreno (Información

y Seguridad, esencialmente) estaremos asegurando un mejor nivel de vida. Cuidemos la salud de nuestros Datos.

Mónica Arenas Ramiro

Profesora de Derecho Constitucional
Universidad de Alcalá de Henares

AEPD - Noticias, Estadísticas y Sanciones

N

· La Agencia Española de Protección de Datos será la encargada de tutelar el Acceso a la Información Pública

· Facebook reconoce que varias Aplicaciones transmitieron Información de sus Usuarios

E

· Estadísticas Mensuales RGPD - Octubre 2010

S

· La Agencia Española de Protección de Datos expedienta a Google por captar datos para Street View

· Multan a la SGAE por la irregular instalación de las Cámaras de Videovigilancia de su sede compostelana

· La Agencia Española de Protección de Datos será la encargada de tutelar el Acceso a la Información Pública

Alcatraz News.- La Agencia Española de Protección de Datos será la encargada de vigilar a las Administraciones Públicas y proteger el Derecho de Acceso de los Ciudadanos a todo lo relativo a la Información Oficial.

Así, con la entrada en vigor de la Ley de Transparencia y Acceso a la Información Pública de los Ciudadanos; la AEPD recibirá nuevas dotaciones de competencias y su denominación pasará a ser Agencia Española de Protección de Datos y Acceso a la Información.

Este nuevo planteamiento llevará a una Institución Pública independiente, como es el caso de la Agencia, a arbitrar una figura legal hasta la fecha carente en España. Y es que nuestro país era de los pocos Estados, junto con Luxemburgo, Malta y Chipre; en los que todavía no se contemplaba esta normativa.

La creación de esta Ley busca dotar de publicidad y transparencia a todos los poderes públicos, salvo en aquellos casos en los que prevalezca un interés, ya sea público o privado, que derive un deber de reserva. No hay que olvidar, por más tiempo, que el principio de Derecho de Acceso de todos los Ciudadanos a la Información Pública es la regla de juego en un país democrático.

Decíamos lo de no olvidar por más tiempo porque, tal y como señala José Luis Piñar, Catedrático de Derecho Administrativo y ex Director de la AEPD; hasta ahora se ha venido poniendo como excusa la Protección de Datos para impedir el Acceso de los Ciudadanos a la Información que

obra en poder de los Poderes Públicos. Antes de que termine el año 2010, tiempo previsto para que se apruebe el anteproyecto de Ley, la AEPD asumirá la tutela y trabajará para garantizar éste Derecho que tenemos los Ciudadanos.

A partir de ese momento, la Agencia compatibilizará la Defensa de la Privacidad, impidiendo el acceso a determinada información, con la custodia del Derecho al Acceso a la Información Pública.

Esta nueva situación no debería presentar mayores dificultades. Sin embargo, fuentes del Ministerio de la Presidencia señalan a las Comunidades Autónomas y Ayuntamientos como los puntos en donde pueden darse los principales problemas. En el caso de las primeras por contar éstas con normativas contradictorias. En lo que respecta a los Consistorios, por ofrecer una gran resistencia a facilitar datos, basándose en la Confidencialidad de las Informaciones y en la Privacidad de los Datos.

A continuación, mostramos algunos de los aspectos destacados de la nueva reforma:

1. Acceso sin Interés Directo

Todas las personas tendrán Derecho a acceder a la Información Pública que deseen con una simple solicitud al Departamento que corresponda.

La normativa impondrá al Poder Público el deber de motivar la negativa a hacer accesible la información solicitada por concurrir alguna de las limitaciones que prevé la propia Ley.

2. Protección de la Intimidad

Este es uno de los objetivos fundamentales de la futura norma.

Las Solicitudes de Acceso que contengan Datos Íntimos o que afecten a la vida privada se denegarán, salvo que exista consentimiento expreso y por escrito del afectado.

