EDITORIAL

El "big bang" de la biometría laboral. De la huella dactilar a los neurodatos

The "big bang" of work biometry. From fingerprint to neurodata

Jesús R. Mercader Uguina
Catedrático de Derecho del Trabajo y la Seguridad Social
Universidad Carlos III
ORCID ID: 0000-0001-6301-6788

doi: 10.20318/labos.2024.8749

"*Wittgenstein menciona que nuestra primera y fundamental certeza es la certeza de nuestro cuerpo, de hecho, su proposición inicial es*[1]*: «si sabes que aquí hay una mano, te concedemos todo los demás»*".

Oliver Sacks, *Musicofilia*

I. El control de la intimidad de la intimidad: La dimensión laboral de la biometría

Debo comenzar reconociendo que la biometría me fascina[2]. Cuando el dominio de lo artificial y de todo lo ajeno al hombre se está convirtiendo en el signo más visible de nuestra era, surge, como irrefrenable paradoja, la centralidad de lo humano que pasa de ser la "medida de todas las cosas" a instrumento de medida de sí mismo. La tecnología sigue teniendo a la persona como centro esencial de su desarrollo y su evolución le conserva como punto de referencia. Y es que, desde los materialistas más radicales, se viene

[1] L. WITTGENSTEIN, *Sobre la certeza*, Barcelona, Gedisa, 2000, §1.

[2] En el presente trabajo retomo y continúo las reflexiones de otros previos que he realizado en esta materia. En concreto, "*Datos biométricos en los centros de trabajo*", Trabajo y Derecho, 2020, monográfico nº 11 (versión electrónica). "*Datos biométricos en los centros de trabajo*", en J. BAZ RODRÍGUEZ (Dir.*), Los nuevos derechos digitales laborales de las personas trabajadoras en España*, Madrid, Wolters Kluwer, 2021, pp. 169 a 198. También en el Prólogo a la obra de A. B. MUÑOZ RUIZ, *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*, Valencia, Tirant lo Blanch, 2023, pp. 13-18 y, más recientemente, *Los neuroderechos laborales: la neurotecnología llega al lugar de trabajo*, Trabajo y Derecho, 2024, nº 117 (septiembre 2024), en colaboración con M. I. RAMOS QUINTANA. Igualmente, me ocupé de este tema en *Algoritmos e inteligencia artificial en el derecho digital del trabajo,* Valencia, Tirant lo Blanch, 2022.

entendiendo que el cuerpo es una máquina[3] en la que todos y cada uno de los factores anatómicos y actuaciones ligadas a su funcionamiento tienen señas diferenciales, propias y específicas, que hacen a cada individuo distinto de todos los demás de su especie.

La identidad biológica es, pues, propia de cada sujeto y, por tanto, cualquier instrumento que la utilice permitirá, a quien de él se sirva, internarse en el terreno más recóndito que cada ser humano tiene. Podría decirse que, a su través, se puede entrar en la intimidad de la intimidad. Mientras que los datos biométricos de una persona pueden suprimirse o alterarse, la fuente de la que se han extraído en general no puede ser modificada ni suprimida. Los sistemas biométricos quedan, de este modo, referidos a características de los individuos que son: universales (todos los individuos las tienen), unívocas (distinguen a cada individuo), permanentes (en el tiempo y en distintas condiciones ambientales) y mensurables (son medibles de forma cuantitativa). Ello permite construir una métrica de cada persona.

Ciertamente, el registro de la jornada laboral a través de sistemas de control de entradas y salidas con control biométrico de la huella digital no es, desde luego, ninguna novedad. Forma también parte de nuestro pasado, los sistemas utilizados durante la pandemia de la COVID-19 para el control de la enfermedad (control de temperatura, pasaportes de inmunidad o controles serológicos). Pero si comienzan a tener carácter disruptivo los sistemas de biometría vocal, tecnología de gran potencial para el teletrabajo, que poseen un alto grado de seguridad (la voz es una característica única en cada persona, por lo que no se puede hackear ni suplantar, ni siquiera con grabaciones o por imitadores). También poseen este carácter, las formas control de identificación mediante la verificación de patrones oculares, a través de patrones del iris o de la retina, considerados los más efectivos ya que en 200 millones de personas la probabilidad de coincidencia es casi 0. Pero estos sistemas no acaban aquí. Hace unos meses aparecía en la prensa el caso de una sociedad belga de marketing digital que había implantado a varios de sus empleados un "chip" bajo la piel que funcionaba como una "llave" de identificación para abrir puertas o acceder al ordenador. La geolocalización integral está en camino. Por no hablar de los sistemas de reconocimiento facial que permiten en un instante detectar una malla de información a través del rostro de una persona (decenas de miles puntos de la imagen que coinciden con decenas de miles de puntos cifrados y almacenados previamente en la base de datos del sistema) y cuyo uso, como seguidamente veremos, está planteando importantes problemas en el terreno laboral.

