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 N.º 40 | Octubre 2023

USO DE DATOS BIOMÉTRICOS PARA EL CONTROL HORARIO

ÍNDICE

USO DE DATOS BIOMÉTRICOS PARA EL CONTROL HORARIO

INTRODUCCIÓN 2

1. NATURALEZA Y CONSIDERACIÓN DEL TRATAMIENTO 3

2. LICITUD DEL TRATAMIENTO DE DATOS BIOMÉTRICOS PARA EL CONTROL DE PRESENCIA.....5

3. PRINCIPIOS Y OBLIGACIONES 8

4. EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS (EIPD) 10

5. CONCLUSIONES 12

NOTICIAS 14

Os invitamos a trasladarnos aquellas temáticas que resulten de vuestro interés para los próximos cuadernos. 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 suscribirse a nuestro Cuaderno accede al siguiente enlace.

ÍNTRODUCCIÓN

El sistema de registro de jornada laboral mediante la captación de la huella dactilar de los empleados se ha extendido en los últimos años. El registro de jornada laboral se ha constituido en una obligación legal, recogida en el artículo 39 del Estatuto de los Trabajadores. Al ser la huella dactilar un dato de carácter personal, en el uso de la misma a los efectos del control horario, deberá respetarse la legislacion de protección de datos de carácter personal.

Es por esto que, en este Cuaderno analizamos todo lo relacionado con la **huella dactilar y la protección de datos**.

Como veremos, es preciso evaluar el tipo de sistema utilizado de acuerdo con su finalidad para poder determinar el camino de licitud que debe seguir. Deberá evaluarse si este sistema cumple con los principios de protección de datos, en particular, si los datos son adecuados, pertinentes y limitados a fines del tratamiento. No debe olvidarse que el uso de datos biométricos constituye, por defecto, un tipo de tratamiento altamente invasivo a la privacidad.

"Deberá evaluarse si el sistema de registro horario cumple con los principios de protección de datos, en particular, si los datos son adecuados, pertinentes y limitados a fines del tratamiento. No debe olvidarse que el uso de datos biométricos constituye, por defecto, un tipo de tratamiento altamente invasivo a la privacidad."

"Los datos biométricos presentan la particularidad de ser producidos por el propio cuerpo y lo caracterizan definitivamente."

1. NATURALEZA Y CONSIDERACIÓN DEL TRATAMIENTO

El artículo 4 del el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos, en adelante RGPD), bajo la rúbrica "*Definiciones*", dispone que:

"A efectos del presente Reglamento se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

El reconocimiento facial y la huella dactilar supone un tratamiento de datos biométricos, definidos en el artículo 4.14 del RGPD de la siguiente manera:

"datos biométricos»: 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."

Los datos biométricos presentan la particularidad de ser producidos por el propio cuerpo y lo caracterizan definitivamente.

Por lo tanto, son únicos, permanentes en el tiempo y la persona no puede liberarse de ellos, no se pueden cambiar nunca, ni con la edad, creando cuestiones de

responsabilidad en caso de compromiso-pérdida o intrusión en el sistema.

Son datos de cuyo uso pueden desprenderse riesgos significativos para los derechos fundamentales y las libertades y, por ello, inicialmente, está prohibido su uso, de conformidad con el artículo 9.1 del RGPD indicándose, además, en el artículo 9.4 del RGPD que:

"*Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud*".

"Los datos biométricos son únicos, permanentes en el tiempo y la persona no puede liberarse de ellos, no se pueden cambiar nunca, ni con la edad, creando cuestiones de responsabilidad en caso de compromiso-pérdida o intrusión en el sistema"

"Entre los principios relativos al tratamiento se encuentra el de la licitud, al que se refiere el artículo 5.1 a) del RGPD, cuando enuncia que los datos personales serán tratados de manera lícita en relación con el interesado."

