UN ANÁLISIS DE URGENCIA DE LA BIOMETRÍA UTILIZADA PARA EL REGISTRO DE LA JORNADA, RESULTADO: CATEGORÍA DE DATOS DE ALTO RIESGO

AN URGENT ANALYSIS OF THE BIOMETRICS USED TO RECORD THE DAY, RESULT: HIGH-RISK DATA CATEGORY

M.ª Elisa Cuadros Garrido
Codirectora Revista Justicia & Trabajo
https://orcid.org/0000-0003-0297-5330

I. DELIMITACIÓN

Los sistemas de registro horario utilizados por las empresas son muy diversos: fichar de manera telemática, utilización de tarjetas personales u otros tipos de objetos token en un sistema de marcado, uso de códigos personales, sistemas de videovigilancia donde quede constancia de la hora de entrada o salida, el control biométrico, etc.[1] La cuestión es que en base a la interpretación actual de la normativa de protección de datos, se aconseja la desinstalación de los medios de control del trabajador más intrusivos por riesgo potencial de los derechos fundamentales del empleado y de posibles sanciones por la AEPD.

1 La forma de proceder de los llamados sistemas de autenticación por posesión y por conocimiento, respectivamente, se realiza a través de un método tradicional de identificación personal que efectúa la autenticación del individuo a través de algo que se posee (una llave, una tarjeta de identificación, etc.), y/o se sabe (una clave, un PIN, etc.). Sin embargo, un sistema biométrico constituye un método de reconocimiento en el que la identidad de un individuo es determinada a partir de alguna de sus características fisiológicas o de comportamiento.

La creciente demanda de acceso a los servicios de la Sociedad de la Información ha dado lugar en las últimas décadas a la aparición de una rama de la Tecnología denominada autenticación biométrica o, simplemente, biometría[2]. El Reglamento General Protección Datos (RGPD)[3] define en su art. 4.14 «los datos biométricos» como 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».

El Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo[4] regula en el Capítulo III «Medidas de lucha contra la precariedad laboral en la jornada de trabajo», y en el art. 10 estableció por primera vez en nuestro ordenamiento jurídico, únicamente existía la obligación de registro para el caso de que el trabajador tuviera un contrato a tiempo parcial[5] o realizase horas extraordinarias art. 35.5 Estatuto de los Trabajadores[6], (ET). A través de una modificación del art. 34 del ET, añadiendo un nuevo apartado 9, el registro horario se introdujo en la norma

2 Un sistema biométrico podría definirse como «un sistema automático que permite el reconocimiento de seres vivos a través de sus rasgos inherentes». Una clasificación sencilla de las tecnologías biométricas se realiza en función de las características de estas: 1.º) Rasgos fisiológicos. Son aquellos que corresponden a características estáticas diferenciadoras del cuerpo humano de índole principalmente física. Ejemplos de ello son la huella dactilar, iris y retina, geometría de la mano, reconocimiento facial. 2.º) Rasgos de comportamiento. Son rasgos que están más relacionados con la conducta de la persona corresponden a características dinámicas. A esta categoría pertenecerían, por ejemplo, firma manuscrita, tecleo, paso, voz… Los principales componentes que se pueden identificar en un sistema biométrico son: 1.º) El sensor. Es el dispositivo de captura de los rasgos o características biométricas. Para registrar y convertir los rasgos biométricos en datos de computador se necesitan sensores adecuados. 2.º) El repositorio. Es la base de datos donde se almacenan las plantillas biométricas inscritas para su comparación. Estas plantillas, deberían protegerse en un área física segura, cifradas y firmadas digitalmente. 3.º) Los algoritmos para extracción de características (procesamiento) y comparación.

3 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos.

4 Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo. «BOE» núm. 61, de 12 de marzo de 2019, páginas 23156 a 23181.

5 Art. 12.4, apartado c) del ET señala que «la jornada de los trabajadores a tiempo parcial se registrará día a día y se totalizará mensualmente, entregando copia al trabajador, junto con el recibo de salarios, del resumen de todas las horas realizadas en cada mes, tanto las ordinarias como las complementarias».

6 Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores. BOE, núm. 255, de 24/10/2015. Como se especifica en el apartado V de la Exposición de motivos del citado Real Decreto Ley 8/2019, el propósito de la obligación establecida tiene como objetivo garantizar el cumplimiento de los límites en materia de jornada, crear un marco de seguridad jurídica tanto para las personas trabajadoras como para las empresas y posibilitar el control por parte de la Inspección de Trabajo y Seguridad Social, como medio para corregir la situación de precariedad, bajos salarios y pobreza que afecta a muchos de los trabajadores que sufren los abusos en su jornada laboral.

laboral[7]. En relación con el control de acceso con fines laborales, éste se suele fundamentar en la previsión contenida en el art. 20.3[8] del ET. La norma no detalla cómo se puede llevar a cabo el registro, limitándose a señalar que se debe realizar de manera diaria e incluir el momento de inicio y la finalización de la jornada, la concreción de dicho extremo se remite a la negociación colectiva, o en su caso, al acuerdo de empresa.

