DIPUTACIÓ DE VALÈNCIA

Protecció de Dades i Seguretat de la Informació

Cuadernos DivalData

Cuadernos dirigidos a delegados,
responsables y especialistas en protección
de datos personales

Cuaderno nº 19 | Enero 2022

TRATAMIENTO DE DATOS BIOMÉTRICOS EN EL ÁMBITO DE LA ADMINISTRACIÓN PÚBLICA

Í N D I C E

TRATAMIENTO DE DATOS BIOMÉTRICOS EN EL ÁMBITO DE LA ADMINISTRACIÓN PÚBLICA

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos boletines informativos. Estas peticiones deberán dirigirse a:

Diputación de Valencia

Dpto. de Protección de Datos y Seguridad de la Información

Pl. de Manises, 4 46003 Valencia

email: dpdsi@dival.es

SUSCRIPCIONES

Si deseas suscribirte a nuestra publicación accede al siguiente

enlace

"LAS RAZONES POR LAS QUE LAS TECNOLOGÍAS BASADAS EN DATOS BIOMÉTRICOS ESTÁN EN AUGE SE PUEDEN REDUCIR A LA FACILIDAD EN SU USO, Y LA GARANTÍA DE NIVELES DE AUTENTICACIÓN MÁS ROBUSTOS QUE OTROS MÉTODOS TRADICIONALES. SIN EMBARGO, SU USO TAMBIÉN HA SUPUESTO LA APARICIÓN DE NUEVOS RIESGOS PARA LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LOS DERECHOS Y LIBERTADES DE LOS TITULARES DE LOS DATOS".

INTRODUCCIÓN

La utilización de tecnologías basadas en datos biométricos -especialmente, la huella dactilar o patrones faciales- se está generalizando en diferentes ámbitos, haciendo uso de la misma para el acceso a servicios bancarios, labores de vigilancia en la docencia online, el control de acceso a instalaciones o el registro de la jornada laboral, entre otros. Incluso en el ámbito de la Administración Pública es frecuente su uso, en especial, con fines de control de acceso a determinadas dependencias y de registro de la jornada laboral.

Las razones por las que las tecnologías basadas en datos biométricos están en auge se pueden reducir a la facilidad en su uso, al permitir prescindir de tarjetas físicas, llaves o la memorización de contraseñas, así como la garantía de niveles de autenticación que, *a priori,* pueden parecer más robustos que otros métodos tradicionales.

Sin embargo, su uso también ha supuesto la aparición de nuevos riesgos para la seguridad de la información y la protección de los derechos y libertades de los titulares de los datos.

En el presente cuaderno, estudiaremos el auge de dos de las técnicas que tienen por objeto el tratamiento de datos biométricos -huella dactilar y reconocimiento facial-, los usos que a estas se suele dar en el ámbito de la Administración Pública y sus implicaciones en materia de protección de datos. Asimismo, expondremos una serie de equívocos con relación a estas tecnologías que se han extendido los últimos años.

"LOS DATOS BIOMÉTRICOS, POR SU NATURALEZA, SON PARTICULARMENTE SENSIBLES, YA QUE EL CONTEXTO DE SU TRATAMIENTO PODRÍA ENTRAÑAR IMPORTANTES RIESGOS PARA LOS DERECHOS Y LAS LIBERTADES FUNDAMENTALES DE LAS PERSONAS Y POR ELLO MERECEN UNA PROTECCIÓN ESPECIAL".

TRATAMIENTO DE DATOS BIOMÉTRICOS EN EL RGPD

Según la definición que ofrece el Reglamento General de Protección de Datos (RGPD), los datos biométricos son *"aquellos datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos".*

Estos datos, por su naturaleza, son particularmente sensibles, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y libertades fundamentales de las personas y es por ello que se consideran "datos de categoría especial" merecedores de una protección especial.

Para empezar, la especial sensibilidad a la que aludíamos se traduce en la prohibición de tratamiento de datos biométricos, a excepción de aquellas situaciones específicas en que se permite su tratamiento, contempladas en el art. 9.2 RGPD, como el consentimiento explícito, el cumplimiento de obligaciones y derechos en el ámbito del derecho laboral y seguridad y protección social, la protección de intereses vitales, razones de interés público esencial, fines de medicina preventiva o laboral o la prestación de asistencia sanitaria o social, entre otras.