Cuando sea posible, se facilitará la información dando carácter anónimo a sus protagonistas y evitando datos identificativos.

3. Exenciones a la Normativa

Fuera del ámbito normativo, la Seguridad Nacional y la Defensa; salvo que lo justifique un Interés Público determinado.

4. Organismos Excluidos

La Ley no se aplicará a la información generada por los Órganos del Poder Legislativo o Judicial, que se rigen por sus propias normas, como también el Tribunal Constitucional y el Tribunal de Cuentas.

Se mantendrá la aplicación de la propia normativa para el Acceso a los Secretos Oficiales.

La Administración podrá negar el acceso cuando las Solicitudes se consideren abusivas por su carácter manifiestamente irrazonable o repetitivo.

Al asumir esta nueva responsabilidad, la Agencia Española de Protección de Datos ve incrementadas sus competencias; lo que pone de manifiesto el importante papel que juega en nuestro panorama social.

· Facebook reconoce que varias Aplicaciones transmitieron Información de sus Usuarios

EFE.- Facebook ha admitido, recientemente, que a través de sus aplicaciones se han transmitido datos confidenciales a empresas de rastreo en la web, pero afirma que el problema se ha "exagerado" en la prensa.

La Compañía respondió así a la denuncia publicada por el diario 'The Wall Street Journal' en un reportaje en el que revela esta violación de la Política de Confidencialidad de Datos de Facebook.

"Recientemente, hemos sabido que varias aplicaciones construidas sobre la plataforma Facebook transmitieron el nombre del usuario -un identificador que utilizamos en nuestros interfaces de programación de aplicaciones-, de un modo contrario a la Política de Confidencialidad de Facebook", informó en el blog de la Compañía el ingeniero Mike Vernal.

Según el diario económico, los nombres de decenas de millones de usuarios y, en algunos casos, los de sus 'amigos', han sido transmitidos a compañías de publicidad y otras de rastreo en internet.

La investigación se centró en diez de las aplicaciones más populares de Facebook, unos pequeños programas incrustados en la red social para compartir intereses o jugar.

A través de este tipo de software, 25 anunciantes y otras empresas han recibido datos confidenciales, incluso los de aquellos usuarios que habían configurado como confidencial esa información en sus perfiles, según el periódico neoyorquino.

En la red social que cuenta ya con más de 500 millones de usuarios, hay más de medio millón de programas de este tipo y la mayoría de ellos son gestionados por profesionales o empresas informáticas independientes a Facebook.

Pero las normas de la red social prohíben a estos la transmisión de datos de sus usuarios a empresas publicitarias, incluso si el usuario lo permite cuando configura sus exigencias

de privacidad en la red.

Seis de las aplicaciones investigadas son de la empresa Zynga: FarmVille (con 59,4 millones de usuarios a nivel mundial), Texas HoldEm (36,3 millones), FrontierVille (30,6), Café World (21,9), Mafia Wars (21,9) y Treasure Isle (15,3).

El resto son Phrases (43,4 millones de usuarios a nivel mundial), Causes (26,7), Quiz Planet (16,5), e IHeart (14,0).

Buscar soluciones

Facebook ha comunicado ya el problema a los principales implicados en el caso para buscar "soluciones posibles", que comunicará próximamente, informó Vernal.

El portavoz admitió que varias aplicaciones "estaban transmitiendo" la identificación del usuario (UID) que se utiliza en las aplicaciones, "de una manera que violaba su Política (de Confidencialidad)".

"En la mayoría de los casos, los desarrolladores no intentaban transmitir esa información, pero lo hicieron debido a detalles técnicos referentes a cómo funcionaban los exploradores ", argumentó.

Sin embargo, para Facebook, "la información en prensa ha exagerado las implicaciones de compartir los UID (identificación de usuarios)".

"Conocer un UID no capacita a cualquiera a acceder a la información privada de un usuario sin su consentimiento explícito", argumentó Vernal.