2. LICITUD DEL TRATAMIENTO DE DATOS BIOMÉTRICOS PARA EL CONTROL DE PRESENCIA

Entre los principios relativos al tratamiento se encuentra el de la licitud, al que se refiere el artículo 5.1 a) del RGPD, cuando enuncia que los datos personales serán tratados de manera lícita en relación con el interesado. Por su parte, el artículo 6.1 del RGPD supedita la licitud de un tratamiento al cumplimiento de al menos una de las condiciones enumeradas en dicho artículo.

2.1. Ejecución de un contrato

En tal sentido, puesto que el tratamiento objeto de análisis responde a la finalidad de controlar el horario del personal, conviene precisar que la prestación de servicios en una Corporación Local se realiza comúnmente sobre la base de una relación jurídica laboral (personal laboral) o estatutaria de naturaleza administrativa (personal funcionario/interino).

Así, la base de licitud o legitimación para el tratamiento de datos a los fines previstos de control de presencia o de jornada podría encuadrarse en el supuesto del artículo 6.1 b) del RGPD: *"el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales"*, el cual, daría también cobertura al tratamiento de datos de los empleados públicos, aunque su relación no sea contractual en sentido estricto.

Al respecto, puede traerse a colación el contenido del artículo 20.3 del Estatuto de los Trabajadores (ET) sobre la potestad de adopción del empresario de la medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales.

2.2. Cumplimiento de una obligación legal

Específicamente para el personal laboral, podría acudirse incluso a considerar la legitimación por la vía del artículo

"La actual normativa legal española no se contiene autorización alguna para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo. A falta de previsión legal, la referida autorización o habilitación, podría estar prevista en los convenios colectivos para el personal laboral y en los acuerdos sobre condiciones de trabajo del personal funcionario en el marco de la negociación colectiva."

6.1.c) del RGPD: "*el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al tratamiento*", en conexión con el artículo 34.9 del ET que dispone la obligación para la empresa de garantizar un registro diario de jornada que deberá incluir el horario concreto de inicio y finalización de jornada de cada persona trabajadora. No obstante, debe tenerse en cuenta que el artículo 9.1. del RGPD, establece una regla general consistente en prohibir el tratamiento de determinadas categorías especiales de datos personales, entre los que se encuentran los *"datos biométricos"*.

En tal sentido, debe significarse que las Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), vienen a superar la posible interpretación de que dicha prohibición solo afectaría a los supuestos de datos biométricos dirigidos a la identificación de una persona a través de la comparación de sus datos con una o varias bases de datos que identifican a un conjunto de personas (proceso de búsqueda de correspondencia "*uno a varios*"), **extendiéndola también** a los supuestos de datos biométricos dirigidos a la autenticación o verificación de la persona con respecto al patrón previamente establecido para la misma (proceso de búsqueda de correspondencia "*uno a uno*").

Únicamente cabe excepcionar la referida prohibición de tratamiento de los datos de categoría especial, cuando concurra alguna de las circunstancias que se especifican en el artículo 9.2. del RGPD. En este caso la letra b) establece que 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, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado"*, partiendo de la premisa de que la aplicabilidad de la excepción puede referirse también al

ámbito funcionarial, tal y como expresa el informe jurídico de la AEPD 0002/2022.

Esta excepción, en el Estado Español, debe entenderse referida la existencia de una norma previsora de rango legal por tratarse del desarrollo de un derecho, el de la protección de datos, reconocido como fundamental. Al hilo de lo indicado, puede afirmarse que en la actual normativa legal española no se contiene autorización alguna para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo: ni para el personal laboral, ni para el personal funcionarial.

A falta de previsión legal, la referida autorización o habilitación, podría estar prevista en los convenios colectivos para el personal laboral y en los acuerdos sobre condiciones de trabajo del personal funcionario en el marco de la negociación colectiva, siempre con el establecimiento de las garantías adecuadas respecto a los derechos fundamentales y de los intereses de los afectados.

"Únicamente podría considerarse la existencia de un consentimiento libre si el interesado dispone de una alternativa de libre elección para cumplir con el control horario o de presencia, de modo que pueda atenderse a los interesados sin que se tenga que realizar un tratamiento de sus datos biométricos."

