Nº 86 noviembre 2023

“Datos biométricos ….. donde dije digo”

La Sentencia del Tribunal de Justicia de la UE Sala Quinta (TJUE) de 26 de enero de 2023 dictada en el asunto C-205/21 que tiene por objeto una petición de decisión prejudicial planteada por el Tribunal Penal Especial de Bulgaria, ha marcado un antes y un después en el tratamiento de datos biométricos en el marco de la normativa europea de protección de datos de carácter personal seguido por la nueva doctrina del Comité Europeo de Protección de Datos.

Esta sentencia resuelve dos cuestiones prejudiciales conjuntamente relacionadas con la Directiva 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, a la luz de la Carta de Derechos Fundamentales de la UE en relación con la pregunta de si el Derecho del Estado miembro autoriza a que las autoridades policiales recojan datos biométricos y genéticos para sus actividades de investigación con fines de lucha contra la delincuencia y de mantenimiento del orden público.

Esta petición al TJUE se presentó en el contexto de un procedimiento penal incoado contra una ciudadana que, a raíz de ser investigada, se negó a que la policía recogiera sus datos biométricos y genéticos a efectos de su registro.

La cuestión que se discute es si las autoridades policiales pueden llevar a cabo el tratamiento de los datos biométricos sobre la base jurídica de que dicho tratamiento se ampara en artículo 9 del Reglamento General de Protección de Datos (RGPD) que establece las condiciones de tratamiento de las categorías especiales de datos, en un marco jurídico interno donde las disposiciones nacionales parecen establecer requisitos contradictorios en cuanto a la legitimidad de esa recogida y tratamiento de dichos datos.

El TJUE declara que, la Directiva que regula el tratamiento de datos personales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, permite que el Derecho del cada Estado miembro autorice, con arreglo a la misma, el tratamiento de datos biométricos y genéticos por parte de las autoridades policiales a efectos de sus actividades de investigación, con fines de lucha contra la delincuencia y de mantenimiento del orden público, siempre que el Derecho de ese Estado miembro contenga una base jurídica suficientemente clara y precisa que lo autorice.

Y concluye que, no es contrario ni a la citada Directiva ni a la Carta de Derechos Fundamentales de la UE que una norma nacional de un Estado miembro establezca que, en caso de que la persona investigada por un delito público doloso se niegue a colaborar voluntariamente en la recogida de sus datos biométricos y genéticos a efectos de su registro, el órgano jurisdiccional penal competente está obligado a autorizar una medida de recogida forzosa, si aprecia que si existen motivos fundados para presumir que la persona ha cometido la infracción penal por la que es investigada, siempre que el Derecho nacional garantice posteriormente el control jurisdiccional efectivo de las condiciones de esa investigación, de la que deriva la autorización para la recogida.

No se opone, por tanto, a que en caso de que la persona investigada por un delito público doloso se niegue a colaborar en la recogida de sus datos biométricos y genéticos, un órgano jurisdiccional penal autorice de forma obligatoria la recogida forzosa de los datos, inclusive sin poder apreciar si existen motivos fundados para presumir que el interesado ha cometido la infracción penal por la que es investigado, siempre que el Derecho nacional garantice posteriormente el control jurisdiccional efectivo de las condiciones de esa investigación.

Aunque advierte que, la Directiva si se opone a que una norma nacional de un Estado miembro establezca que la recogida sistemática de datos biométricos y genéticos de cualquier persona investigada por un delito público doloso a efectos de su registro, pueda llevarse a cabo sin una obligación para la autoridad competente a comprobar y demostrar, por una parte, que esa recogida es estrictamente necesaria para satisfacer los objetivos concretos perseguidos y, por otra parte, que tales objetivos no pueden lograrse mediante medidas que constituyan injerencias menos graves en los derechos y libertades del interesado.