El mayor problema que pueden plantear los datos biométricos en relación con el control empresarial es la posible colisión con los derechos fundamentales de los trabajadores a la intimidad y a la protección de datos. Respecto al grado de afectación en el empleado de estas tecnologías, se nos afirma, ahora por la AEPD, que hay que optar en el registro de la jornada con una evaluación de alternativas equivalentes y menos intrusivas que las biométricas, se recomienda que se exploraren opciones que no sean únicamente tecnológicas. Ya hace más de una década se afirmó que cabía predecir que, salvo escasas situaciones en las que pudiera apreciarse una necesidad real de implantar un sistema de seguridad muy estricto, el resultado del «juicio de proporcionalidad» en la mayor parte de casos posiblemente derivaría en una conclusión contraria[9].

La AEPD no duda en afirmar que los distintos productos disponibles en el mercado para la recogida de datos biométricos que registran dichos datos con una precisión, detalle o frecuencia que están muy por encima de las necesidades de un determinado tratamiento específico y vulneran el principio de minimización recogido en el art. 5 RGPD[10].

Por su parte, la jurisprudencia ha resuelto litigios en relación con los medios que están utilizando las empresas para hacer efectiva esta obligación, sirva como botón de muestra, la STJUE de 14 de mayo de 2019, Gran Sala, C-55/2018 *Caso Federación de Servicios de Comisiones Obreras (CCOO) contra Deutsche Bank*[11], que considera contraria al Derecho de la

7 «La empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo. Mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores en la empresa, se organizará y documentará este registro de presencia. La empresa conservará los registros a que se refiere este precepto durante cuatro años y permanecerán a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social».

8 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».

9 Selma Penalva, Alejandra: «El control de accesos por medio de huella digital y sus repercusiones prácticas sobre el derecho a la intimidad de los trabajadores», *Revista Doctrinal Aranzadi Social* núm. 3, 2010.

10 Art. 5 apartado 1 letra c), RGPD recoge que los datos serán: «adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);» El considerando 39 explica muy claramente que unos datos que no son necesarios para cumplir con la finalidad del tratamiento no deben ser tratados: «…Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios…»

11 STJUE de 14 de mayo de 2019, C-55/2018 (ECLI:EU:C:2019:402). El auto de la AN 19 enero 2018 (ECLI:ES:AN:2018: 2.ª) planteó cuestión prejudicial al TJUE en el sentido de si resultaba exigible no

Unión, en concreto, la Directiva 2003/88/CE respecto a la Ordenación del tiempo de trabajo[12], con la regulación española en la que en aquel momento no contemplaba, expresamente, la obligación empresarial de llevar un registro de la jornada diaria[13]. Cabe precisar que para el TJUE es necesario implantar «un sistema objetivo, fiable y accesible» de registro horario; se ha de adoptar por parte del empresario un instrumento que permita determinar objetivamente y de manera fiable el número de horas de trabajo diario y semanal, a fin de que se respeten los períodos mínimos de descanso y para impedir que se sobrepase la duración máxima del tiempo de trabajo semanal. Y el TJUE considera *idóneo* un sistema de registro de jornada como instrumento objetivo.

Para la AEPD, los datos biométricos siempre han sido son datos personales, porque cumplen las de notas definición de dato personal, pero en lo que se ha evolucionado es en el grado de calificación de ese dato y en consecuencia de protección de este. Como norma general, el uso de la biometría para las exigencias generales de seguridad de los bienes y las personas no puede considerarse un interés legítimo que prevalezca sobre los intereses o los derechos y libertades fundamentales del interesado. Por el contrario, el tratamiento de datos biométricos solo puede justificarse como un instrumento necesario para asegurar los bienes o las personas cuando se disponga de pruebas, sobre la base de las circunstancias objetivas y documentadas, de la existencia de un riesgo considerable.

La Agencia Española de Protección de Datos publicó en mayo de 2021 la guía «La Protección de Datos en las Relaciones Laborales»[14], 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, en el texto se interpretaba la autenticación biométrica fuera de las categorías especiales de datos[15].

sólo a los trabajadores a tiempo parcial, ferroviarios, de marina mercante y trabajadores móviles, sino también a los empleados a tiempo completo, la existencia de un control diario de la jornada trabajada y de los excesos de jornada.

12 DIRECTIVA 2003/88/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 4 de noviembre de 2003 relativa a determinados aspectos de la ordenación del tiempo de trabajo, DOUE 18-11-2003, L 299/9.