2.3. Consentimiento explícito

También podría considerarse el levantamiento de la prohibición del tratamiento de datos biométricos por concurrencia de la prestación del consentimiento explícito por parte del interesado para el tratamiento de dichos datos personales, según se establece en el artículo 9.2 a) del RGPD. Ahora bien, debe evaluarse si su prestación o no prestación *"puede depararle al interesado algún tipo de perjuicio o ha de producir algún tipo efecto desfavorable que condicione precisamente la libertad con la que ha de ser emitido"*.

Trasladado esto al supuesto que nos ocupa, únicamente podría considerarse la existencia de un consentimiento libre si el interesado dispone de una alternativa de libre elección para cumplir con el control horario o de presencia, de modo que pueda atenderse a los interesados sin que se tenga que realizar un tratamiento de sus datos biométricos.

3. PRINCIPIOS Y OBLIGACIONES

El tratamiento, de producirse, deberá cumplir también con el resto de principios y obligaciones derivados de la normativa de protección de datos. En concreto, el Dictamen 3/2012 del Grupo de Trabajo del artículo 29, sobre la evolución de tecnologías biométricas, afirma lo siguiente en relación con el análisis del cumplimiento:

*"Al analizar la **proporcionalidad** de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no sólo lo más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la **necesidad** en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar. Un tercer aspecto a ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la **idoneidad** de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado."*

"El tratamiento, de producirse, deberá cumplir también con el resto de principios y obligaciones derivados de la normativa de protección de datos."

Parece clara la necesidad de admitir la instalación de sistemas de control del cumplimiento horario por parte del personal. Ahora bien, no parece tan claro que la utilización de sistemas de control horario basados en datos biométricos tengan que ser admitidos como medio preferente para llevar a cabo al control. Más bien al contrario. Atendida la especial naturaleza de estos datos habrá que optar, en primer lugar, por otros sistemas de control que, sin utilizar categorías de datos especialmente protegidos, puedan permitir lograr la misma finalidad.

Por otra parte, se enumeran a continuación una serie de directrices y obligaciones:

- El trabajador debe ser informado sobre el tratamiento.

"Parece clara la necesidad de admitir la instalación de sistemas de control del cumplimiento horario por parte del personal. Ahora bien, no parece tan claro que la utilización de sistemas de control horario basados en datos biométricos tengan que ser admitidos como medio preferente para llevar a cabo al control. Más bien al contrario. Atendida la especial naturaleza de estos datos habrá que optar, en primer lugar, por otros sistemas de control que, sin utilizar categorías de datos especialmente protegidos, puedan permitir lograr la misma finalidad."

- El principios de limitación de la finalidad deber respetarse junto con los demás principios de protección de datos: especialmente, los de necesidad, proporcionalidad y minimización de datos.

- El tratamiento deberá ser adecuado, pertinente y no excesivo en relación con dicha finalidad. Por tanto, los datos biométricos que no sean necesarios para esa finalidad deben suprimirse y no siempre se justificará la creación de una base de datos biométricos.

- Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible. La plantilla deberá extraerse de una manera que sea específica para el sistema biométrico en cuestión y no utilizada por otros responsables del tratamiento de sistemas similares a fin de garantizar que una persona solo pueda ser identificada en los sistemas biométricos que cuenten con una base jurídica para esta operación.

- El sistema biométrico utilizado y las medidas de seguridad elegidas deberán asegurarse de que es imposible o al menos rastreable la reutilización de los datos biométricos en cuestión para otra finalidad.

- Deberán utilizarse mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de datos biométricos.

- Los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad.

- Deberá optarse por utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.

- Los datos biométricos deben ser suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento y, si fuera posible, deben implantarse mecanismos automatizados de supresión de datos.

"Al tratarse el sistema de registro y uso de huellas de sistemas de identificación novedosos y muy intrusivos para los derechos y libertades fundamentales de las personas físicas, el RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone esos tratamientos".