Tras la citada sentencia, el Comité Europeo de Protección de Datos (EDPB por sus siglas en inglés) actualizó en abril de 2023 su Guía de reconocimiento facial en el ámbito de aplicación de la ley, con el fin de proporcionar unas directrices a los legisladores y a las autoridades de los Estados miembros sobre el uso de la tecnología de reconocimiento facial y lo hizo de la forma más restrictiva posible con relación al tratamiento de datos biométricos partiendo de la premisa general de que, el tratamiento de datos biométricos constituye en cualquier circunstancia *una intromisión grave en sí misma.*

El documento está destinado a ser utilizado para su consideración por los Estados Miembros a la hora de evaluar futuras medidas legislativas y administrativas, así como al implementar la legislación existente que involucre tecnologías de reconocimiento facial, *"caso por caso".*

De hecho, en la Guía, el EDPB advierte a los Estados Miembros de que antes de que el legislador nacional cree una nueva base jurídica para cualquier forma de tratamiento de datos biométricos mediante reconocimiento facial, se debe consultar a la autoridad de control de protección de datos competente (en España, la Agencia Española de Protección de Datos) puesto que, un objetivo de interés general –por fundamental que sea– no justifica, por sí solo, una limitación de un derecho fundamental como es el derecho a la protección de datos.

Así, la Guía pone de manifiesto que el uso de tecnologías de reconocimiento facial está intrínsecamente vinculado al tratamiento de datos personales de categoría especial, con un impacto directo o indirecto en una serie de derechos fundamentales consagrados en la Carta de Derechos Fundamentales de la UE, siendo particularmente relevante en el área de aplicación de la ley y justicia penal, por ello, aunque es comprensible la necesidad de que las autoridades encargadas de hacer cumplir la ley se beneficien de las mejores herramientas posibles para identificar rápidamente a los autores de actos terroristas y otros delitos graves, sin embargo, tales herramientas deben utilizarse en estricto cumplimiento del marco jurídico aplicable y solo en los casos en que cumplan los requisitos de necesidad y proporcionalidad, porque, puesto que, *si bien las tecnologías modernas pueden ser parte de la solución, de ninguna manera son una "solución milagrosa".*

Inclusive, hay ciertos casos de uso de tecnologías de reconocimiento facial que plantean riesgos inaceptablemente elevados para los individuos y la sociedad (*las llamadas "líneas rojas"*), motivo por el cual, el EDPB y el Supervisor Europeo de Protección de Datos (por sus siglas en inglés, EDPS) han pedido su prohibición general (estos casos pueden verse en la Opinión conjunta del EDPB y el EDPS sobre la propuesta de Ley de Inteligencia Artificial).

La Guía concluye que el uso del reconocimiento facial impacta directa o indirectamente en una serie de derechos y libertades fundamentales consagrados en la Carta de la UE de Derechos Fundamentales que pueden ir más allá de la privacidad y la protección de datos, como la dignidad humana, libertad de movimiento, libertad de reunión, y otros.

Esto es particularmente relevante en el área del derecho en aplicación de la ley y justicia penal y aunque reconoce la necesidad de que las autoridades encargadas de hacer cumplir la ley se beneficien de las mejores condiciones posibles, incluso del uso de herramientas para identificar rápidamente a los autores de actos terroristas y otros delitos graves, sin embargo, tales herramientas *deben utilizarse en estricto cumplimiento del marco legal aplicable y sólo en los casos en que cumplir los requisitos de necesidad y proporcionalidad* establecidos en el artículo 52, apartado 1, de la Carta de Derechos Fundamentales.

En este contexto pero tres años antes, la Agencia Española de Protección de Datos (AEPD), en el año 2020, con una resolución mediática en el sector de las técnicas biométricas y en el marco de las relaciones laborales, la Resolución E07273-2020, concluía, respecto de la implantación de un sistema de control de horario mediante huella dactilar que, había que acudir a la distinción entre identificación biométrica (*proceso de búsqueda de correspondencias uno-a-varios*) y la verificación/autenticación biométrica (*proceso de búsqueda de correspondencias uno-a-uno sobre dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona*).

Así, en el año 2020 la AEPD interpretaba que dicho tratamiento de datos biométricos sería lícito para el cumplimiento de relaciones contractuales de carácter laboral (inclusive el tratamiento de datos de los empleados públicos aunque su relación no sea contractual en sentido estricto) siempre que se tratase de procesos de búsqueda de correspondencia "*uno-a-uno"* (procesos de verificación/autenticación) sobre la base 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".*

De esta forma, a criterio de la AEPD tanto el artículo 20 del Estatuto de los trabajadores *(posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales)*, como el artículo 54 del Estatuto Básico del Empleado Público, *(el desempeño de las tareas correspondientes a su puesto de trabajo se realzará de forma diligente y cumpliendo la jornada y el horario establecidos*) constituían base jurídica suficiente para el uso de sistemas basados en datos biométricos con el fin de llevar a cabo el control de acceso y horario, reconociendo en todo caso que, para el desarrollo de estas funciones laborales servían otros medios sin tratamiento de datos biométricos como tarjetas personales, códigos personales, puntos de marcaje u otros igualmente eficaces para llevar a cabo el control laboral y menos invasivos para el derecho a la protección de datos.