Las técnicas de medida de base humana vienen a "filtrar" el cuerpo[4]. Pero es que, además, "el desarrollo tecnológico está permitiendo extraer cada vez más detalles de los

[3] J. O. DE LA METTRIE, *El hombre máquina, el hombre planta y otros escritos*, Buenos Aires, El cuenco de plata, 2014, p. 43. Para situar debidamente el pensamiento de este autor de la Ilustración francesa (1709-1751), es recomendable la lectura de M. ONFRAY, *Los ultras de las luces. Contrahistoria de la filosofía*, IV, Madrid, Anagrama, 2010, pp. 99-134.

[4] M. FOESSEL, A. GARAPON, *Biométrie : les nouvelles formes de l'identité*. Esprit, 2006, nº 8, 165-172, cuando señalan que: "La biométrie désigne une technologie d'identification et d'authentification qui (...) comme toute science classificatrice, n'a affaire qu'à des «objets filtrés».

rasgos biométricos de una persona. Por ejemplo, un análisis biométrico de la voz humana puede recoger más de cien parámetros distintos que permiten extraer información de salud, problemas físicos o sicológicos, entre otros. En sistemas biométricos basados en el reconocimiento facial se pueden tratar datos que revelan el origen racial o étnico, y también se puede extraer información de salud, problemas físicos o sicológicos como en el caso de la voz, incluso algunos sistemas de identificación mediante huella dactilar permiten el registro de parámetros como la temperatura o la presión sanguínea"[5].

A ello se añade la creciente expansión de las neurotecnologías y su aterrizaje en el mundo del trabajo. Recientemente se ha advertido sobre el uso de pulseras en conductores del transporte público de Pekín con el fin registrar sus estados emocionales durante su jornada. A ello se unen fórmulas de contenido diverso como los cascos de seguridad o gorras que forman parte del uniforme que permiten monitorerar en forma permanente las ondas cerebrales del trabajador o los auriculares multipropósito que, de forma inédita, facilitan la obtención masiva de datos de las personas trabajadoras a partir de la observación de su actividad cerebral, entre las que cabe incluir, como se ha puesto de manifiesto recientemente, las características neuronales que posibilitan la identificación, seguimiento o perfilado de dichas personas. El resultado de todo ello es el fin del dominio sobre nuestra propia identidad y un auténtico "Big Bang" de la biometría en lo laboral.

II. Biometría y derechos fundamentales

Cuestión a valorar es, sin duda, el impacto en el ejercicio de derechos fundamentales de los sistemas de control biométrico. Una cuestión a la que ya nos hemos enfrentado, pero cuyas respuestas han venido marcadas por un estado tecnológico de desarrollo menos evolucionado que el actual.

Y es que el uso de los sistemas biométricos plantea dudas sobre el alcance de su afectación a la "integridad personal" (art. 15 CE) y, a sus territorios de frontera, como el derecho a la salud (art. 43 CE). La incertidumbre que lleva consigo el desarrollo de los sistemas biométricos complejos recomienda prudencia. Razonamientos, como los utilizados en su día por el Tribunal Supremo en la STS (Contencioso-Administrativo) 2 de julio de 2007 (Rº 5017/ 2003) en relación con los primeros desarrollos biométricos, pueden resultar hoy manifiestamente insuficientes. Decir que estas técnicas no pueden considerarse lesivas para el derecho a la integridad física y moral ya que el empleado, "ni sufre una injerencia no consentida, ni genera un resultado perjudicial físico o moral para el empleado", pueden resultar conclusiones apresuradas. Como también lo puede ser concluir que tampoco queda afectado el derecho a la protección a la salud, cuando no se prueba fehacientemente su nocividad. El principio de precaución debe hacernos presente que, por ejemplo, al extraer ADN de un individuo, lo que compromete su in-

[5] AEDP, "*Guía sobre tratamientos de control de presencia mediante sistemas biométricos",* Madrid, AEDP, 2023, p. 14.

tegridad no es el acto mismo del contacto con el cuerpo (difícilmente una intromisión por cuanto basta con un cabello tomado de la ropa), sino el acervo de información que cabe extraer del cuerpo, su análisis y, por extensión, los procesos que cabe llevar a cabo con esa información.

