Tres claves para cumplir la LOPDGDD durante el control a los trabajadores

La nueva Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), ha supuesto un cambio en el paradigma del Derecho laboral, y en concreto, en la capacidad de control que ostentan los empresarios.

El pasado mes de diciembre se cumplió un año desde su publicación y ya existe jurisprudencia relevante al respecto, por lo que podemos detallar las **principales claves para un correcto cumplimiento**.

1. EL FICHAJE A TRAVÉS DE LA HUELLA DEL EMPLEADO

A raíz de la aprobación del Real Decreto-ley 8/2019, que introdujo la obligación de registrar la jornada laboral de los trabajadores, han surgido diversos sistemas para el registro de la jornada, siendo uno de los más populares el registro mediante la huella digital del trabajador.

Sin embargo, la Agencia Española de Protección de Datos (AEPD), de conformidad con el criterio de la Audiencia Nacional, se ha proclamado en diversas ocasiones **contraria al tratamiento de la huella digital**, considerada por el Reglamento General de Protección de Datos como un dato biométrico, al permitir identificar de forma inequívoca a una persona. En concreto, esta **Agencia considera que el tratamiento de la huella digital para el registro de la jornada de los trabajadores no cumple el principio de proporcionalidad**, al existir otros métodos menos intrusivos.

No obstante, la AEPD indica que podrá utilizarse este método si el dato de la huella del trabajador se almacena de forma cifrada únicamente en una **tarjeta portada por el propio empleado**, debiendo aproximar al terminal tanto la tarjeta como la huella digital, para la confirmación de su identidad.

De esta manera, se pretende evitar que el empresario trate directamente los datos derivados de la huella digital del trabajador, al no conservarse esta información en sus sistemas.

2. EL CONTROL A TRAVÉS DE LA GEOLOCALIZACIÓN

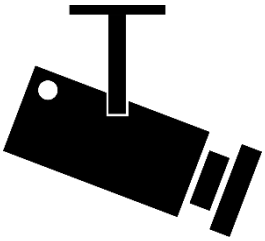
La propia normativa regula la geolocalización de los empleados y describe los requisitos necesarios para poder implementar un sistema de geolocalización sin vulnerar la intimidad del empleado y, por ende, sin infringir la normativa de protección de datos.

Así, para una correcta geolocalización, **el empleado deberá conocer si está siendo geolocalizado** y los términos de dicha geolocalización: la finalidad (seguridad, control de las obligaciones laborales…), duración del tratamiento, conservación de los datos, derechos que ostenta, etc.

Además, como establece el art. 90 de la LOPDGDD y en cumplimiento de los principios de licitud y de proporcionalidad, el empleador podrá "*tratar los datos obtenidos a través de sistemas de geolocalización para el ejercicio de las funciones de control de los trabajadores […] siempre que estas funciones se ejerzan* ***dentro de su marco legal y con los límites inherentes al mismo***."

La geolocalización deberá ceñirse a la propia **jornada laboral del trabajador**, resultando excesiva la geolocalización realizada fuera de su horario laboral, periodos de descanso e, incluso, periodos de baja por enfermedad.

3. LA VIDEOVIGILANCIA EN LAS ZONAS DE TRABAJO



El empresario tiene el derecho de controlar a los trabajadores a través de la instalación de sistemas de videovigilancia en el lugar de trabajo, si bien se debe respetar el derecho a la intimidad de los trabajadores.

Es imprescindible, por lo tanto, que los empleadores **informen con carácter previo y de forma expresa** a los trabajadores acerca de esta medida. A mayores, los sistemas de videovigilancia **no podrán captar en ningún caso lugares destinados al descanso o esparcimiento de los trabajadores**, tales como vestuarios, aseos o comedores.

Finalmente, será totalmente **contrario a la normativa que estos sistemas graben los sonidos** del lugar de trabajo, siendo admitida dicha grabación únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo.

En relación a las **cámaras ocultas**, únicamente se podrán instalar sin informar a los empleados cuando existan sospechas de que se está cometiendo un acto ilícito y se haya cumplido el deber de información mediante la colocación de carteles informativos de videovigilancia.

La AEPD publica la nueva guía sobre las cookies

Las cookies permiten almacenar datos relativos a la navegación de los usuarios y, por ende, tienen el potencial de obtener grandes cantidades de información del mismo: sus hábitos, intereses, ideología política… Esto, multiplicado por todas las páginas web que un usuario puede visitar en un día, hace que sea indispensable un cauteloso cumplimiento de la normativa de protección de datos, con el ánimo de respetar la **intimidad de los usuarios** de internet.