13 Esta sentencia, sin duda, vino avalar la reforma operada por Real Decreto-Ley 8/2019, de 8 de marzo.

14 *https://www.aepd.es/documento/la-proteccion-de-datos-en-las-relaciones-laborales*

15 En su informe de 2021 la AEPD distinguía dos clases de usos de los datos biométricos:
-*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). La AEPD sostenía con carácter general, que los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a- varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).

II.CAUSANTES DEL CAMBIO

2.1. Comité Europeo de Protección de Datos

El Comité Europeo de Protección de Datos[16] (CEPD), a través de *las Directrices 05/2022*[17] *sobre el uso de técnicas de reconocimiento facial en el ámbito de la aplicación de la ley,* estableció, finalmente, en mayo de 2023, que los datos biométricos siempre serán datos de categoría especial, tanto los supuestos de identificación como de autenticación. Las implicaciones de esta interpretación por parte del CEPD son de envergadura, ya que determinan que, para poder llevar a cabo cualquier tratamiento de datos biométricos, tanto identificación como autenticación, se exige la concurrencia no solo de alguno de los supuestos recogidos en el art. 6.1 del RGPD relativos a licitud del tratamiento de datos, sino también de alguna de las circunstancias previstas el art. 9.2[18] del RGPD.

16 Antes era el Grupo de Trabajo del Artículo 29 (GT29). El Comité Europeo de Protección de Datos fue creado en 2018, su misión esencial es garantizar que el Reglamento General de Protección de Datos y la Directiva sobre protección de datos en el ámbito penal se apliquen de manera coherente en los países de la UE, así como en Noruega, Liechtenstein e Islandia.
https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_es

17 *Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement* https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_202304_frtlawenforcement_v2_en.pdf Adoptadas el 12 de mayo de 2022 y sometidas a consulta pública hasta el 22 de junio 2022. Aprobadas el 17 de mayo de 2023, habiendo actualizado y añadido algunas recomendaciones. El CEPD pese a distinguir en el punto 10 de las directrices (página 7) igualmente dos supuestos en las técnicas biométricas:
-Autenticación, con el fin de verificar que una persona es quien dice ser. En este caso, el sistema comparará una plantilla o muestra biométrica pregrabada, como la de una persona que se presente en un puesto de control, para verificar si se trata de una y la misma persona. Por lo tanto, esta funcionalidad se basa en la comparación de dos plantillas, uno a uno.
-Identificación, dirigida a encontrar a una persona entre un grupo de individuos, en un área específica, una imagen o una base de datos. En este caso, el sistema debe realizar una prueba en la muestra biométrica capturada para generar una plantilla biométrica y comprobar si coincide con una persona conocida por el sistema. Por lo tanto, esta funcionalidad se basa en comparar una plantilla con una base de datos de plantillas o muestras, uno a varios. Y en el punto 12 de las directrices (página 8) establece: «Si bien ambas funciones (autenticación e identificación) son distintas, ambas se relacionan con el tratamiento de datos biométricos relacionados con una persona física identificada o identificable y, por lo tanto, constituyen un tratamiento de datos personales y, más específicamente, un tratamiento de categorías especiales de datos personales».

18 Art. 9.2 RGPD» 2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
b) 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 se-

Las actividades que supone la biometría; identificación y autenticación, son operaciones que no están definidas en el RGPD, no obstante, sí que se encuentran reguladas en otra normativa de ámbito europeo como es el Reglamento 910/2014, del Parlamento Europeo y del Consejo, de 23 de julio de 2014[19], conocido comúnmente como *Reglamento eIDAS*[20], en su art. 3 del se definen los términos de la siguiente manera:

– «Identificación electrónica», el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.

---

guridad 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;
c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,
j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el art. 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado».

19 REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, DOU 28-8-2014 L 257/73.

20 El Reglamento *eIDAS* pretende ayudar a las empresas, los ciudadanos y las autoridades a llevar a cabo interacciones electrónicas seguras y sin fisuras.

– «Autenticación», un proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.

La norma considera a la autenticación como un proceso electrónico que posibilita la identificación. De una manera informal o intuitiva, cabe explicar el concepto de identificación como el proceso por el cual se reconoce a un individuo particular dentro de un grupo, comparándose los datos del individuo que se desea identificar con los datos de cada individuo en el grupo (uno-a-varios). La verificación o autenticación sería el proceso de probar que es cierta la identidad reclamada por un individuo, comparándose los datos del individuo únicamente con los datos asociados a la identidad reclamada (uno-a-uno).

La consideración de categoría especial de datos debe interpretarse de manera amplia. El art. 9.1 del RGPD establece que categorías especiales de datos son aquellos que «revelen» cierto tipo de información. El concepto «revelen» debe entenderse en el sentido que, además de los datos que por su naturaleza contienen información sensible, también constituyen categorías especiales los datos de los que *puede deducirse* información sensible relativa a una persona. En apoyo de esta afirmación, se manifestó hace dos décadas[21] la STJUE 8 6 noviembre 2003, *Bodil Lindqvist*, C-101/01[22], «con relación al propósito de la Directiva de Protección de Datos[23], en relación con la expresión «datos relativos a la salud» el tribunal consideraba que debía tener una interpretación amplia para incluir la información concerniente a todos los aspectos, físicos y mentales, de la salud de un individuo».