Vernal dijo que ya habían sufrido este tipo de problemas antes, en referencia a un incidente que ocurrió en mayo y que también afectó a la red social MySpace, pero los desafíos técnicos en esta ocasión han sido "mayores".

Noticias

El incidente anterior permitió ofrecer información de usuarios a compañías publicitarias cuando los miembros de Facebook y MySpace entraban a uno de los anuncios que aparecían en sus web.

Por el momento, Facebook ha suspendido alguna de estas aplicaciones, como 'Phrases'. La empresa que desarrolla ese programa ha declarado en su web desconocer las causas de esa medida e instó a la Compañía a comunicarle las razones.

Facebook ha dicho que está "en conversaciones con los socios y la comunidad on line en su sentido más amplio para buscar posibles soluciones".

Estadísticas Mensuales

· Estadísticas Mensuales RGPD - Octubre 2010

· La Agencia Española de Protección de Datos expedienta a Google por captar datos para Street View

EFE.- La Agencia Española de Protección de Datos (AEPD) informó hoy de la apertura de un procedimiento sancionador a Google España por la Captación de Datos Personales de las Redes WIFI para Street View, tras finalizar la fase de investigación iniciada en mayo.

Según la AEPD, se han constatado indicios de dos infracciones graves y tres muy graves de la Ley Orgánica de Protección de Datos (LOPD) imputables a Google Spain e Inc., como la Captación y Almacenamiento de Datos Personales sin consentimiento.

Se ha verificado la Captación de Datos de localización de Redes WIFI con identificación de sus Titulares, y de Datos Personales de diversa naturaleza del contenido de las comunicaciones: direcciones de correo electrónico (con nombre y apellidos), mensajes asociados a dichas cuentas y servicios de mensajería, o códigos de usuario y contraseñas, entre otros.

Tras la apertura del procedimiento sancionador a Google, la AEPD ha dado traslado al Juzgado el Informe Final de la Inspección y, conforme a la Legislación de Procedimiento Administrativo, suspende la tramitación del expediente sancionador, hasta la resolución del procedimiento judicial que la Compañía tiene abierto en el Juzgado de Instrucción Nº 45 de Madrid.

· Multan a la SGAE por la irregular instalación de las Cámaras de Videovigilancia de su sede compostelana

EFE.- La Agencia Española de Protección de Datos ha sancionado con 30.000 € a la Sociedad General de Autores y Editores (SGAE), por irregularidades en la instalación de las Cámaras de Videovigilancia en su sede de Santiago de Compostela, según ha informado hoy el Movimiento por los Derechos Civiles (MpDC).

La Asociación recuerda en un comunicado que había presentado la denuncia hace año y medio y que la Agencia ha entendido que el enfoque de las cámaras supone una Infracción Grave a la Ley Orgánica de Protección de Datos.

Fuentes del Movimiento valoraron a EFE esta sanción, aunque agregaron que la cantidad de la multa no va a crear una gran preocupación a una Entidad como la SGAE.

También comentaron que las cámaras objeto de esta sanción, como en otros casos en que han presentado denuncia, fueron instaladas por una empresa especializada, que conoce la legislación y debe informar a su Cliente.

Explicaron que esta situación se da también en numerosas instituciones, como los Ayuntamientos de La Coruña o Santiago de Compostela, así como en distintas Entidades de la Xunta y de la propia Administración Central del Estado.

El MpDC resalta que, además, estas Instituciones Públicas no son sancionadas, como debían, sino que la Agencia Española de Protección de Datos sólo les avisa para que procedan a la corrección de las irregularidades.

Alcatraz

La amplia experiencia en Derecho Tecnológico y nuestra Comunidad con más de 400 Partners, nos sitúan como referente en el ámbito de la Protección de Datos de Carácter Personal con más de 60.000 Adaptaciones realizadas, un 25% de Cuota de Mercado.

www.lopdgest.com

marketing@lopdgest.com

902 169 121

darse de baja