De igual modo, su impacto en el derecho a la intimidad (art. 18.1 CE) resulta enorme y ello va a imponer una reflexión en profundidad sobre el contenido esencial de este derecho fundamental, un derecho cada vez más difuminado por el de protección de datos[6]. Y es que, como en el caso anterior, pecan de obsoletos razonamientos utilizados, en este caso, por el Tribunal Constitucional en su ATC 57/2007, de 26 de febrero, cuando en relación con el uso de estos sistemas biométricos se argumentaba, para considerar no violentado el referido derecho fundamental, desde una concepción de la intimidad entendida como ritual social. Afirmar, así, que "el ámbito de la intimidad corporal constitucionalmente protegido no es una entidad física, sino cultural, y en consecuencia determinada por el criterio dominante en nuestra cultura sobre el recato corporal", dado que el ámbito de intimidad corporal constitucionalmente protegido se fundamenta en "el sentimiento de pudor personal, en tanto responda a estimaciones y criterios arraigados en la cultura de la propia comunidad"[7] y, sobre lo anterior, concluir que "carece de todo sustento constitucional afirmar que el derecho a la intimidad corporal se ve vulnerado por la utilización de la mano como instrumento identificativo", son razonamientos que pecan, a la luz de las transformaciones a las que nos enfrentamos, de simplistas.

La intervención física para obtener la información es, probablemente, lo menos relevante. Todos estos sistemas de procesamiento de datos biométricos se basan en recoger y procesar datos personales relativos a las características físicas, fisiológicas o conductuales de las personas físicas pero los mismos se unen a otros sistemas tecnológicos que amplifican el uso de esa información. No sorprende que uno de los focos esenciales del Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteli-

[6] Como han señalado D. CORDOVA y L. M. DÍEZ PICAZO en un luminoso trabajo: *Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico*, Asociación de Letrados del Tribunal Constitucional, La privacidad en un nuevo entorno tecnológico, Madrid, CEPC, 2016), "la protección de datos, si bien nació tímidamente, se ha convertido en un agujero negro que lo absorbe todo y no deja escapar nada de su entorno". Una idea que viene de lejos, I. GARCÍA-PERROTE ESCARTÍN y J.R. MERCADER UGUINA, *La protección de datos se come a la intimidad: La doctrina de la Sentencia del Tribunal Europeo de Derechos Humanos de 5 de septiembre de 2017*, Revista de Información Laboral, 2017, nº 10, pp. 7-12.

[7] Y a lo anterior añadió que: "Es obvio que el derecho a la intimidad corporal no protege frente a una actuación como la presentación de la mano a una máquina o escáner, pues no puede decirse que entre en colisión con el criterio de recato arraigado socialmente acerca de la parte del cuerpo humano afectada, cuyo empleo a fines de identificación tiene, por lo demás, una ya larga tradición en nuestro país, en el que la impresión dactilar está incorporada al documento nacional de identidad desde hace tiempo (…) o se utiliza como medio supletorio de asegurar la identidad de los otorgantes de los documentos notariales (…)".

gencia Artificial) ("**RIA**") se haya puesto, precisamente, en el control de los usos biométricos de la Inteligencia Artificial. Un repaso a los conceptos empleados por estar norma ponen de manifiesto su significado: "datos biométricos" (art.3.34), "identificación biométrica" (art. 3.35), "verificación biométrica" (art. 3.36), "sistema de reconocimiento de emociones" (art. 3.39), "sistema de categorización biométrica" (art. 3.40), "sistema de identificación biométrica remota" (art. 3.41), "sistema de identificación biométrica remota en tiempo real" (art. 3.42), o "sistema de identificación biométrica remota en diferido" (art. 3.43). Un conjunto de usos que deja a las claras la centralidad de estas técnicas y su potencial, en algunos casos inaceptable, del riesgo asociado a su conexión con los sistemas de IA.

Ese carácter invasivo pone en peligro la dignidad humana, máxime si tenemos en cuenta que el uso de los sistemas biométricos se está convirtiendo, por momentos, en una potente herramienta de control empresarial. La inescindible conexión del RIA con el Reglamento (UE) 2016/679, 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 ("**RGPD**"), resulta evidente y ello se pone de manifiesto en las múltiples y recíprocas interacciones que se producen entre ambas normativas, cobrando, por ello, especial protagonismo el derecho a la protección de datos personales como instrumento de tutela frente a los usos desviados de estos sistemas.

III. El cuerpo como dato personal y su tutela

Aunque "el derecho a la protección de datos no es un Derecho general sobre libertades ni de protección de la autonomía personal"[8], se ha convertido en la primera barrera que ha construido lo jurídico para enfrentarse a los importantes riesgos que lleva consigo el uso de estas técnicas de medición de los patrones humanos. A la espera de una regulación propia, como la existente en otros países, debemos acudir en el nuestro a la referencia constitucional contenida en el art. 18.4 CE y al marco general que ofrece la normativa vigente en materia de protección de datos[9]. Dicha regulación se encuentra integrada, de un lado, por citado **RGPD** y por la Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales ("**LOPD**"). Disposición esta última, que viene a adaptar el ordenamiento jurídico español al RGPD al asumir la posibilidad que el mismo otorga a los Estados miembros de aclarar y especificar algunos aspectos.