Además, de forma previa a su implantación, será necesario valorar la necesidad de llevar a cabo una Evaluación de Impacto en la Protección de Datos (EIPD). El RGPD, en su art. 35.1, señala que cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, se deberá realizar dicha Evaluación. La EIPD es requerida, en particular, cuando se lleva a cabo un tratamiento a gran escala de este tipo de datos. También en la lista de tipos de tratamiento que requerirían EIPD, elaborada por la AEPD, se encuentran los tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.

"LOS DATOS BIOMÉTRICOS ÚNICAMENTE CONSTITUIRÍAN UNA CATEGORÍA ESPECIAL DE DATOS EN EL CASO DE QUE SE SOMETAN A UN TRATAMIENTO TÉCNICO ESPECIFICO DIRIGIDO A IDENTIFICAR DE MANERA UNÍVOCA A UNA PERSONA FÍSICA".

DISTINCIÓN ENTRE IDENTIFICACIÓN Y VERIFICACIÓN/AUTENTICACIÓN BIOMÉTRICA

Antes de continuar, debe realizarse una puntualización, y es que el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, ya que:

- El artículo 4.14 del RGPD define como «datos biométricos» aquellos *"datos personales obtenidos a partir de un tratamiento técnico especifico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona".*
- El artículo 9.1 del RGPD incluye entre los datos de categoría especial los *"datos biométricos dirigidos a identificar de manera univoca a una persona física".*
- El Considerando 51 del RPGD señala que *"El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física".*

Según la AEPD, en su Informe Jurídico 36/2020, una interpretación conjunta de estos preceptos daría a entender que los datos biométricos únicamente constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico especifico dirigido a identificar de manera unívoca a una persona física.

Al objeto de aclarar las dudas interpretativas, la AEPD atiende al 'Dictamen 3/2012, sobre la evolución de las tecnologías biométricas' del extinto Grupo de Trabajo del Artículo 29 (GT29), en el que se distingue:

"LA IDENTIFICACIÓN DE UN INDIVIDUO POR UN SISTEMA BIOMÉTRICO ES NORMALMENTE EL PROCESO DE COMPARAR SUS DATOS BIOMÉTRICOS CON UNA SERIE DE PLANTILLAS BIOMÉTRICAS ALMACENADAS EN UNA BASE DE DATOS (PROCESO DE BÚSQUEDA DE CORRESPONDENCIAS UNO-A-VARIOS). CON CARÁCTER GENERAL, LOS DATOS BIOMÉTRICOS ÚNICAMENTE TENDRÁN LA CONSIDERACIÓN DE CATEGORÍA ESPECIAL DE DATOS EN ESTOS SUPUESTOS".

- **Identificación biométrica:**

La identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias *uno-a-varios*).

- **Verificación/autenticación biométrica:**

La verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias *uno-a-uno*).

Atendiendo a la citada distinción, la AEPD entiende que, si bien el concepto de dato biométrico incluye ambos supuestos, con carácter general, únicamente tendrán la consideración de categoría especial de datos en los supuestos de identificación biométrica *(uno-a varios).*

No obstante, la AEPD considera que se trata de una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo atenderse al caso concreto. Esta termina expresando que, en tanto en cuanto no se pronuncia al respecto el Comité Europeo de Protección de Datos o los órganos jurisdiccionales, debe adoptarse, en caso de duda, la interpretación más favorable para la protección de los derechos de los afectados.

"ALGUNAS PERSONAS NO PUEDEN UTILIZAR DETERMINADOS TIPOS DE BIOMETRÍA PORQUE SUS CARACTERÍSTICAS FÍSICAS NO SON RECONOCIDAS POR EL SISTEMA. EN CASOS DE LESIONES, ACCIDENTES, PROBLEMAS DE SALUD (COMO PARÁLISIS) Y OTROS, LA INCOMPATIBILIDAD PUEDE SER TEMPORAL. LA INCOMPATIBILIDAD BIOMÉTRICA PERMANENTE PUEDE SER UNA CAUSA DE EXCLUSIÓN SOCIAL".