4. EVALUACIÓN DE IMPACTO EN PROTECCIÓN DE DATOS (EIPD)

El RGPD establece la obligación, de acuerdo con su art. 35, de gestionar el riesgo que para los derechos y libertades de las personas supone un tratamiento. Este riesgo surge tanto por la propia existencia del tratamiento, como por las dimensiones técnicas y organizativas del mismo. La realización de una EIPD es únicamente obligatoria cuando el tratamiento "*entrañe probablemente un alto riesgo para los derechos y libertades de las personas físicas*".

Al tratarse el sistema de registro y uso de huellas de sistemas de identificación novedosos y muy intrusivos para los derechos y libertades fundamentales de las personas físicas, el RGPD establece la obligación de gestionar el riesgo que para los derechos y libertades de las personas supone esos tratamientos.

El tratamiento biométrico presenta entre otros los **siguientes riesgos**:

- La definición del tamaño (cantidad de información) de la plantilla biométrica es una cuestión crucial.
- Riesgos que conlleva la utilización de datos biométricos para fines de identificación en grandes bases de datos centralizadas, dadas las consecuencias potencialmente perjudiciales para las personas afectadas.
- No hace falta decir que toda pérdida de las cualidades de integridad, confidencialidad y disponibilidad con respecto a las bases de datos sería claramente perjudicial para cualquier aplicación futura basada en la información contenida en dichas bases de datos, y causaría asimismo un daño irreparable a los interesados.
- La transferencia de la información contenida en la base de datos.

"La implantación del sistema de registro horario sin realizar la preceptiva EIPD conforme a todo lo anteriormente expuesto, dado el alto riesgo que supone el tratamiento para los derechos y las libertades de los empleados, constituye una clara infracción del RGPD".

- Se puede crear la ilusión de que la identificación a través de la huella siempre es correcta, por ello se debe incluir un análisis de los errores que se pueden producir en su uso, medidores de evaluación del rendimiento, tasa de falsa aceptación-probabilidad de que un sistema biométrico identifique incorrectamente a un individuo o no rechace a un individuo que no pertenece al grupo, y tasa de falso rechazo o falso negativo: no se establece la correspondencia entre una persona y su propia plantilla.

- Deben adoptarse medidas de seguridad con motivo del tratamiento de datos biométricos (almacenamiento, transmisión, extracción de características y comparación, etc.) y sobre todo si el responsable del tratamiento transmite esos datos a través de Internet.

- Se acepta generalmente que el riesgo de reutilización de datos biométricos obtenidos a partir de rastros físicos dejados por personas sin darse cuenta (por ejemplo: huellas digitales) para fines incompatibles es relativamente bajo si los datos no están almacenados en bases de datos centralizadas, sino en poder de la persona y son inaccesibles para terceros.

- Riesgos evidentes si la tecnología empleada no garantiza de manera suficiente que la plantilla obtenida a partir de los datos biométricos no coincidirá con la empleada en otros sistemas similares.

En consecuencia de todo ello, la implantación del sistema de registro horario sin realizar la preceptiva EIPD, conforme a todo lo anteriormente expuesto, dado el alto riesgo que supone el tratamiento para los derechos y las libertades de los empleados, constituye una clara **infracción del RGPD.**

"Los datos biométricos son una categoría especial de datos personales, por lo que su tratamiento debe considerarse, en principio prohibido, conforme a lo dispuesto en el artículo 9.1 del RGDP. No obstante, a los efectos de adoptar el registro de jornada mediante esta tecnología biométrica, puede hallarse salvedad en el artículo 9.2.a) y b) RGPD ".

