Protección de datos: errores legales comunes en Internet

¿A qué nos referimos con protección de datos?

Ni más mi menos que a respetar lo dispuesto en la LOPD (Ley Orgánica de Protección de Datos de Carácter Personal, ley orgánica 15/99). Esta ley es aplicable también al ámbito de Internet – y no sólo a él – siempre y cuando poseamos datos de terceras personas y que siendo calificados como de carácter personal sean objeto de un tratamiento automatizado por parte nuestra, o sea, con ordenador.

Hay que saber que en caso de incumplir dicha norma, al igual que su normativa de desarrollo, podemos ser objeto de sanciones económicas más que severas, pudiendo llegar las mismas a importes de 600.000 euros.

¿Cuál es el error más común y más simple?

El más habitual es, poseyendo ya una base de datos con información sobre terceros – por ejemplo, con direcciones e-mail para un boletín – no llevar a cabo su preceptiva inscripción en el llamado Registro General de Protección de Datos. Esta inscripción es gratuita, siendo su trámite en parte a través de Internet y en parte remitiendo documentación en papel. Para el caso de no efectuar dicho trámite, se estaría cometiendo una infracción, cuya sanción podría oscilar entre tan sólo 600 euros, o llegar incluso a los 60.000 euros en determinados casos.

¿Cuál es otro error habitual?

Consiste en no advertir a las personas de las cuales obtenemos sus datos de que los mismos van a formar parte de un fichero automatizado del cual somos el responsable, de cuál es la finalidad del mismo, de otros posibles destinatarios de dicha información, de qué respuestas a las preguntas que en su caso solicitemos de los mismos son obligatorias y de cuáles no, e incluso de la dirección e identidad del responsable del fichero, pues en más de una ocasión ni se indica o advierte quién va a poseer dichos datos.

También es básico y obligatorio recordar que a dicho titular de los datos le asisten determinados derechos en cuanto a los mismos, como son el de acceso, cancelación, rectificación y oposición. Junto a ello hemos de explicar cómo ejercerlos, dentro de qué plazos, de qué manera, y demás trámites que en cuanto a ellos sean precisos y necesarios para que dichos derechos se vean cumplidos de una forma recta y cabal.

¿Y si los datos los *trata* realmente otra empresa a la cual le encargamos dicho tratamiento?

Más de una vez nos encontramos con que, por motivos generalmente de falta de experiencia o búsqueda de una mayor profesionalidad, o incluso de reducción de costos, el tratamiento de dichos datos lo lleva a cabo una tercera empresa. Ejemplo habitual es aquel en el cual ante una campaña de marketing on line no es el dueño o responsable del portal el que realiza el tratamiento automatizado, sino que lo es una tercera empresa o profesional, cuyo servicio o prestación es precisamente el llevar a cabo la campaña de publicidad, albergando en su propia base de datos dichas direcciones e-mail, o incluso otro tipo de dato más personal.

En el caso expuesto estaríamos ante lo que la LOPD denomina Encargo de Tratamiento a terceros, exigiéndose en dicho caso, siempre, que dicha relación esté debidamente plasmada en un contrato, por escrito, en el que figure hasta dónde llega el encargo contratado, qué medidas de seguridad se aplicarán a dichos datos, y la prohibición de destinarlos a otro fin distinto del contratado, y por supuesto también la prohibición de cederlos o comunicarlos a cualquier tercero.

No aplicación de medidas de seguridad.

La norma que comentamos hoy divide o califica los datos según sea el tipo de los mismos, estableciendo varias categorías. Los niveles que así establece son tres, y a cada uno le corresponde un nivel concreto y diferente de medidas de seguridad. Por ejemplo, al considerar – con buen criterio, además – la LOPD que no es igual de sensible poseer de alguien simplemente su dirección e-mail que poseer del mismo el dato de cuánto dinero debe por multas de tráfico, o incluso de alguna enfermedad que padezca, debido a todo ello, se aplicarían diferentes medidas de seguridad. No olvidemos que el no aplicar dichas medidas es igualmente objeto de sanción, y que junto a ello hay que elaborar el llamado Documento de Seguridad, que será el documento escrito en el cual se recogerán dichas medidas, concretas, especificándose qué tipo de ficheros serán objeto de las mismas, y cómo se llevarán a buen término. Este documento no hay que inscribirlo en ningún lugar, pero si un día nos encontramos con la visita de una inspección de la Agencia de Protección de Datos se nos pedirá para su correspondiente análisis, y evidentemente para ver si coincide con la realidad del tratamiento que realizamos con los datos.

Transferencias internacionales.

Este es uno de los supuestos en los cuales se suele caer con menos conciencia de su ilegalidad, pues la mayoría de las veces el sujeto infractor ni era consciente de que lo que estaba haciendo era ilegal. En concreto nos referimos a que si los datos van a *viajar* a otro país, no habrá problema si éste pertenece a la Unión Europea, pues se considera que poseen un nivel equivalente de protección de datos al regulado por nuestra legislación, pero... si el país de destino es otro, habrá que ver si se trata de un Estado en relación al cual la Agencia de Protección de Datos considere – por convenio internacional – que cumple también los mínimos de la legislación española.

Un caso habitual es el de las transferencias a los EE. UU. Este Estado, aunque parezca una contradicción, no está dentro de los reconocidos ni por España ni por la Unión Europea como poseedor de un nivel de protección de datos a considerar como confiable, y es por ello que habrá previamente que comprobar si la empresa concreta de destino de los datos en dicho país está en la relación de la Unión Europea denominada de Puerto Seguro. Es una relación que se puede ver en la página web del Departamento de Comercio norteamericano, y las empresas que figuren en ella tendrán el visto bueno. Lo que ocurre es que son poquísimas las empresas que figuran en dicho listado, y de no figurar ahí la empresa concreta que nos interese, habrá que solicitar autorización al Director de la Agencia de Protección de Datos.

El fenómeno indicado suele darse, por ejemplo, al remitir a una filial en USA, donde estaría la empresa madre, datos de nuestros clientes, o incluso en materia de hosting, contratando servidores ubicados físicamente en dicho país, que generalmente son más baratos y por tanto más competitivos.

Una adecuada política de protección de datos es claro, por lo expuesto, que debería preocuparse por legalizar tal tipo de situaciones, existiendo incluso un trámite para que tal tipo de actuación tenga el visto bueno en toda la Unión Europea, quitándonos de tal modo y manera la preocupación constante de una posible inspección de la Agencia de Protección de Datos (la sanción sería del tipo grave, pudiendo llegar a 600. 000 euros, siendo el tramo mínimo de esta sanción de 300.000 euros).

Javier Hernández Martínez, abogado
E-mail: bufete@opinionvirtual.com
Web: www.opinionvirtual.com
Abogado especialista en Derecho de Internet y de las Nuevas Tecnologías