Resolución de la AEPD relativa al tratamiento de la huella dactilar en el ámbito laboral

Datos biométricos: licitud, transparencia y evaluación de impacto del tratamiento.

Marzo 2021

Ponte en contacto con PwC Tax & Legal:

Assumpta Zorraquino Rico
Socia responsable de Regulación Digital en PwC Tax & Legal
assumpta.zorraquino@pwc.com

Inmaculada Lleberia Sedó
Abogada en el área de Regulación Digital de PwC Tax & Legal
inmaculada.lleberia.sedo@pwc.com

1. Cuestiones previas

El procedimiento sancionador se incoa a raíz de la reclamación presentada por un empleado de un ayuntamiento ante la AEPD, en méritos de la cual denunciaba que el citado ente público no había dado respuesta a su solicitud de información relacionada con el tratamiento de su huella dactilar para el control de acceso y fichaje.

Tras el requerimiento de información efectuado por la AEPD, el ayuntamiento aportó un Documento de Seguridad en el cual, entre otras cuestiones, indicaba:

i. que utilizaba como **control de presencia y acceso un sistema de detección de huella dactilar** que no realizaba en ningún momento un análisis biométrico, sino que elaboraba un algoritmo identificativo a raíz de una lectura de varios puntos de la huella personal y

ii. que los datos del algoritmo **no podían ser descifrados** ni desmontados por ninguna entidad no autorizada.

Adicionalmente, en virtud de un segundo requerimiento de información, el ayuntamiento aportó un informe sobre la Evaluación de Impacto realizada para el tratamiento de las huellas dactilares de sus empleados.

2. Hechos Probados

De las actuaciones practicadas en el procedimiento sancionador y la documentación aportada quedan probados a juicio de la AEPD los siguientes hechos:

- Que en fecha 07/05/2019 tiene entrada en la AEPD un escrito presentado por el interesado contra el reclamado, manifestando que se dirigió al mismo **solicitándole la aportación de información** sobre el control de fichaje mediante huella dactilar, sin que a día de la fecha haya obtenido respuesta a dicha solicitud.
- Que se aporta por el reclamante carta dirigida al reclamado solicitando la información de conformidad con el RGPD.
- Que consta aportado por el reclamado el **Informe de Evaluación de Impacto del tratamiento del dato de la huella dactilar para control de presencia de los empleados**, junto con el Documento de Seguridad y documento de empresa Syon, Soluciones & Identificación, sobre huellas dactilares de los trabajadores.

En el presente número analizamos la resolución del procedimiento sancionador PS/ N.º 00128/2020 dictada por la AEPD. Contra un ayuntamiento al que le impone como sanción un apercibimiento por haber infringido el deber de información previsto en el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), respecto del tratamiento de la huella dactilar de sus empleados."

3. Análisis del tratamiento de datos basado en la huella dactilar

Tras analizar la información aportada por el organismo investigado, la AEPD procede a determinar los requisitos y recomendaciones que deben respetarse para llevar a cabo un tratamiento lícito, leal, transparente y proporcionado, de conformidad con el RGPD.

Se relacionan, a continuación, los referidos requisitos y las recomendaciones emitidas por la AEPD respecto de los tratamientos basados en la huella dactilar:

a) Cumplimiento del deber de informar:

A pesar de tratarse de una cuestión obvia, la AEPD recuerda que la implantación e integración de un sistema de **control horario basado en la huella dactilar por parte del empleador ha de ser informado** a los empleados de manera completa, clara, concisa y, además, la citada información debe ser completada con referencia tanto a las bases legales que den cobertura a dicho tipo de control de acceso, como a la información básica a la que hace referencia en el artículo 13 del RGPD.

b) Tipología de datos tratados:

La AEPD determina que la huella dactilar debe ser calificada como **dato biométrico.**

Asimismo, matiza que, tal como pone de relieve el considerando 51 del RGPD**, los datos biométricos son de categoría especial en los supuestos de identificación biométrica** (art. 9.1 RGPD). Consecuentemente, ello implica que, de conformidad con el artículo 9.1 del RGPD, se les aplique el régimen específico previsto para las categorías especiales de datos contenido en el artículo 9 del RGPD.

Llegados a este punto, conviene recordar que **no todo dato biométrico implicará por defecto el tratamiento de datos de categorías especiales.** En este sentido, la AEPD ha declarado que, *"el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, ya que el artículo 9.1. se refiere a los "datos biométricos dirigidos a identificar de manera unívoca a una persona física", por lo que, de una interpretación conjunta de ambos preceptos parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física".*

Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la **distinción entre *"identificación biométrica"* y *"autenticación biométrica"*** que ya establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas (véase, a tales efectos, la resolución de la AEPD N/REF: 010308/2019):

- **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).
- **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).