La concepción de los datos biométricos como categorías especiales de datos, debe tener en cuenta la posibilidad de que, mediante el análisis biométrico, se puedan inferir y recoger otras categorías especiales de datos y, en particular, datos relativos a la salud o datos que revelen el origen racial o étnico entre otros. La especial protección que establece el RGPD en su art. 9 a determinadas categorías de datos[24] deriva del impacto que el tratamiento de estos datos puede tener en los derechos fundamentales y libertades de las personas. Únicamente cabe excepcionar la prohibición de tratamiento de los datos de categoría especial cuando concurra alguna de las circunstancias que se especifican en el apartado 2 del art. 9 del RGPD. El responsable tiene la obligación de valorar muy seriamente y con diligencia si

21 La conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un «tratamiento total o parcialmente automatizado de datos personales» en el sentido del art. 3, apartado 1, de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
2) Un tratamiento de datos personales de esta naturaleza no está comprendido en ninguna de las excepciones que figuran en el art. 3, apartado 2, de la Directiva 95/46.

22 STJUE 8 TJUE, 6 noviembre 2003, Bodil Lindqvist, C-101/01 (ECLI:EU:C:2003:596).

23 Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos, DOC núm. 281, de 23 de noviembre de 1995, páginas 31 a 50.

24 Art. 9 RGPD «Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física».

tiene una razón sólida para tratar categorías especiales que aparezca enumerada en dicho art. 9.2 del RGPD. El interés legítimo, la ejecución de un contrato o medidas precontractuales no se encuentran entre las excepciones enumeradas.

En el art. 9 del RGPD, apto. 2, letra b), se levanta la prohibición del tratamiento de categorías especiales de datos 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».

Cabe indicar que la mención a la autorización por el Derecho de los Estados miembros de la UE debe entenderse referida, en el caso del Estado Español, a la existencia de una norma previsora de rango legal[25] en consonancia con lo dispuesto en el art. 53.1 de la Constitución Española, por tratarse del desarrollo de un derecho, el de la protección de datos personales, reconocido como derecho fundamental en el art. 18.4 CE.

Por último, quedar poner de relieve que la conclusión del CEPD es totalmente contraria, a la que se alcanzó en octubre de 2023 por parte de la autoridad de protección de datos británica, *Information Comissioner's Office* (ICO) que, consideró que si se proporciona un método alternativo para aquellos empleados que deseen optar por no usar datos biométricos, y los trabajadores no están en desventaja con dicha decisión, el consentimiento es la base legal más probable para aplicar al uso de datos biométricos para el control de acceso.

25 La STC núm. 76/2019, de 22 de mayo, precisa que la norma legal debe reunir todas las características indispensables como garantía de la seguridad jurídica, expresando todos y cada uno de los presupuestos y condiciones de la intervención, de forma que las limitaciones del derecho fundamental establecidas por una ley pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad.

2.2. STJUE 22 junio 2023 C-579/21, Pankki

La STJUE de 22 de junio de 2023, C-579/21, *Pankki*[26], pese a ser muy reciente, su relevante doctrina ya ha sido retirada por el TJUE en varias ocasiones por incumplimiento de la normativa de protección de datos, mereciendo destacarse las SSTJUE 7 diciembre 2023 C-634/21 *Land Hessen*[27], 26 octubre 2023 C-307/2022[28].

La STJUE 22 junio 2023 C-579/21, resuelve la reclamación de un empleado y cliente del banco *finés Suomalainen Pankki*[29] que había detectado que por parte de personal de su

26 STJUE (Sala Primera) 22 junio 2023, C-579/21, *Pankki* (ECLI:EU:C:2023:501).

27 STJUE (Sala Primera) 7 diciembre 2023 C-634/21, (ECLI:EU:C:2023:957). Se plantea cuestión prejudicial por el tribunal alemán *Verwaltungsgericht Wiesbaden* (Tribunal de lo Contencioso-Administrativo de Wiesbaden) sobre si se infringe el art. 22 del RGPD por la negativa a instar la financiera SCHUFA Holding AG a que accediera a la solicitud presentada por OQ al objeto de tener acceso a determinados datos personales que la concernían y de suprimirlos porque se basaban en Inteligencia Artificial (IA) (Decisiones individuales automatizadas, elaboración de perfiles) y tal información podía perjudicar al interesado para futuros préstamos. Se declara que se lesiona el art. 22 RGPD ya que «la generación automatizada, por una agencia de información comercial, de un valor de probabilidad a partir de datos personales relativos a una persona y acerca de la capacidad de esta para hacer frente a compromisos de pago en el futuro constituye una «decisión individual automatizada», en el sentido de la mencionada disposición, cuando de ese valor de probabilidad dependa de manera determinante que un tercero, al que se comunica dicho valor, establezca, ejecute o ponga fin a una relación contractual con esa persona».