Más adelante, en mayo de 2021, la AEPD publicaba su Guía de relaciones laborales, en la que se abordaba en el apartado "Los datos biométricos" del capítulo 4.6 el empleo de biometría en la implementación de los tratamientos de registro de presencia, interpretando la autenticación biométrica fuera de las categorías especiales de datos.

Pero, como se suele decir, "*de aquellos barros estos lodos*" y tras los recientes pronunciamientos del TJUE y el EDPB en relación con el uso de datos biométricos, el pasado 23 de noviembre en curso, la AEPD ha publicado una nota de prensa para anunciar su nueva Guía sobre tratamientos de control de presencia mediante sistemas biométricos y "*donde dije digo, digo Diego*" de forma que, tanto para identificación como para autenticación, la AEPD, siguiendo el camino marcado por el TJUE y el EDPB, considera el tratamiento de datos biométricos *"un tratamiento de alto riesgo de categorías especiales de datos"* y para poder tratar esas categorías es necesario la concurrencia de una circunstancia que levante la prohibición de su tratamiento recogida en el artículo 9 del RGPD y de una condición que lo legitime.

Y en este sentido, según la AEPD, para el control de presencia en el ámbito laboral (que incluye tanto la función de registro de jornada como la de control de acceso con fines laborales) mediante técnicas biométricas de identificación o autenticación, las entidades responsables (empresas y administraciones públicas) deben contar con una norma con rango de ley que concrete la posibilidad de utilizar datos biométricos para dicha finalidad, lo cual advierte la AEPD que *no se encuentra en la actual normativa legal española*, sin que, *ni el consentimiento de las personas interesadas ni la ejecución del contrato de trabajo o relación de empleo público, sean circunstancias que levanten la prohibición del artículo 9 del RGPD*.

Así, en caso en que la entidad responsable de dichos tratamientos considere la necesidad de proponer operaciones biométricas para dichas funciones laborales, deberá justificar las circunstancias por las que no es posible utilizar los sistemas de registro de presencia que se estaban empleando en el mismo centro hasta ese momento, o que se están empleando en entidades equivalentes. Además, deberá justificar que el empleo de otros sistemas existentes como tarjetas, certificados, claves, sistemas contact-less, etc. que evitan el tratamiento de categorías especiales de datos biométricos no son adecuados.

Como indica la AEPD en su guía, los sistemas automáticos de control de jornada existen desde 1890 y el registro de presencia se ha realizado durante varios siglos a través de medios no biométricos, como se evidencia en el hecho de que, por poner un ejemplo, en los años 80 del siglo XX existían más de doce millones de trabajadores en España sometidos a control de jornada y la mayor factoría de vehículos en España tenía en esa época más de 30.000 trabajadores (cifra que actualmente no llega a la mitad) y el empleador disponía de potestad y capacidad para establecer un control de jornada eficaz.

Advierte la AEPD que, la interpretación que ella misma realizaba en su guía "La Protección de Datos en las Relaciones Laborales" en el *capítulo 4.6 "Los datos biométricos"* dejando fuera de las categorías especiales de datos la autenticación biométrica empleada en la implementación de los tratamientos laborales de registro de presencia (para el registro de jornada y el control de acceso con fines laborales), ha sido superada por las Directrices antes citadas, por lo que la interpretación de esta AEPD ha de adaptarse a las Directrices del CEPD mencionadas de 26 de abril de 2023. Por si no queda claro, en otras palabras, en la actualidad no hay legitimación suficiente en nuestro Derecho para utilizar datos biométricos en sistemas laborales de control de presencia. Y, *"donde dije digo.. digo Diego"*

Ana Marzo
EQUIPO MARZO
Mediadora inscrita en el Registro de Mediadores e
Instituciones de Mediación del Ministerio de Justicia