Por consiguiente, sólo en los casos de *"identificación biométrica"* la huella dactilar será considerada, además de dato biométrico, dato de categoría especial.

En el presente número analizamos:

La resolución del procedimiento sancionador PS/ N.º 00128/2020 dictada por la AEPD, en fecha 1 de marzo de 2021, contra un ayuntamiento al que le impone como sanción un apercibimiento por haber infringido el deber de información previsto en el artículo 13 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (RGPD), respecto del tratamiento de la huella dactilar de sus empleados.

En dicha resolución la AEPD analiza en detalle las características e implicaciones de los tratamientos basados en la huella dactilar con fines de control de acceso y jornada laboral, estableciendo de forma clara los requisitos que este tipo de tratamientos deben cumplir para entender que son lícitos, leales, transparentes y proporcionados.

En definitiva, la AEPD se pronuncia de forma expresa sobre cuestiones que hasta la fecha no habían sido tratadas con este detalle.

c) Base legitimadora para el tratamiento de datos:

Como bien es sabido a etas alturas, todo tratamiento de datos requiere de la concurrencia de una de las bases legitimadoras previstas en el artículo 6 de RGPD.

Respecto de la base legitimadora para el tratamiento de los datos objeto de este análisis, la AEPD se remite al artículo **6 del RGPD apartado 1, letra b),** el cual dispone que "El tratamiento será lícito si se cumple al menos una de las siguientes condiciones: (…) b) 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 (…)". En virtud de este precepto, el tratamiento sería lícito y no requeriría el consentimiento, cuando el tratamiento de datos se realice para el cumplimiento de relaciones contractuales de carácter laboral. En este punto la AEPD precisa que dicho precepto legal daría cobertura también al tratamiento de datos de los empleados públicos, aunque su relación no sea contractual en sentido estricto.

Por otra parte, y tal como pone de relieve el considerando 51 del mismo RGPD, **en la medida en que los datos biométricos son de categoría especial en los supuestos de identificación biométrica** (art. 9.1 RGPD), será necesario que concurra, -además de una de las bases legitimadoras establecidas en el artículo 6 del RGPD-, alguna de las **excepciones previstas en el artículo 9.2** del RGPD, que permitirían levantar la prohibición general del tratamiento de estos tipos de datos establecida en el artículo 9.1.

En este punto hay que hacer especial mención de la letra b) del artículo 9.2 del RGPD, según la cual la prohibición general de tratamiento de datos biométricos no será 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, 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".*

Al respecto la AEPD declara que en el ordenamiento español, el artículo 20 del Texto refundido del Estatuto de los trabajadores (TE), aprobado por el Real decreto legislativo 2/2015, de 23 de octubre, prevé la posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales de sus trabajadores. En este sentido, el citado precepto legal establece lo siguiente:

> *"Art.20.3 ET:*
> *El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad".*

d) Evaluaciones de impacto:

Respecto de las Evaluaciones de Impacto, la AEPD declara expresamente que *"**En cualquier caso,** con carácter previo a la decisión sobre la puesta en marcha de un sistema de control de este tipo y teniendo en cuenta sus implicaciones, tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física, **sería preceptivo llevar a cabo una evaluación de impacto** relativa a la protección de datos de carácter personal".*

Por ello, cualquier tratamiento de datos que implique el recabado y uso de la huella dactilar requerirá de la previa realización de una Evaluación de Impacto en la privacidad de las personas.

4. Recomendaciones y medidas a implementar por parte del responsable del tratamiento

La AEPD pone de manifiesto que el avance de las tecnologías biométricas permite la distinción de diversos tipos de tratamientos, señalando que *"Los datos biométricos pueden tratarse y almacenarse de diferentes formas. A veces, la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar o una grabación de voz. Otras veces, la información biométrica bruta capturada es tratada de manera que solo se extraen ciertas características o rasgos y se salvan como una plantilla biométrica."*

Tal y como se viene indicando, el tratamiento de estos datos estará expresamente permitido por el RGPD cuando el empresario cuente con una base legitimadora que le habilite al tratamiento de los mismos, que, tal y como se ha adelantado, por regla general será el propio contrato de trabajo.