Con dos años de retraso desde la publicación del RGPD, la Agencia Española de Protección de Datos (AEPD) plasma el criterio que venía mostrando en los últimos años en una guía sobre el uso de las cookies, con las obligaciones que todos los sitios web deberán acatar para un correcto cumplimiento de la normativa.

A continuación, repasaremos las principales novedades que contiene esta guía:

Información por capas. En este sentido, los responsables de las páginas web deberán seguir mostrando la información utilizando el sistema de capas: la información básica deberá mostrarse en un banner informativo, que contenga un enlace a una segunda capa denominada política de cookies, con la restante información. No obstante, la información contenida en la primera capa es ahora más completa, debiendo informar al usuario de aspectos tan relevantes como la identidad del responsable, la finalidad de las cookies utilizadas o el modo en el que el usuario puede aceptar, rechazar o configurar las cookies.

Panel de configuración de cookies: la gran novedad. Con el ánimo de reforzar la capacidad de decisión del usuario en relación al uso de sus datos personales, la AEPD obliga a los responsables a desarrollar un panel de configuración de cookies en sus páginas web, con el ánimo de que el propio usuario, de una manera sencilla e intuitiva, pueda aceptar o rechazar las cookies según su finalidad (analíticas, de publicidad, de elaboración de perfiles…).

De esta manera, se pretende dotar a los usuarios de una capacidad real de decisión sobre el tratamiento de sus datos personales.

Actualización del consentimiento. Cuando un usuario configura las cookies en función de su propio criterio, el responsable deberá conservar la selección realizada por el usuario durante un periodo no superior a 24 meses. Pasado este periodo, el responsable deberá solicitar de nuevo el consentimiento del usuario a través del banner de cookies y el panel configurador.

Cookies: la AEPD sanciona a IKEA por incumplir la ley

La AEPD sanciona a IKEA por incumplir la normativa de protección de datos, en relación a la información otorgada al interesado sobre el uso de las cookies y la forma de recabar el consentimiento para su instalación.

La **sanción de 10.000 €** se ve motivada, en concreto, porque el sitio web *ikea.com/es* **instalaba cookies en el navegador de los usuarios sin ofrecerles la opción de aceptarlas o rechazarlas**. Así, como consecuencia del mero acceso a la página web y sin haberse pulsado el botón de "aceptar" contenido en el banner de cookies, se descargaban cookies que analizaban la navegación de los usuarios y realizaban un análisis de su perfil con fines publicitarios.

Además, la información que otorgaba el responsable en sus textos legales (tanto en el banner de cookies como en la política de cookies) resultaba confusa, al utilizar expresiones imprecisas que no ofrecían información real al interesado, como "*Utilizamos cookies para ofrecerte una mejor experiencia*"; e insuficiente, al no informar sobre la identidad de los terceros que podían acceder a esta información.

A mayores, **IKEA no ofrecía a los usuarios la capacidad de aceptar o rechazar las cookies** en función de sus finalidades, a través de un panel de configuración de cookies.

Sanción de 60.000 € a RTVE por la pérdida de varios pendrives con datos de 11.000 empleados

El hecho que motivó la sanción fue la **pérdida de seis dispositivos extraíbles sin cifrar** de la Oficina de atención al Partícipe del Plan de Pensiones de RTVE, que **contenían datos personales de aproximadamente once mil trabajadores**. Estos dispositivos se encontraban guardados en una "bolsita monedero", sin ninguna medida de seguridad que obstaculizara su acceso.

Los datos afectados por esta brecha de seguridad, que databan los más antiguos del año 1995, no solamente permitían identificar al interesado (nombre, apellidos, DNI, teléfono, dirección electrónica y postal…), sino que **revelaban información especialmente sensible, como datos relativos al nivel salarial, a la salud o a la afiliación sindical de los afectados**, entre otros.

Por todo esto, la AEPD ha considerado imponer una **sanción de 60.000 €** por la vulneración del art. 32 del Reglamento General de Protección de Datos, relativo a la seguridad de los datos personales, así como del art. 73 de la LOPDGDD, por la "falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para aplicar de forma efectiva los principios de protección de datos desde el diseño, así como la no integración de las garantías necesarias en el tratamiento".

Para modular esta sanción, la AEPD ha tenido en cuenta como agravante la acción negligente cometida por RTVE sobre datos que revelan información especialmente sensible de los interesados; y como atenuantes, **la implementación de medidas de formación y concienciación entre el personal**.

Editado por Microlab Hard

Madrid. C/ Cronos 8, 1º, Madrid

Barcelona. C/ Santiago Rusiñol 8, Molins de Rei