28 STJUE (Sala Primera) 26 octubre 2023 C- 307/2022 (ECLI:EU:C: 2023:811). Se plantea cuestión prejudicial por el Bundesgerichtshof (Tribunal Supremo Federal de lo Civil y Penal, Alemania). El litigio entre FT y DW, en versa en relación con la negativa de FT, dentista, de facilitar a su paciente gratuitamente una primera copia de su historia clínica. El TJUE recoge no se permite adoptar una normativa nacional que, con el fin de proteger los intereses económicos del responsable del tratamiento, imponga al interesado los gastos de una primera copia de sus datos personales objeto del tratamiento. Ya que en el marco de una relación médico-paciente, el derecho a obtener una copia de los datos personales objeto de tratamiento implica que se entregue al interesado una reproducción fiel e inteligible de todos esos datos. Este derecho conlleva el de obtener una copia íntegra de los documentos recogidos en su historia clínica que contengan, entre otros, dichos datos, si la entrega de tal copia es necesaria para permitir al interesado verificar su exactitud y exhaustividad, así como para garantizar su inteligibilidad. Por lo que respecta a los datos relativos a la salud del interesado, este derecho incluye, en todo caso, el de obtener una copia de los datos de su historia clínica que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas».

29 Al albergar dudas sobre la licitud de esas consultas, el trabajador, que entretanto había sido despedido de su puesto en S-Pankki, solicitó, el 29 de mayo de 2018, que le comunicara la identidad de las personas que habían consultado sus datos como cliente, las fechas exactas de las consultas y los fines del tratamiento de dichos datos. En su respuesta de 30 de agosto de 2018, Pankki, se negó a comunicar la identidad de los trabajadores que habían llevado a cabo las operaciones por considerar que esa información constituía datos personales de esos trabajadores. el Supervisor Adjunto de Protección de Datos denegó la solicitud de J. M. Explicó que el objeto de tal solicitud era permitirle acceder a los datos de protocolo de los empleados que habían tratado sus datos, cuando, en virtud de su práctica decisoria, tales archivos no constituyen datos personales relati-

empleadora se había accedido al registro del fichero de sus datos en la entidad financiera. Los datos de protocolo cuyo acceso fue denegado al trabajador correspondían a registros de actividades, en el sentido del art, 30 del RGPD y, posteriormente, fue despedido. En el procedimiento prejudicial[30] se cuestiona el alcance del derecho de acceso a la información del RGPD, art. 4 y 15, en sus apartados 42 a 46. El TJUE *secciona* varios términos que considera claves y son los siguientes:

- La expresión *toda información* en la definición del concepto de *datos personales*, del art. 4.1 RGPD, pone de relieve que el objetivo del legislador de la UE de atribuir al término un significado muy amplio, que puede abarcar todo género de información, tanto objetiva como subjetiva, en forma de opiniones o apreciaciones, siempre que sean *sobre* la persona en cuestión[31]; una información se refiere a una persona física identificada o identificable cuando, debido a su contenido, finalidad o efectos, la información está relacionada con una persona identificable.El carácter *identificable*[32] de una persona, supone que una definición amplia del concepto de *datos personales* que abarca los datos recabados y conservados por el responsable del tratamiento, e incluye toda la información resultante de un tratamiento de datos personales que se refiera a una persona identificada.

- El concepto de *tratamiento*, tal como se regula en el art. 4, punto 2, del RGPD, supone *cualquier operación*, esto significa productos aplicados a datos personales o conjuntos de datos personales, que comprenden, entre otras cosas, la recogida, el registro, la conservación o incluso la consulta.

La primera cuestión prejudicial que se plantea es en relación con el ámbito de aplicación temporal del RGPD. Se considera aplicable la normativa a la solicitud de acceso a la información del empleado del banco *Pankki* ya que, aunque las operaciones de tratamiento a que se refiere la solicitud se habían efectuado antes de la fecha en que empezó a ser aplicable el RGPD, la petición del trabajador se presentó después su entrada en vigor.

Respecto a la doble condición de persona trabajadora y cliente de un banco que el tribunal que plantea la cuestión prejudicial había preguntado si influía como exención del deber de información, el TJUE responde que no concurre, así declara en el hecho de que el responsable del

vos al interesado, sino a los empleados que trataron los datos de esa persona. J. M. interpuso un recurso contra esa decisión ante el órgano jurisdiccional remitente. El órgano en cuestión, *Itä-Suomen hallinto-oikeus* (Tribunal de lo Contencioso-Administrativo de Finlandia Oriental, Finlandia), plantea cuestión prejudicial y pregunta si la comunicación de los datos de protocolo generados con ocasión de las operaciones de tratamiento, que contienen tal información, en particular, la identidad de los empleados del responsable del tratamiento está comprendida en el ámbito de aplicación del art. 15 RGPD, dado que esos archivos podrían resultar necesarios para que el interesado pudiera apreciar la licitud del tratamiento de que han sido objeto sus datos.