[8] W. HOFFMANN-RIEM, W., *Big Data. Desafíos también para el Derecho*, Pamplona, Civitas, 2018, p. 139.

[9] Sobre la situación anterior a la entrada en vigor del RGPD, J.L. GOÑI SEIN, *Controles empresariales: geolocalización, correo electrónico, Internet, videovigilancia y controles biométricos*, Justicia Laboral, 2009, nº. 39, pp. 11-58. También, I. GARCIA-PERROTE y J.R. MERCADER, *El control biométrico de los trabajadores***,** *Revista de Información Laboral*, 2017, nº 3, pp. 7 a 12. Un primer acercamiento a esta materia tras el RGPD, J.L. GOÑI SEIN. *La nueva regulación europea y española de protección de datos y su aplicación al ámbito de la empresa*, Albacete, Bomarzo, 2018, pp. 43-47. También, M. RODRÍGUEZ-PIÑERO ROYO, *Las facultades de control de datos biométricos del trabajador*, Temas Laborales, 2019, nº 150, pp. 91-109.

El RGPD define como "datos biométricos" 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" (art. 4.14 RGPD)[10]. Un concepto que asume por remisión el RIA (art. 3.34). Y que, como recuerda el Considerando (14) del RIA, permite "la autenticación, la identificación o la categorización de las personas físicas y el reconocimiento de las emociones de las personas físicas", conceptos también precisados por la referida norma[11].

El desarrollo de estos sistemas facilita, como expresamente recoge el WP80 del GT29, Documento de trabajo sobre biometría, adoptado el 1 de agosto de 2003 (en adelante, "**WP 80 del GT 29**"), el registro o codificación de dos categorías principales de técnicas biométricas, las basadas en aspectos físicos que miden las características fisiológicas de una persona (comprobación de las huellas digitales, análisis de la imagen del dedo, reconocimiento del iris, análisis de la retina, reconocimiento facial, resultados de muestras de las manos, reconocimiento de la forma de la oreja, detección del olor corporal, el reconocimiento de venas de la palma y el reconocimiento de venas del dedo reconocimiento de la voz, análisis de muestras del ADN y análisis de los poros de la piel, etc…) y las que se fundamentan en aspectos comportamentales y miden el proceder de una persona (la comprobación de la firma manuscrita, el análisis de la pulsación sobre las teclas, el análisis de la forma de caminar, la forma de moverse, pautas que indiquen pensamiento subconsciente como mentir, etc.). También, el WP 193, Dictamen 3/2012 del GT29, sobre evolución de las tecnologías biométricas, adoptado el 27 de abril de 2012 (en adelante, "**WP 193 del GT 29**"), añade "las técnicas basadas en elementos

[10] De acuerdo con la anterior definición, tres son los "componentes" principales que pueden distinguirse en la citada noción, los datos biométricos: (i) Son "*datos personales*". El RGPD entiende por tales: "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 (…) uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, (…)" (art.4.1 RGPD). (ii) Deben ser objeto de "*tratamiento técnico específico*". Según el WP80 del GT29, el tratamiento de estos datos se realiza a través de sistemas biométricos que son: "aplicaciones de las tecnologías biométricas que permiten la identificación automática, y/o la autenticación/comprobación de una persona. Se suelen utilizar aplicaciones de autenticación/comprobación para diversas tareas en campos muy distintos y bajo la responsabilidad de una amplia gama de entidades diferentes". (iii) Y, finalmente, son "*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*".

[11] El RIA define la «identificación biométrica» (art. 3.35) como "el reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico para determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de personas almacenados en una base de datos" y la «verificación biométrica» (art. 3.36), como "la verificación automatizada y uno-a-uno, incluida la autenticación, de la identidad de las personas físicas mediante la comparación de sus datos biométricos con los datos biométricos facilitados previamente". Y, en fin, la «categorización biométrica» (art. 3.40) como "un sistema de IA destinado a incluir a las personas físicas en categorías específicas en función de sus datos biométricos, a menos que sea accesorio a otro servicio comercial y estrictamente necesario por razones técnicas objetivas". Sobre el concepto, "reconocimiento de emociones" (art. 3.39), volveremos más adelante.

psicológicos, que incluyen la medición de la respuesta a situaciones concretas o pruebas específicas que se ajusten a un perfil psicológico".

El límite al uso de esta categoría especial de datos se encuentra en el art. 9.1 RGPD que establece que: "*Quedan prohibidos el tratamiento de* (…) *datos biométricos dirigidos a identificar de manera unívoca a una persona física* (…)". Categóricamente, el RGPD sienta un principio general en relación con las categorías especiales de datos: la prohibición de su tratamiento. Ahora bien, el art. 9.2 RGPD establece un amplio listado de excepciones a tan contundente regla.

