

OBLIGACIONES LEGALES EN TORNO A LAS BASES QUE INCORPORAN DATOS DE CARÁCTER SENSIBLE



La protección de los datos personales de los viajeros

El marco jurídico vigente establece importantes límites y obligaciones para todas las personas o entidades que tratan datos personales, cuestión especialmente delicada para las empresas del ámbito turístico.

La potencialidad que tienen las tecnologías de la información para el control individual y social hacen que, hoy en día, de forma mucho más dramática que hace unos años, sea necesario proteger jurídicamente los datos personales.

Bajo esa premisa la Unión Europea ha desarrollado uno de los modelos más elaborados para la protección de los datos personales, modelo que ha resultado ser notablemente más estricto que cualquiera de sus homólogos en otras partes del mundo.



Para volar
Las aerolíneas
trabajan con datos
personales de sus
pasajeros.

En nuestro país la regulación del derecho a la protección de datos de carácter personal tiene su punto de partida en el artículo 18.4 de la Constitución, que establece 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”.

En ese contexto, el 29 de octubre de 1992 se dictó la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD), derogada tras la entrada en vigor de la Ley Orgá- ➤

➤ nica 15/1999 de 13 de Diciembre, de protección de datos de carácter personal (LOPD), modificada por la Ley 62/2003 de 30 de diciembre, de Medidas Fiscales, Administrativas y del Orden Social.

Esta Ley Orgánica es la actualmente vigente e incorpora a nuestro ordenamiento jurídico las disposiciones contenidas en la 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.

Este marco jurídico establece importantes límites y obligaciones para todas aquellas personas o entidades que tratan datos personales, en especial respecto a los límites en la recogida y el tratamiento de los datos, el necesario consentimiento del afectado, el derecho de información, los deberes de secreto, las previsiones para el acceso por cuenta de terceros, las comunicaciones o cesiones de datos, las transferencias internacionales, el conjunto de derechos del afectado (acceso, rectificación, cancelación) y las medidas específicas para el tratamiento automatizado de datos, entre otros.

Todas aquellas entidades que manejan ficheros físicos o automatizados –bases de datos– que contienen datos de carácter personal, deben someterse a la referida normativa, lo cual supone, además de cumplir los límites y cautelas respecto a los derechos de los afectados, un conjunto de inscripciones en el Registro General de Protección de Datos (RGPD), dependiente de la Agencia Española de Protección de Datos (AEPD).

La Agencia Española

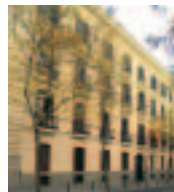
A partir del año 1992, en que se crea la Agenda de Protección de Datos –hoy llamada Agencia Española de Protección de Datos (AEPD)–, viene creciendo en la sociedad, incluidos los propios operadores jurídicos y los actores económicos, la conciencia sobre el significado de este derecho fundamental, en el que inciden de manera tan significativa el desarrollo de las tecnologías de la información y la globalización. Dicha tendencia se observa de forma significativa en el considerable incremento de la

actividad de la Agencia Española de Protección de Datos Personales. Según su última memoria institucional, a finales de 2005 el número total de inscripciones se elevaba a 650.733, de las que 598.916 son privadas y 51.817 públicas, alcanzándose una inscripción media de 600 ficheros al día.

En cuanto a las funciones de investigación y sanción que tiene encomendadas la AEPD, durante 2005 se iniciaron un total de 1.158 expedientes de investigación. Se iniciaron 387 procedimientos sancionadores frente a responsables de ficheros de titularidad privada, 52 frente a responsables de ficheros de titularidad pública y 579 procedimientos de tutela, alcanzándose la cifra total de 2.176 actuaciones. En el año 2005 el importe por multas impuestas por dicha entidad ascendió a 21.105.083,99 euros.

Los datos del turismo

El establecimiento de políticas internas y mecanismos para la adecuada protección de los datos personales es un deber jurídico para las empresas españolas en general y para las empresas dedicadas al sector del turismo



El papel de la AEPD

La Agencia Española de Protección de Datos (AEPD), creada en 1992, es la encargada de velar por el respeto los límites y cautelas con respecto a los datos personales.



Prioridad para el turismo

Para Carlos Garmendia, socio de Garmendia & Asociados Abogados (www.garmendia-asociados.com), firma líder en Derecho de las Nuevas Tecnologías y Propiedad Intelectual, “el cumplimiento de la normativa de protección de los datos personales de los viajeros debe ser prioritario para el sector turístico español”.

en particular. Éstas últimas necesitan para el desarrollo de su actividad trabajar de forma particularmente intensa con diversos datos personales de sus clientes.

Una agencia de viajes debe incorporar los datos de sus clientes a sus ficheros para llevar a cabo multitud de cesiones y encargos de tratamiento sobre los mismos, como, por ejemplo, los datos solicitados a la hora de formalizar una reserva hotelera o de cumplimentar la Información Anticipada sobre Pasajeros (API) para viajar a los países que así lo requieran. Esta información obligatoria solicitada por algunos países –como EE UU, Cuba o México– incluye, según la regulación de cada país, desde datos de pasaporte hasta visado y dirección postal.