5. CONCLUSIONES

a) El uso de dispositivos de reconocimiento facial y/o huella dactilar con la finalidad de un control horario del personal de una Administración Pública implica un tratamiento de datos personales biométricos, sujeto a la normativa de protección de datos.

b) La base de legitimación para el tratamiento de datos con fines de control laboral podría encontrarse en la relación contractual, así como en el cumplimiento de una obligación legal, este último exclusivamente para el personal laboral.

c) Los datos biométricos son una categoría especial de datos personales, por lo que su tratamiento debe considerarse, en principio prohibido, conforme a lo dispuesto en el artículo 9.1 del RGDP.

d) El levantamiento de la referida prohibición no puede ampararse en la actualidad en la concurrencia de la circunstancia prevista en el artículo 9.2 b) del RGPD puesto que en la actual normativa legal española no se contiene autorización para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo. A falta de tal previsión legal, la referida autorización o habilitación podría preverse en los convenios colectivos para el personal laboral y en los acuerdos sobre condiciones de trabajo del personal funcionario en el marco de la negociación colectiva.

e) El levantamiento de la prohibición basada en la concurrencia de la circunstancia del consentimiento explícito del interesado prevista en el artículo 9.2.a), debe analizarse con cautela ante la situación de desequilibrio entre dicho interesado y la Administración Pública responsable del tratamiento. Podría considerarse únicamente si se dispone de una alternativa de libre elección para cumplir el control horario o de presencia y si el consentimiento es

informado, inequívoco y demostrable por el responsable del tratamiento.

f) El tratamiento de datos biométricos con la finalidad de control de presencia deberá cumplir con el resto de principios y obligaciones derivados de la normativa de protección de datos, destacando el de minimización (artículo 5.1 c) del RGPD).

g) El responsable del tratamiento de datos biométricos con la finalidad de control de presencia realizará antes del tratamiento la evaluación del impacto relativa a la protección de datos establecida en el artículo 35 del RGPD.

"El responsable del tratamiento de datos biométricos con la finalidad de control de presencia realizará antes del tratamiento la evaluación del impacto relativa a la protección de datos establecida en el artículo 35 del RGPD."

MATERIAL COMPLEMENTARIO

- Dictamen 1/2023 publicado por el Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA) en este enlace.
- Resolución de procedimiento sancionador, Expediente Nº: EXP202208695, publicado por la Agencia Española de Protección de Datos (AEPD) en este enlace.
- Dictamen CNS 2/2022 publicado por la Agència Catalana de Protecció de Dades (APDCAT) en este enlace.
- Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público, en este enlace.
- Dictamen CNS 21/2020 publicado por la Agència Catalana de Protecció de Dades (APDCAT) en este enlace.
- Dictamen 3/2012 sobre la evolución de las tecnologías biométricas publicado por el Grupo de Trabajo del Artículo 29 (GT29), en este enlace.

NOTICIAS

Las Administraciones Públicas y autoridades en protección de datos publican varias noticias de interés:

1. **Informe sobre denegación de información sobre los méritos presentados en un proceso de selección en trámite.**

   La APDCAT considera que, en ejercicio del derecho de defensa y a los efectos de poder comprobar eventuales actuaciones arbitrarias del órgano calificador contrarias a los principios de igualdad, mérito, capacidad y transparencia que deben regir en cualquier procedimiento del mismo tipo, resultaría justificado que la persona solicitante pudiera disponer de información sobre los diferentes aspectos que se hayan podido valorar en el proceso selectivo, tales como los conocimientos y las capacidades (mediante el acceso a los exámenes y/o pruebas efectuadas), los méritos (tanto académicos como de experiencia) y la puntuación obtenida. Consulta el Informe en este enlace.

2. **Informe sobre Denegación de acceso a expedientes disciplinarios de la policía local.**

   La APDCAT entiende que la normativa de protección de datos no impide el acceso de la persona reclamante a la información relativa a los empleados públicos que hubiesen intervenido en las diferentes actuaciones de investigación previa y expedientes disciplinarios ya resueltos, que no hayan participado en las conductas irregulares, salvo que concurra alguna circunstancia excepcional. Ahora bien, el acceso a los expedientes puede facilitarse a través del mecanismo de la anonimización o bien, cuando esta medida no sea efectiva, a través de un resumen de los expedientes, de forma que en ningún caso sean identificables las personas físicas afectadas (personas investigadas y, en su caso, denunciantes o bien de testigo). Consulta el Dictamen en este enlace.