Se excepciona, en primer lugar, a la prohibición de tratamiento, "*aquellos en los que 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 art.9.1 RGPD no puede ser levantada por el interesado*" (art. 9.2.a) RGPD). Aunque la LOPD no impide, en este caso, que el consentimiento pueda ser una forma de levantar la prohibición de tratamiento en el ámbito laboral sus posibilidades de su uso son, ciertamente, limitadas[12]. La AEPD en su Resolución R/0041/2019, ha llegado a afirmar que "los trabajadores no están nunca en condiciones de dar, denegar o revocar el consentimiento libremente, habida cuenta de la dependencia que resulta de la relación". Precisamente, por ello, es más que justificado que algunos autores hayan entendido que en una materia tan sensible como ésta no tenga espacio de juego el consentimiento[13]. No obstante, como han precisado el apartado 22 de las Directrices 5/2020 del CEPD, sobre el consentimiento en el sentido del RGPD ("**Directrices 5/2020 del CEPD**"), aunque su uso venga a resultar excepcional en el campo laboral, ello "*no significa que los empleadores no puedan basarse nunca en el consentimiento como base jurídica para el tratamiento de datos. Puede haber situaciones en las que el empleador pueda demostrar que el consentimiento se ha dado libremente. Dado el desequilibrio de poder entre un empleador y los miembros de su personal, los trabajadores únicamente pueden dar su libre consentimiento en circunstancias excepcionales, cuando el hecho de que otorguen o no dicho consentimiento no tenga consecuencias adversas"*.

El art. 9.2 RGPD, como expresamente recuerda el WP 259 del Comité Europeo de Protección de datos, Directrices sobre el consentimiento en el sentido del Reglamento 2016/679, "*no reconoce la circunstancia de (ser) «necesario para la ejecución de un contrato» como una excepción a la prohibición general de tratar categorías especiales de datos*". Por lo tanto, los responsables que deban tratar categorías especiales de datos deberán acudir a las excepciones específicas que figuran en el art. 9. 2, letras b) a j) RGPD. Por ello, en el campo laboral posee especial importancia, como tendremos oportunidad de señalar a lo largo este trabajo, la regla del art. 9.2 b) RGPD: "*aquellos casos en que éste es necesario*

[12] En general, sobre los límites del consentimiento en materia laboral, J.R. MERCADER UGUINA, *Protección de datos y garantía de los derechos digitales en las relaciones laborales*, Madrid, Francis Lefebvre, 2019, 3ª ed., pp. 40-42.

[13] J. BAZ RODRIGUEZ, en su excelente y riguroso estudio, *Privacidad y protección de datos de los trabajadores en el entorno digital*, Madrid, Bosch, 2019, p. 247, entiende que "debe excluirse la alusión al consentimiento explícito del trabajador" en los controles biométricos.

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".

La existencia de una lícita condición para el tratamiento no excluye el cumplimiento de una serie de garantías adicionales, entre las que ocupa un lugar preferente el deber de informar. Los responsables deben informar a los interesados y a otros responsables (art.11.2, 12 y 13 RGPD). El principio de transparencia posee una importancia extraordinaria que queda subrayada en materia laboral por el propio RGPD cuando señala que dentro de "*las disposiciones legislativas o de convenios colectivos, que establezcan normas más específicas para garantizar la protección de los derechos y libertades en relación con el tratamiento de datos personales de los trabajadores en el ámbito laboral*", se incluirán medidas adecuadas y específicas «*prestando especial atención a la transparencia del tratamiento*» (art.88.2 RGPD).

Igualmente, la implantación de sistemas biométricos debe cumplir con las exigencias derivadas de la protección de datos en el diseño (art. 25.1 RGPD) y, en especial, del principio de minimización, que obligan a escoger aquella tecnología que resulte menos intrusiva desde el punto de vista de la protección de datos. Ello conlleva que, si se puede alcanzar una determinada finalidad sin tener que tratar datos de categorías especiales, esta opción debe prevalecer ante otras opciones que sí que impliquen el tratamiento de estos tipos de datos.

El art. 35.1 RGPD establece, con carácter general, la obligación que tienen los responsables de los tratamientos de datos de realizar una Evaluación de Impacto en la Protección de los Datos Personales ("**EIPD**") con carácter previo a la puesta en funcionamiento de tales tratamientos cuando sea probable que éstos por su naturaleza, alcance, contexto o fines entrañen un alto riesgo para los derechos y libertades de las personas físicas, alto riesgo que, según el propio Reglamento, se verá incrementado cuando los tratamientos se realicen utilizando "nuevas tecnologías". La Agencia Española de Protección de Datos (en adelante, "**AEPD**") ha publicado una lista de actividades de tratamiento que requieren la realización de una EIPD[14].En el ámbito laboral la referida evaluación resultará imprescindible en la medida en que, por un lado, que se trate de "tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva" y, por otro, que los tratamientos "impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física".