EQUÍVOCOS COMUNES EN RELACIÓN CON EL TRATAMIENTO DE DATOS BIOMÉTRICOS

Dada la popularización del uso de datos biométricos para fines de identificación y autenticación, se han extendido una serie de equívocos con relación a esta tecnología. La AEPD los enumera y explica su fundamento en el documento '14 equívocos con relación a la identificación y autenticación biométrica'. Algunos de estos equívocos son:

"La identificación/autenticación biométrica es suficientemente precisa para diferenciar siempre entre dos personas"

La AEPD señala que está demostrado que el parecido biométrico entre hermanos o familiares ha confundido a sistemas biométricos. En particular, la identidad de patrones biométricos para la identificación de hermanos gemelos más allá del reconocimiento facial es un campo de estudio. Es más, las condiciones medioambientales en entornos no controlados (i.e., reconocimiento facial en espacios públicos, el uso de con pintura facial o máscaras antivirales) provoca el aumento de la tasa de error y, por tanto, que la confusión sea más probable.

"La identificación/ autenticación biométrica es adecuada para todas las personas"

Algunas personas no pueden utilizar determinados tipos de biometría porque sus características físicas no son reconocidas por el sistema. En casos de lesiones, accidentes, problemas de salud (como parálisis) y otros, la incompatibilidad puede ser temporal. La incompatibilidad biométrica permanente puede ser una causa de exclusión social.

"El proceso de identificación/autenticación biométrica no se puede burlar"

Existen procedimientos y técnicas que permiten burlar sistemas de autenticación biométrica y asumir la identidad de otra persona. Algunos de esos medios, como el uso de máscaras o de reproducciones de la huella, no requieren de grandes conocimientos técnicos o recursos económicos. Existen también los denominados "sistemas adversarios", que están diseñados específicamente para tratar de engañar a los sistemas de reconocimiento de imágenes y que pueden utilizarse para burlar la identificación biométrica.

"Los sistemas de identificación/autenticación biométrica son más seguros para los usuarios"

Cualquiera de los sistemas en los que los datos biométricos estén siendo procesados puede sufrir una brecha de seguridad. El acceso no autorizado a nuestros datos biométricos en un sistema permitiría o facilitaría (en el caso de utilizar múltiples factores de autenticación) el acceso al resto de los sistemas que utilicen dichos datos biométricos.

Podría tener el mismo efecto que usar la misma contraseña en muchos sistemas distintos, por lo que la escala en la implantación biométrica es un problema en sí mismo. Y, a diferencia de los sistemas basados en contraseñas, una vez que la información biométrica ha sido comprometida, esta no se puede cancelar.

Si antes la información biométrica se almacenaba en unas pocas bases de datos (principalmente con fines relacionados con la seguridad pública o el control de las fronteras), ahora está almacenada cada vez en más entidades y dispositivos. Eso aumenta enormemente la probabilidad de una brecha de seguridad de información biométrica (durante su recogida, transmisión, almacenamiento o proceso).

"CUALQUIERA DE LOS SISTEMAS EN LOS QUE LOS DATOS BIOMÉTRICOS ESTÉN SIENDO PROCESADOS PUEDE SUFRIR UNA BRECHA DE SEGURIDAD".

TRATAMIENTO DE DATOS BIOMÉTRICOS PARA EL REGISTRO DE LA JORNADA LABORAL

En el presente apartado, analizaremos la cuestión relativa a la implementación de un sistema de registro horario en la Administración Pública mediante tecnologías biométricas como la de la huella dactilar o el reconocimiento facial y el impacto de estas en la protección de los datos personales de las personas trabajadoras.

"EL TRATAMIENTO DE DATOS BIOMÉTRICOS PARA EL REGISTRO DE LA JORNADA LABORAL REQUERIRÍA, EN PRIMER LUGAR, DE LA CONCURRENCIA DE, AL MENOS, UNA DE LAS BASES JURÍDICAS ESTABLECIDAS EN EL ART. 6.1 RGPD".

BASE DE LEGITIMACIÓN

El tratamiento de datos biométricos para el registro de la jornada laboral requeriría, en primer lugar, la concurrencia de, al menos, una de las seis bases jurídicas establecidas en el art. 6.1 RGPD.