30 A petición de decisión prejudicial planteada, con arreglo al art. 267 TFUE, por el *Itä-Suomen hallinto-oikeus* (Tribunal de lo Contencioso-Administrativo de Finlandia Oriental, Finlandia), mediante resolución de 21 de septiembre de 2021, recibida en el Tribunal de Justicia el 22 de septiembre de 2021.

31 Como ya decía la STJUE 4 mayo 2023, Österreichische Datenschutzbehörde y CRIF, C-487/21, EU:C:2023:369, apartado 23).

32 El considerando 26 del RGPD precisa que deben tenerse en cuenta *todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.*

tratamiento desarrolle un negocio bancario en el marco de una actividad reglada y de que la persona cuyos datos personales fueron tratados en su condición de cliente del responsable del tratamiento también fuera empleada de ese responsable no tiene efectos jurídicos, en principio, en el alcance del derecho del que goza ese interesado en virtud de la citada disposición[33].

El TJUE afirma que el art. 30, apartado 4, del RGPD regula que se pondrán a disposición los datos solicitados de la autoridad de control que lo solicite cuestión que en el supuesto enjuiciado que no se cumplió. El empleado del banco *Pankki* tenía derecho a la información relativa a las operaciones de consulta de sus datos personales, a las fechas y a los fines de estas operaciones, porque tal extremo constituye información que tiene el derecho a obtener del responsable del tratamiento según el RGPD. Por el contrario, a la información relativa a la identidad de los empleados que llevaron a cabo esas operaciones, no se tiene derecho salvo que la excepción concurra concurra[34].

2.3. Tribunal Supremo

2.3.1. Precedentes

La doctrina de la Sala III de la STS 2 de julio de 2007[35] recogió lo siguiente: «La novedad o complejidad de un sistema de biometría, no lo convierte en lesivo de los derechos fundamentales y que el recurso a la tecnología escogida es plenamente admisible al no haber norma que lo prohíba, no se aportan elemento alguno que pruebe que dicho sistema fuera nocivo para la salud».

En el orden social, la STS 19 diciembre 2005[36] anuló un sistema de biometría en la empresa por haberse saltado el trámite de audiencia al comité de empresa, mientras que la STS 16 septiembre 2015[37] se pronunció sobre la pausa del bocadillo de veinte minutos, tras la implantación de un sistema de biometría por huella dactilar, que había sustituido a un sistema anterior de acceso al trabajo por tornos, pero no cuestionó el nuevo mecanismo de control, porque el conflicto colectivo versaba sobre la pérdida de ese tiempo como parte de la jornada de trabajo. Por último, la STS 2 febrero 2017[38] válida la utilización por parte de un gimnasio de cámaras de videovigilancia al conocer el trabajador su existencia en el centro de trabajo, como dato curioso, hay que mencionar que todos los socios del establecimiento accedían al mismo por biometría. Estos ejemplos, nos ponen de relieve que la cuestión que nos ocupa, no se ha enjuiciado por la Sala IV del TS como principal, desde el punto de vista de la posible lesión de esos datos biométricos a los derechos fundamentales del trabajador. Pero los pronunciamientos *ut infra*, validan mecanismos de registro de jornada favorables al trabajador y no intrusivos, por lo que no resulta arriesgado afirmar que el TS, aún sin haberse pronunciado de manera expresa como sin duda hará, opta por otros medios más suaves, en consonancia con la doctrina TJUE, como el Alto Tribunal recoge.

33 Considerando 89.

34 A menos que esa información sea indispensable para permitir al interesado ejercer efectivamente los derechos que le confiere el RGPD y siempre bajo la condición de que se tengan en cuenta los derechos y libertades de esos empleados.

35 STS 2 de julio de 2007, rec. 5017/2003.

36 STS 19 diciembre 2005 rec.138/2005

37 STS 16 septiembre 2015, rec. 330/2014, (ECLI:ES:TS:2015:4417).

38 STS 2 febrero 2017 (ECLI:ES:TS: 2017:817).

2.3.2. Caso Zurich

La STS 5 abril 2022[39] confirma la SAN 29 octubre 2019[40] y declara válido el pacto suscrito entre empresa y la mayoría sindical se acuerda que el registro de la jornada consista en el acceso por parte de la persona trabajadora al ordenador asignado introduciendo el usuario o al conectarse a la red vía VPN. Además, se aplica un factor corrector genérico, de 2 horas/día en jornada partida y 30 minutos/día en jornada continuada, para contemplar descansos, pausa para la comida y/o desayuno, permisos no retribuidos, cualquier clase de pausa o descanso, etc.