Como ha recordado el WP 193 del GT 29, en lo que respecta a los datos biométricos, "*la seguridad debería ser una preocupación fundamental, ya que los datos biométricos son irrevocables. Por consiguiente, una violación por lo que respecta a los datos biométricos constituye una amenaza para el uso seguro de la biometría como identificador y para el derecho a la protección de datos de los interesados, para los que no existe ninguna posibilidad*

[14] https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

de mitigar los efectos de la violación". Sobre esta base se aconseja que se adopten *"medidas adecuadas para proteger los datos almacenados y tratados por el sistema biométrico: la información biométrica deberá almacenarse siempre de forma cifrada. Deberá definirse un marco de gestión de las claves para garantizar que las claves de descifrado solo sean accesibles por razón de la necesidad de conoce*r".

Finalmente, los datos de carácter personal, tal y como se extrae del art. 5 e) RGPD, tienen que ser "*mantenidos durante no más tiempo de aquel necesario a los efectos de la identificación de los interesados, en función de las finalidades previstas para su tratamiento*". En relación con la limitación del almacenamiento el WP 193 del GT 29 recomienda que "*el responsable del tratamiento deberá determinar un periodo de conservación de los datos biométricos que no podrá ser superior al necesario para los fines para los que dichos datos fueron recabados o para los que se traten ulteriormente. El responsable del tratamiento deberá garantizar que los datos, o los perfiles derivados de esos datos, se supriman una vez transcurrido este periodo de tiempo justificado*".

La Guía de la AEPD para la "*Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción"*[15]), que tiene como objetivo ser una "primera aproximación" para el ajuste al RGPD de productos y servicios que incluyan componentes de Inteligencia Artificial, pone especial acento en el respeto al principio de exactitud en el tratamiento de los datos biométricos. Señala, a tal efecto que: "La exactitud es particularmente crítica cuando el tratamiento está basado en información biométrica, como Inteligencia Artificial sobre reconocimiento facial, huellas dactilares, voz, etc. En ese caso, se han de tener en cuenta factores de rendimiento (falsos positivos, falsos negativos y otros) y también el impacto sobre la recogida de los datos de personas con alguna discapacidad o singularidad física". El responsable ha de tener en cuenta que, aunque dichos usuarios pueden ser una minoría, "se han de establecer mecanismos alternativos para evitar la exclusión de un sujeto porque la solución de IA no es capaz de procesar las características biométricas de los interesados", en definitiva, evitar una discriminación por no ser "biométricamente adecuado"[16].

Las respuestas normativas especializadas en lo laboral han sido, hasta el momento, escasas y todas ellas vienen de la mano de la aplicación de la normativa de protección de datos personales. El famoso Titulo X de la LOPD desaprovechó una magnífica oportunidad para haber sentado los primeros cimientos en esta materia de modo que, como doctrinalmente se ha señalado, hubiera sido conveniente que esta norma "hubiese dedicado un cierto esfuerzo a visibilizar esta problemática, aportando al menos una regulación minimalista para este escenario como la que contempla para otros tratamientos de datos de los trabajadores"[17].

[15] https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

[16] En concreta referencia a los "fines abiertamente decisionales" con que pueden ser usados los datos biométricos, J. BAZ RODRIGUEZ, *Privacidad y protección de datos de los trabajadores en el entorno digital*, cit., p. 244.

[17] J. BAZ RODRIGUEZ, *Privacidad y protección de datos de los trabajadores en el entorno digital*, cit. p. 239.

En su ausencia, resulta especialmente interesante, la respuesta dada por el modelo francés en la Délibération nº 2019-001 de 10 de enero de 2019, de la Commission Nationale de l'Informatique et des Libertés, que aprueba el Règlement type relatif à la mise en oeuvre de dispositifs ayant pour finalité le contrôle d'accès par authentification biométrique aux locaux, aux appareils et aux applications informatiques sur les lieux de travail. Esta norma concreta el mandato contenido en la loi no 2018-493 de 20 de junio de 2018 relative à la protection des données personnelles, que atribuye la función de establecer y publicar "regulaciones tipo para garantizar la seguridad de los sistemas de tratamiento de datos personales y para regular el tratamiento de datos biométricos, genéticos y de salud"[18].