La base jurídica que legitima el tratamiento de estos datos en el supuesto de los **funcionarios de carrera, interinos y personal eventual** radica en el cumplimiento de una misión de **interés público [art. 6.1.e) RGPD]**. Y es que, si tenemos en cuenta que el artículo 54 de la Ley 7/2007, de 12 de abril, del Estatuto Básico del Empleado Público (EBEP) establece como principio de conducta de los empleados públicos, entre otros, el cumplimiento por parte de las personas trabajadoras de la jornada y el horario establecidos, el Ayuntamiento podría realizar actuaciones de control con el fin de verificar el cumplimiento de este deber. Así lo entiende la Agencia Catalana de Protección de Datos (APDCAT) en su Dictamen 49/2009: *"En este sentido, se puede afirmar que el Ayuntamiento, en su condición de "empresario", también puede ejercer un control cuando éste tenga como finalidad verificar el cumplimiento por parte de los trabajadores de sus obligaciones laborales".* Asimismo, el tratamiento de los datos personales podría contar como base con la necesidad de la **ejecución del contrato de trabajo [6.1.c) RGPD]** aunque su relación no sea contractual en sentido estricto. Así lo manifestó la AEPD en el Procedimiento Nº: PS/00128/2020.

De otro lado, el tratamiento de los datos del **personal laboral** encontraría base de licitud, además de en la

"POR OTRA PARTE, EN LA MEDIDA EN QUE LOS DATOS BIOMÉTRICOS DIRIGIDOS A IDENTIFICAR DE FORMA UNÍVOCA A UN INTERESADO FORMAN PARTE DE LA CATEGORÍA DE DATOS ESPECIALES, JUNTO A LA BASE JURÍDICA DEL ART. 6 RGPD, DEBERÁ CONTARSE TAMBIÉN CON ALGUNA DE LAS EXCEPCIONES PREVISTAS EN EL ART. 9.2 RGPD, QUE EXCEPTUARÍAN LA PROHIBICIÓN GENERAL DEL TRATAMIENTO DE ESTE TIPO DE DATOS".

citada misión realizada en **interés público [art. 6.1.e) RGPD]**, en la necesidad de dar cumplimiento a una **obligación legal [art. 6.1.b) RGPD]** derivada de los artículos 20.3 y 34.9 del Estatuto de los Trabajadores, que establecen la obligación del empleador de adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por la persona trabajadora de sus obligaciones y deberes laborales, así como la obligación del registro diario de jornada, respectivamente. Asimismo, el tratamiento de los datos personales del personal laboral contaría como base con la necesidad de la **ejecución del contrato de trabajo [6.1.c) RGPD].**

Por otra parte, en la medida en que los datos biométricos dirigidos a identificar de forma unívoca a una persona forman parte de la categoría de datos especiales, junto a la base jurídica del art. 6 RGPD, se deberá contar también con alguna de las excepciones previstas en el art. 9.2 RGPD, que exceptuarían la prohibición general del tratamiento de este tipo de datos.

La primera de las excepciones que podría concurrir sería la del **consentimiento explícito [art. 9.2.a) RGPD]**, en virtud de la cual no será de aplicación la prohibición cuando *«el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales* …». No obstante, no parece que la aplicación del consentimiento como excepción a la prohibición pueda proporcionar seguridad jurídica al empleador, pues el consentimiento del empleado será, en todo caso, revocable. El GT29, en su Dictamen nº 03/2012, aunque no excluye completamente la utilización del consentimiento «en los casos en que existan garantías suficientes de que es realmente libre», sí considera que hay motivos de peso para suponer que el consentimiento es una base de licitud débil debido al habitual desequilibrio entre empleador y empleado, afirmando que su uso en el contexto del empleo debe cuestionarse y justificarse debidamente. Por su parte, la Agencia Española de Protección de Datos (AEPD), en su Informe número 0392/2011, procedía a descartar el consentimiento como causa legitimadora en estas situaciones: *«(…) habida cuenta del carácter esencialmente revocable del mismo. En efecto, teniendo en cuenta la finalidad de control perseguida, no puede considerarse admisible un sistema basado en el*

consentimiento del afectado, dado que en caso de que aquel voluntariamente quisiese revocar el tratamiento, lo que implicaría la necesaria cesación en el tratamiento de los datos por parte del responsable, no sería posible el cumplimiento de la finalidad perseguida.»