Además, según la nueva normativa de la Unión Europea, también se recopilan previamente datos de documentación de personas que viajen a España desde países que no pertenezcan al Espacio Schengen y de aquellos que regresen al país.

Estos trámites y normativas obligan a los operadores de servicios de turismo a ser especialmente cuidadosos en el cumplimiento de las obligaciones y limitaciones impuestas por la LOPD, a fin de garantizar la seguridad de su actividad y evitar la imposición de cuantiosas sanciones, que pueden alcanzar hasta los 600.000 euros.

Por todo ello, la Agencia Española de Protección de Datos –posiblemente la más estricta de toda la Unión Europea frente a eventuales infracciones a la normativa sobre protección de datos personales– lleva a cabo una especial tutela del sector turístico, uno de los motores de la economía de nuestro país.

El establecimiento de mecanismos, salvaguardas, procedimientos y protocolos de seguridad para el cumplimiento de la normativa sobre protección de datos debe ser una de las prioridades del sector turístico.

Algo que no es incompatible con el adecuado desenvolvimiento empresarial ya que, pese al grado de exigencia que establece el régimen jurídico en la materia, es necesario que toda adecuación esté basada en el conocimiento profundo del modelo de negocio, junto a un cuidadoso diagnóstico que determine las especificidades propias de cada entidad. □

EE UU y la UE acuerdan la cesión de datos de pasajeros

Las autoridades estadounidenses conservarán 19 datos personales de los pasajeros europeos durante un periodo de 15 años. El acuerdo, vigente desde agosto, es válido para los próximos siete años.



Tras meses de arduas negociaciones, y para satisfacción de las compañías aéreas europeas, la Unión Europea y Estados Unidos han alcanzado un acuerdo para la transferencia de datos personales de pasajeros de vuelos europeos con destino al país norteamericano. Después de los atentados del 11 de septiembre, alegando la necesidad de aumentar la seguridad en contra del terrorismo, EE UU logró la firma de un acuerdo con la Unión Europea que obligaba a las aerolíneas a entregar hasta 34 fragmentos de información personal de cada pasajero que volaba a los EE UU. El primer acuerdo, alcanzado en mayo de 2004, fue anulado por el Tribunal de Justicia Europeo y sustituido por otro provisional en octubre de 2006. El nuevo acuerdo, válido para los próximos siete años, entró en vigor el pasado mes de agosto.

Las claves del nuevo acuerdo

Fecha del viaje, nombre, dirección, modalidad de pago, número de tarjeta de crédito, teléfonos de contacto, dirección electrónica, agencia de viajes, itinerario... Estos son algunos de los datos incluidos en esa lista, reducida a 19 campos (aunque con un nivel de detalle más elevado) que EE UU

recibirá de los pasajeros procedentes de la UE. En esa lista también está el tipo de maletas con las que se viaja, el origen racial del pasajero, su afiliación sindical, datos sobre su salud y hábitos sexuales e ideología política y religiosa. Información sensible que suscita recelos por parte de muchos y que sólo podrá ser empleada por el Departamento de Seguridad Interior de EE UU (ahora receptor de estos datos) en circunstancias "excepcionales". El tratamiento, recogida, utilización y conservación de estos datos no se rige por un acuerdo jurídico, sino por una serie de garantías no vinculantes que podrían ser modificadas y el periodo de retención de los datos se ha visto ampliado de 42 meses a 15 años. Como novedad, ahora serán las aerolíneas las que envíen la información a las autoridades estadounidenses, que antes accedían directamente a ella a

La información será enviada a la otra orilla del Atlántico, donde será procesada por el Departamento de Seguridad Interior de Estados Unidos

Información anticipada

Los pasajeros de Iberia podrán introducir los datos personales requeridos por algunos países a través de www.iberia.com, reduciendo así el tiempo de espera en los mostradores de facturación.

través de los sistemas informáticos de las compañías aéreas.

Las valoraciones

A pesar de la ventaja que supone tener un único acuerdo en lugar de 27 bilaterales, la Eurocámara ha firmado una resolución conjunta que afirma que éste no asegura una protección adecuada de los datos personales de los europeos. El Parlamento Europeo considera que el acuerdo tiene importantes lagunas en materia de seguridad jurídica, protección de datos y derecho de recurso para los ciudadanos de la UE. La Agencia Española de Protección de Datos (AEPD) también ha criticado ciertos aspectos del acuerdo, como la posibilidad de que las autoridades americanas puedan hacer uso de datos sensibles, la ampliación del periodo de retención de los datos, y el que éstos puedan ser empleados en procedimientos judiciales. Además, el acuerdo contempla la posibilidad de que la información sea transmitida a terceros países, y no hay garantías sobre su uso una vez en posesión de terceros. Como punto positivo, la AEPD destaca el que los europeos puedan recurrir ante el Departamento de Seguridad Nacional de los EE UU en las mismas condiciones que los estadounidenses. **□**