Dentro de las fórmulas de soft law, en nuestro país, contamos desde noviembre de 2023, con la "*Guía sobre tratamientos de control de presencia mediante sistemas biométricos"* elaborada por la AEPD ("**Guía sobre sistemas biométricos de la AEPD**"), que teniendo en cuenta las Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley del Comité Europeo de Protección de Datos ("**Directrices 5/2022 del CEPD**"), y ha venido a establecer reglas específicas en relación con el uso de estos sistemas en relación con los controles de presencia laborales y extralaborales. A ella nos referiremos seguidamente.

IV. Huellas dactilares y registro de jornada

Las normas sobre registro de jornada [art. 34.9 del 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 ("**ET**")] llevaron al primer plano el tratamiento de las huellas dactilares. Es importante recordar que, si bien la huella dactilar completa identifica completamente a la persona, también es susceptible de identificarse a la misma persona con la toma de muestras o minucias recogidas de partes de la huella y transformadas en una plantilla, aunque sea a través de un algoritmo. Esas minucias, convertidas en algoritmos, mediante su registro en una base de datos, o incluso en una tarjeta o plantilla que porte el usuario permitirían, al ser tratados, la identificación de la persona cuando acceda a la instalación, a través del proceso de matchmaking (emparejamiento por comparación), entran también en el ámbito del dato de carácter personal.

La AEPD se había venido pronunciando, incluso antes de la reforma que en 2019 alumbró la normativa sobre registro de jornada, sobre si el tratamiento de la huella dactilar directamente obtenida, como dato biométrico que es, podía considerarse excesivo para el fin que motiva dicho tratamiento. Así originariamente, concluyó (entre otros, AEPD Informe 000/1999; 0324/2009) que "el tratamiento de la huella digital para el control de acceso por los trabajadores podría considerarse una medida de control ampa-

[18] He analizado extensamente esta disposición en "*Datos biométricos en los centros de trabajo*", Trabajo y Derecho, 2020, monográfico nº 11 (versión electrónica) y. "*Datos biométricos en los centros de trabajo*", en J. Baz Rodríguez (Dir.), Los nuevos derechos digitales laborales de las personas trabajadoras en España, Madrid, Wolters Kluwer, 2021, pp. 169 a 198.

rada en el art. 20.3 ET, por lo que no se exigiría el consentimiento del empleado". No obstante, para implantar esta medida debería aplicarse el principio de minimización, es decir, debería limitarse a supuestos en que se considere realmente necesaria para que el control sea eficaz". Además, la AEPD había señalado en diversos informes que podrían existir buenas prácticas que permitieran el control a través de la huella digital sin que el sistema tuviera que almacenar el dato biométrico (por ejemplo, por su incorporación a una tarjeta inteligente que se contrastase con la huella y se mantuviera siempre en poder del trabajador) (Informe 0324/2009).

Sobre esta cuestión también resolvieron las Agencias autonómicas de protección de datos que se mostraron más reticentes a su admisión. Ejemplo de ello fue la Agencia Vasca de Protección de Datos que enfrentó a esta cuestión en su Dictamen 11-024 (Exp. CN11-006) (en el que consideró excesivo su uso dada las circunstancias en las que se realizaba) y en el Dictamen 17-005 (Exp. CN17-004), en el que concluía la necesidad de valorar en cada caso concreto la oportunidad de la instalación de un sistema de acceso que incorporase el control a través de la huella dactilar.

Idénticas cautelas mantuvo la Agencia Catalana de Protección de Datos (en adelante, "**APDCAT**") en su Dictamen CNS 63/2018 de 14 de febrero de 2019[19]. En él dio respuesta a este problema, pero, en este caso, partiendo de la premisa de que "algunas autoridades de control en materia de protección de datos no han admitido la utilización de sistemas de control basados en datos biométricos como sistema generalizado de control horario de los trabajadores por parte del empresario. Sería el caso de la CNIL de Francia o *Garante per la protezione dei dati personali* de Italia". La APDCAT se mostró cauta a la hora de admitir su uso como instrumento para materializar el registro de jornada y concluyó en el citado Informe, que "la inclusión de los datos biométricos, entre ellos los de la huella dactilar, entre las categorías especiales de datos previstas por el RGPD no permite concluir de manera automática que la implantación de un sistema de control horario basado en la recogida de este tipo de datos pueda considerarse proporcionada y, por lo tanto, conforme con el principio de minimización".

Los criterios de modulación se han venido reiterando en los últimos tiempos y la AEPD ha ido reforzando las exigencias para la admisibilidad de estos sistemas. Esta línea se muestra, tanto la Resolución que puso fin al PS/00010/2021 de la AEPD (empresa tenía instalado un fichero en la puerta de acceso en la entrada de la nave industrial con lectura de huella digital y clave de operario), como en la del PS/00050/2021 de la AEPD (sistema de control presencial de los trabajadores a través de un sistema biométrico que se conjuga con el lector de tarjeta). En ambos supuestos se sancionó a la empresa, en un caso por la inidoneidad, desproporcionalidad, no pertinencia ni adecuación del sistema de toma de huellas para acceder a vestuarios/aseos (art. 5.1 c) RGPD) y, en el otro, por incumplir con la obligación de EIPD exigida por el art. 35 RGPD.