Como apunta la Agencia Catalana de Protección de Datos (APDCAT) en el Dictamen CNS 63/2018, aquella excepción en la que convendría detenerse sería la **letra b) del art. 9.2 RGPD**, según la cual la prohibición general de tratamiento de datos biométricos no es de aplicación cuando: *«el tratamiento es necesario para el **cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social**».*

"PARA LEGITIMAR EL TRATAMIENTO DE DATOS BIOMÉTRICOS LA EXCEPCIÓN EN LA QUE CONVENDRÍA DETENERSE SERÍA LA DEL ART. 9.2.B) RGPD: EL CUMPLIMIENTO DE OBLIGACIONES Y EL EJERCICIO DE DERECHOS ESPECÍFICOS DEL RESPONSABLE DEL TRATAMIENTO O DEL INTERESADO EN EL ÁMBITO DEL DERECHO LABORAL Y DE LA SEGURIDAD Y PROTECCIÓN SOCIAL".

La AEPD, en lo relativo a la base de legitimación del tratamiento de datos biométricos de los empleados a efectos de registrar la jornada, deja claro en el apartado de Preguntas Frecuentes (FAQS) de su página web, en respuesta a la pregunta *"13.10 ¿Qué tipo de sistema pueden utilizar las empresas para el control horario?"* que se podrá habilitar el sistema que considere más adecuado y, por tanto, desde la perspectiva del derecho fundamental de la protección de datos, tendrían la misma base de legitimación y no precisarían el tratamiento consensuado con los trabajadores los sistemas manuales, analógicos o digitales al efecto de generar la correspondiente prueba justificativa del registro diario de la jornada de cada trabajador.

Además, la AEPD, en la 10ª Sesión Anual Abierta celebrada en fecha 4 de junio de 2018, tal y como recoge el documento de Preguntas de los asistentes, señala en relación con el sistema de reconocimiento facial, lo siguiente: *«En el ámbito laboral el uso de estas tecnologías podría considerarse una medida de control por el empresario, admitida por el artículo 20 ET siempre y cuando sea proporcional, lo que exigiría tener en cuenta la naturaleza de la actividad y de las instalaciones para cuyo acceso se requiriese el reconocimiento facial».*

"EN EL ÁMBITO LABORAL, EL USO DE ESTAS TECNOLOGÍAS PODRÍA CONSIDERARSE UNA MEDIDA DE CONTROL POR EL EMPRESARIO SIEMPRE Y CUANDO SEA PROPORCIONAL".

JUICIO DE PROPORCIONALIDAD

A pesar de que la AEPD admite que el uso de los sistemas de registro horario mediante el tratamiento de datos biométricos no es contrario a la normativa sobre protección de datos personales, exige proporcionalidad en la medida.

El documento de la 10ª Sesión Anual Abierta de la AEPD antes citado ya recogía que, en el ámbito laboral, el uso de estas tecnologías podría considerarse una medida de control por el empresario *"siempre y cuando sea proporcional, lo que exigiría tener en cuenta la naturaleza de la actividad y de las instalaciones"*. Aunque esto no es algo nuevo, ya que en informes anteriores a la entrada en vigor del RGPD, como el Informe 0392/2011, la Agencia ya nos hablaba de la necesidad de proporcionalidad en la medida a adoptar, en base a lo dictado por el Tribunal Constitucional:

«Siguiendo la doctrina emanada por el Tribunal Constitucional, el cumplimiento del principio de proporcionalidad exigirá superar los ***principios de idoneidad, necesidad y proporcionalidad****. (…) para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (****juicio de idoneidad****); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (****juicio de necesidad****); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)» No existiendo duda alguna de que el tratamiento de los datos biométricos resulta idóneo para alcanzar las finalidades de control perseguidas,* ***el problema estribará, precisamente en si en el supuesto planteado será posible alcanzar la finalidad perseguida a través de medios menos intrusivos en la esfera íntima del afectado con similar eficacia y si el uso de esta medida depara un mayor beneficio al interés general que el perjuicio que eventualmente pueda ocasionarse al afectado****. Ello irá, como se ha reiterado, vinculado al grado de necesidad de realización del tratamiento para el mantenimiento de la*

relación jurídica en que pretende justificarse el mismo… En resumidas cuentas, deberán eludirse en el análisis juicios genéricos que conduzcan a respuestas únicas que no atiendan a las circunstancias del caso, a partir, al menos, de los tres parámetros que acaban de indicarse. De este modo, no resultaría acorde a un adecuado juicio de proporcionalidad partir de la consideración de que el tratamiento de los datos biométricos debe siempre considerarse contrario a la legislación de protección de datos, dado que de hecho el legislador lo permite en determinadas ocasiones, como ya se ha indicado en relación con los identificadores únicos.».