2.3.3. Caso CECA

La STS 18 enero 2023[41] considera que cumple los requisitos de ser objetivo, fiable y accesible el auto registro telemático de la jornada implantado por la Confederación Española de Cajas de Ahorros (CECA) conforme exige la STJUE 14 mayo 2019 (asunto C-55/18). Es acorde con la normativa que sea el propio trabajador el que haya de reflejar diariamente en la aplicación informática de la empresa las horas de inicio y finalización de la jornada de trabajo, las interrupciones y periodos de descanso, pues lo riesgos potenciales que se invocan no pueden erigirse como determinantes de la validez del sistema, teniendo en cuenta las particularidades propias de cada sector de actividad e incluso las especificidades de determinadas empresas. En consecuencia, se valida, el acuerdo de registro de jornada entre empresa y sindicatos firmantes del convenio sobre el modelo auto declarativo, al considerarlo objetivo y fiable (SAN 9 diciembre 2020[42]).

2.4. Autoridad Catalana de Protección de Datos

El Dictamen 2/2022[43], de la Autoridad Catalana de Protección de Datos[44], recoge que el consentimiento del personal no puede considerarse una base jurídica adecuada para la implantación de un sistema de control horario mediante reconocimiento facial, porque *dado que no puede considerarse que en el caso planteado pudiera existir un consentimiento realmente libre*. En cualquier caso, La Autoridad Catalana considera que antes de la implantación de un sistema de estas dimensiones, es preciso hacer una evaluación del impacto sobre la protección de datos a la vista de las circunstancias concretas en que se lleve a cabo el tratamiento para determinar la licitud y la proporcionalidad, incluida el análisis de la existencia de alternativas menos intrusivas, y establecer las garantías adecuadas que «la afectación por el derecho a la protección de datos que se derive de la norma debe ser previsible» y que «no se puede considerar previsible la norma si no concreta la posibilidad de utilizar datos biométricos con el fin de realizar el control horario».

39 STS 5 abril 2022, rec.7/2020 (ECLI:ES:TS:2022:1434).
40 SAN 29 octubre 2019, proc. núm. 188/2019 (ECLI:ES:AN: 2019:4065).
41 STS 18 enero 2023, rec. núm. 78/2021 (ECLI:ES:TS: 2023:85).
42 SAN 9 diciembre 2020 Proc. 218/2020, (ECLI:ES:AN:2020:3596).
43 Dictamen en relación con la consulta formulada por un Ayuntamiento relativa a la conformidad con la normativa de protección de datos del uso de dispositivos de control de presencia en el puesto de trabajo mediante reconocimiento facial.
44 https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2022/Documents/es_cns_2022_002.pdf

2.5. Consejo de Transparencia y Protección de Datos de Andalucía

El Consejo de Transparencia y Protección de Datos de Andalucía, en su Dictamen 1/2023[45], «Relativo al tratamiento de categorías especiales de datos biométricos mediante el uso de dispositivos de reconocimiento facial y/o huella dactilar para el control horario del personal de un Ayuntamiento», concluye que en la actual normativa legal española no se contiene autorización suficientemente específica alguna para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo.

III. GUÍA DE LA AEPD SOBRE TRATAMIENTOS DE CONTROL DE PRESENCIA MEDIANTE SISTEMAS BIOMÉTRICOS NOVIEMBRE 2023

La Resolución AEPD de 21 de julio de 2022 del expediente 218/2021[46] declaró que la instauración de un sistema de registro diario de jornada laboral de los empleados a través de técnica de reconocimiento facial no era acorde al art. 18. 4 CE. La AEPD destacaba que en que no se trataba del primer tipo de reclamación que, por la técnica de biometría, habiendo resuelto algunas. Sin embargo, si era la primera vez que la cuestión estaba relacionada con el tratamiento de datos como entidad empleadora que decide utilizar el registro y almacenamiento de datos originados por el RF para la finalidad de registro diario de jornada laboral. Y concluía que el control horario de la jornada laboral diaria sólo alcanza a la obligación de realizarla, pero no a realizarla utilizando datos biométricos, y su uso, sin causa de excepción para el tratamiento,

Los precedentes anteriores han llevado a la AEPD a replantearse la situación y a la publicación en noviembre de 2023 de la guía AEDP sobre *Tratamiento de control de presencia mediante sistemas biométricos*[47] con la que modifica el anterior criterio de 2021, basándose en que no es obligatorio, ni recomendable, que la implementación de un tratamiento, se limite exclusivamente a la selección de recursos tecnológicos.