Sin embargo, a pesar de que el tratamiento de datos basados en la huella dactilar disponga de base legitimadora, la AEPD advierte del hecho que el tratamiento de esta tipología de datos debe cumplir, además, con los siguientes requisitos:

i. Respeto de los **principios de limitación de la finalidad, necesidad, proporcionalidad y minimización de datos.**
ii. Uso de **plantillas biométricas:** Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible y deberá extraerse de forma 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 legitimadora para esta operación.
iii. El sistema biométrico utilizado y las medidas de seguridad elegidas deberán **garantizar que no es posible la reutilización de los datos** biométricos en cuestión para otra finalidad.
iv. Uso de mecanismos basados en **tecnologías de cifrado,** a fin de evitar la lectura, copia, modificación o supresión no autorizadas de los datos biométricos.
v. Posibilidad de **anonimizar los datos.** Al respecto, la AEPD dispone que los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad.
vi. Utilización de formatos de datos o tecnologías específicas **que imposibiliten la interconexión** de bases de datos biométricos y la divulgación de datos no comprobada.
vii. Supresión de los datos biométricos cuando no se vinculen a la finalidad que motivó su tratamiento. Adicionalmente, si fuera posible, deberán implementarse mecanismos **automatizados** de supresión de datos.

5. Sanción

En el presente caso, la AEPD considera que el ayuntamiento ha cometido una infracción del artículo 13 del RGPD, **sancionándole como consecuencia de ello con un apercibimiento** de conformidad con el artículo 77.2 de la LOPDGDD, y acuerda requerir al ayuntamiento para que, en el plazo de un mes desde la notificación de la resolución, acredite ante la AEPD **la adopción de las medidas necesarias y pertinentes para corregir** los tratamientos de datos que no se adecuan a la normativa en materia de protección de datos de carácter personal y evitar que vuelvan a producirse vulneraciones como las que han dado lugar a la reclamación objeto del procedimiento sancionador analizado.

6. Conclusiones

La realización de cualquier tratamiento de datos que implique el uso de la huella dactilar requerirá de la previa realización de la correspondiente **Evaluación de Impacto y de la determinación e implementación de las medidas técnicas y organizativas necesarias** para garantizar la debida protección de los datos y la proporcionalidad del tratamiento en sí. Es altamente recomendable el empleo de mecanismos que posibiliten la anonimización de este tipo de datos, especialmente, en aquellos casos en que los datos biométricos ostenten la condición de “categorías especiales de datos”.

Adicionalmente, el uso de nuevas tecnologías biométricas deberá ser debidamente evaluado por parte del responsable del tratamiento, en la medida que éstas pueden resultar altamente intrusivas para los derechos y libertades de los interesados, particularmente, en aquellos casos en los que exista una relación jerárquica entre el responsable y el interesado, como sucede en el ámbito laboral.

Finalmente, no puede perderse de vista que para llevar a cabo el control de acceso y de jornada laboral, **no siempre será necesario tratar datos biométricos.** Al respecto la AEPD considera que el sistema biométrico **tampoco parece que *“sea o deba ser el único sistema que puede ser usado”*.** Así deberá valorarse si puede recurrirse a otros sistemas basados, por ejemplo, en el uso de tarjetas personales, la utilización de códigos personales, la visualización directa del punto de marcaje, etc., que pueden constituir, por sí mismos o en combinación con alguno de los otros sistemas disponibles, medidas igualmente eficaces para llevar a cabo el control pretendido por el empresario.

El presente documento ha sido preparado a efectos de orientación general sobre materias de interés y no constituye asesoramiento profesional alguno. No deben llevarse a cabo actuaciones en base a la información contenida en este documento, sin obtener el específico asesoramiento profesional. No se efectúa manifestación ni se presta garantía alguna (de carácter expreso o tácito) respecto de la exactitud o integridad de la información contenida en el mismo y, en la medida legalmente permitida. PricewaterhouseCoopers Tax & Legal Services, S.L., sus socios, empleados o colaboradores no aceptan ni asumen obligación, responsabilidad o deber de diligencia alguna respecto de las consecuencias de la actuación u omisión por su parte o de terceros, en base a la información contenida en este documento o respecto de cualquier decisión fundada en la misma.
Para cualquier solicitud de alta, baja o cambio de dirección no dude en ponerse en contacto con nosotros o en la dirección: data.protection.office@pwc.com
© 2021 PricewaterhouseCoopers Tax & Legal Services, S.L. Todos los derechos reservados. "PwC" se refiere a PricewaterhouseCoopers Tax & Legal Services, S.L., firma miembro de PricewaterhouseCoopers International Limited; cada una de las cuales es una entidad legal separada e independiente.