En definitiva, podemos concluir que el uso de las tecnologías biométricas en el ámbito laboral debe considerarse una medida de control de naturaleza excepcional, que únicamente podría implementarse previo juicio favorable de proporcionalidad y necesidad de la medida.

"EL USO DE LAS TECNOLOGÍAS BIOMÉTRICAS EN EL ÁMBITO LABORAL DEBE CONSIDERARSE UNA MEDIDA DE CONTROL DE NATURALEZA EXCEPCIONAL, QUE ÚNICAMENTE PODRÍA IMPLEMENTARSE PREVIO JUICIO FAVORABLE DE PROPORCIONALIDAD Y NECESIDAD DE LA MEDIDA".

RESOLUCIONES DE LA AEPD EN RELACIÓN CON EL TRATAMIENTO DE DATOS BIOMÉTRICOS

En el Procedimiento Nº: PS/00128/2020, la AEPD sancionó a un Ayuntamiento que implantó un sistema de fichaje mediante huella dactilar. Apunta la AEPD que es innegable la posibilidad de utilización de sistemas basados en datos biométricos para llevar a cabo el control de acceso y horario, aunque señala que tampoco debe ser este el único sistema que puede ser usado. En cualquier caso, con carácter previo a la decisión sobre la puesta en marcha de un sistema de control de este tipo, expresa la necesidad de llevar a cabo una EIPD que, en este supuesto, se había realizado. La entidad fue sancionada por no dar cumplimiento al deber de información.

En el Procedimiento Nº: PS/00050/2021, la AEPD sancionó a una entidad por la utilización de un sistema biométrico de huella dactilar para el registro de la jornada laboral. En concreto, la sanción se impuso por no haber realizado una EIPD.

MATERIAL COMPLEMENTARIO

- Dictamen 3/2012, sobre la evolución de las tecnologías biométricas (GT29). Consulta este enlace.
- 14 equívocos con relación a la identificación y autenticación biométrica (AEPD). Consulta en este enlace.
- Tecnologías biométricas aplicadas a la ciberseguridad (INCIBE). Consulta este enlace.
- Consultas frecuentes (FAQS) de la Sede Electrónica de la AEPD. Consulta este enlace.
- Preguntas de los asistentes a la 10ª Sesión Anual Abierta de la Agencia Española de Protección de Datos, celebrada en fecha 4 de junio de 2018. Consulta este enlace.
- Informe 0036/2020 (AEPD), sobre cuestiones relativas al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online. Consulta este enlace.
- Dictamen Nº D17-005 (AVPD), relativo a la implantación de un sistema de control de acceso por huella biométrica a instalaciones municipales. Consulta este enlace.
- Lista de tipos de tratamientos de datos que requieren EIPD (AEPD). Consulta este enlace.
- Procedimiento Nº: PS/00050/2021 (AEPD). Consulta este enlace.
- Procedimiento Nº: PS/00128/2020 (AEPD). Consulta este enlace.

NOTICIAS

- **La Agencia Española de Protección de Datos (AEPD) colabora con el Supervisor Europeo de Protección de Datos en la publicación en español de las Guías sobre la necesidad y proporcionalidad de los tratamientos en políticas y medidas legislativas.**

  Estos documentos del Supervisor Europeo de Protección de Datos tienen como objetivo ayudar a las instituciones y organismos a diseñar y aplicar sus políticas o medidas legislativas respetando la Carta de los Derechos Fundamentales de la UE en lo relativo a los derechos a la intimidad y Protección de Datos. Consulta la Guía para evaluar la necesidad en este enlace, y la Guía para evaluar la proporcionalidad en este enlace.

- **La AEPD hace público el informe de notificaciones de brechas de seguridad de datos personales del mes de octubre de 2021.**

  En este informe se resumen las características principales de las notificaciones de brechas de datos personales recibidas en la Agencia Española de Protección de Datos (AEPD) en virtud del artículo 33 del Reglamento (UE) 2016/679, General de Protección de Datos. El informe recoge las notificaciones de brechas de datos personales recibidas durante octubre de 2021, siendo un total de 117 notificaciones. Destaca la Agencia que este mes han ocupado un lugar predominante las notificaciones de brechas de datos personales ocurridas en encargados de tratamiento y que afectan a múltiples responsables. Consultael informe en este enlace.