45 https://www.ctpdandalucia.es/sites/default/files/inline-files/dictamen-1-2023.pdf
46 https://www.aepd.es/documento/ps-00218-2021.pdf
47 *https://www.aepd.es/documento/guia-control-presencia-biometrico.pdf*

Entre las opciones de establecer un determinado tratamiento hay que considerar, entre otros, la utilización de recursos humanos, las garantías jurídicas y los procedimientos organizativos, en definitiva, se aboga por la introducción de un factor humano frente a una automatización del control de accesos en el puesto de trabajo. Cabe preguntarse la razón del cambio de criterio de la AEPD que se justifica en una relectura y replanteamiento del RGPD y fundamentalmente en los siguientes preceptos:

– **Art. 9.2.b**

Con relación al tratamiento en el ámbito del Derecho laboral y de la seguridad y protección social, no solo exige que exista una habilitación legal o convenio colectivo, sino que impone en primer término el requisito de que el tratamiento sea «necesario».

– **Art. 9.2.b**

En todo caso, dicha ley —o convenio colectivo— que establece el tratamiento deberá respetar el principio de proporcionalidad,

– **Art. 9.2.a**

En relación con la excepción de control de presencia para registro de jornada, control de acceso con fines laborales o no, cabría considerar 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 con uno o más de los fines especificados. En el caso del registro de jornada laboral, como el interesado tiene la obligación de registrar su jornada, únicamente podría considerarse la existencia de un consentimiento libre a un tratamiento adicional de datos, en este caso biométricos, si el interesado dispone de una alternativa de libre elección para cumplir con dicha obligación. Cuando existan opciones realmente equivalentes y disponibles para todos los trabajadores, se podría estudiar si el consentimiento fuese válido, cumpliendo con los requisitos del art. 4.11 del RGPD y el resto de las condiciones del art. 7 del RGPD. Sin embargo, y respecto de este requisito de la posible «equivalencia de los tratamientos» hay que tener en cuenta que, si existen alternativas disponibles al tratamiento de datos biométricos que impliquen menor riesgo para los derechos y libertades de las personas cuyos datos personales se van a tratar, que permitan que en un momento dado todos los trabajadores opten por otras alternativas, el procesamiento de datos biométricos deja de ser necesario para la implementación del tratamiento. Al no ser necesario el tratamiento de datos biométricos, no se estaría cumpliendo con lo establecido en el art. 5.1.c del RGPD. Por lo tanto, en un tratamiento de registro de jornada implementado con técnicas biométricas el consentimiento del interesado no levanta la prohibición del tratamiento, con carácter general, al existir una situación en la que existe un desequilibrio con el responsable del tratamiento, como ocurre en el ámbito de una relación laboral (o administrativa/funcionarial), y no superaría la evaluación de necesidad, requisito para tratamientos de alto riesgo. Un tratamiento de alto riesgo requerirá del responsable la superación, previa al inicio de tratamiento, de la evaluación de impacto relativa a la protección de datos establecida en el art. 35 del RGPD.

Para concluir, la Agencia recuerda que es indispensable que, con carácter previo a cualquier decisión de implantación de un sistema de control de presencia a través de sistemas biométricos, debe realizarse una Evaluación de Impacto para la Protección de Datos que incluya y también supere el principio de proporcionalidad superando los subprincipios de idoneidad[48], necesidad[49] y proporcionalidad en sentido estricto[50].

IV. ¡ADVERTENCIA!

La *Guía sobre tratamientos de control de presencia mediante sistemas biométricos* supone un nuevo criterio de la AEPD, tendrá un impacto significativo en las empresas que hayan optado por implementar sistemas biométricos para supervisar la presencia de sus trabajadores ya que justificar tales datos siendo de alto riesgo es una tarea harto difícil, sino imposible, por lo que, sin duda, se recomienda un cambio en el sistema de control de la jornada cambiando el biométrico por otro menos intrusivo.

48 De acuerdo con el concepto juicio de idoneidad, toda intervención en los derechos fundamentales debe ser adecuada para contribuir a la obtención de un fin constitucionalmente legítimo. Y aplicándolo al control empresarial, si la medida del empleador es susceptible de conseguir el objetivo propuesto, supera la idoneidad. De modo que se convierte, de inicio, en legítimo cualquier interés empresarial que pueda ser satisfecho por la medida de control; lo único que se precisa es adecuación.

49 El juicio de necesidad implica la comparación entre la medida adoptada por la empresa, y otros medios alternativos que se pudieran haber escogido. En esta comparación se examina si alguno de los medios opcionales logra cumplir dos exigencias: en primer lugar, si reviste el grado de idoneidad para contribuir a alcanzar el objetivo inmediato de esta última; y, en segundo término, si afecta al derecho fundamental en un grado menor. Es decir, que no exista otra medida más moderada para la consecución del propósito.

50 El principio de proporcionalidad en sentido estricto es el procedimiento de aplicación jurídica mediante el cual se establecen las relaciones de prelación entre principios en colisión. Si la medida es ponderada o equilibrada, porque derivan de ella más beneficios o ventajas para el interés general que perjuicios o valores en conflicto.