[19] Una reflexión de conjunto sobre el referido Dictamen puede verse en D. GRACIA GARCÍA, *El impacto de la privacidad en los sistemas biométricos de control de acceso y horario laboral tras el Dictamen 63/2018 de la Autoridad Catalana de Protección de Datos*, Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal, 2019, nº 8, pp. 56-65.

Con posterioridad, la AEPD publicó en mayo de 2021 la Guía "La Protección de Datos en las Relaciones Laborales" ("**Guía para la protección de datos en las relaciones laborales de la AEPD**"), 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. Sin embargo, esta interpretación fue superada por las Directrices 5/2022 del CEPD.

La "*Guía sobre sistemas biométricos de la AEPD*", ha venido a establecer que antes de implementar cualquier sistema de este tipo debe valorarse su necesidad para la consecución de la finalidad pretendida, en el sentido de que no haya otro medio igual de eficaz y menos intrusivo. Ejercicio que recae en el responsable del tratamiento, que tiene la obligación de justificar por qué "*ya 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, "debe 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 no son adecuados". En definitiva, cuestiona la necesidad de la implantación del tratamiento de datos biométricos, al existir otros medios alternativos que, en ocasiones complementándose con intervención humana, puedan razonablemente lograr la finalidad pretendida, es decir, "no existe una obligación a que se implementen exclusivamente con medios tecnológicos".

Igualmente, ha sentado que el 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, que no superaría la evaluación de necesidad, requisito para tratamientos de alto riesgo. La referida "Guía" subraya además que, en este caso, si el levantamiento de la prohibición se basa en el 9.2.b) RGPD, el responsable debe contar con una norma con rango de ley que concrete la posibilidad de utilizar datos biométricos para dicha finalidad". Y, en la actualidad, "la autorización suficientemente específica no se encuentra para el personal laboral, puesto que los arts. 20.3 y 34.9 ET, no contienen tal autorización". Y es que, aunque no se cita, la STJUE de 30 de marzo de 2023, C-34/2021, está seguramente en el fondo de esta interpretación[20].

Este nuevo criterio de la AEPD tiene importantes consecuencias si tenemos en cuenta que borra la posibilidad del consentimiento explícito y, en la actualidad, no existe una norma con rango de ley que concrete la posibilidad de utilizar datos biométricos. Así las cosas, la adecuación de las empresas a estas nuevas exigencias aparece como una necesidad real y actual derivada del principio básico de responsabilidad proactiva (art. 5.2 RGPD), de acuerdo con el cual "el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento (...), incluida la eficacia de las medidas" (Considerando 74 del RGPD). Hasta el punto

[20] Un comentario que realicé sobre la misma puede encontrarse, *¿Hay vida más allá del RGPD?: Límites a las previsiones legales o convencionales de tratamiento de datos personales en materia laboral (a propósito de la STJUE de 30 de marzo de 2023", asunto C34/21)*, El Foro de Labos, 11 de abril de 2023.

que, como se ha avisado, los responsables del tratamiento que habiendo implementado los referidos sistemas biométricos y perseveren en su uso sin cumplir con los mencionados criterios, tienen "el riesgo de enfrentarse a posibles reclamaciones iniciadas por parte de los trabajadores y, por consiguiente, potenciales sanciones por parte de la Agencia"[21].

V. Controles panópticos y técnicas de reconocimiento facial

El reconocimiento facial es una tecnología probabilística que puede reconocer automáticamente a las personas por su rostro para autenticarlas o identificarlas y está técnica se inserta en la categoría más amplia de la tecnología biométrica[22]. Como precisara el RGPD, "el tratamiento del rostro con software de reconocimiento facial se encuentra dentro de los datos biométricos" (Considerando 51 RGPD). La cara, al igual que las huellas dactilares, ha sido ampliamente utilizada como fuente de datos biométricos durante años. Como advierte el WP 193 del GT 29, "no solo la identidad puede determinarse a partir de una cara, sino también características fisiológicas y psicológicas tales como el origen étnico, emociones y bienestar. La capacidad para extraer este volumen de datos de una imagen y el hecho de que una fotografía puede tomarse a distancia sin conocimiento del interesado demuestra la cantidad de problemas de protección de datos que pueden derivarse de estas tecnologías".

La imagen es, indudablemente, un dato de carácter personal (art. 4.1 RGPD) y las fotografías poseen esa misma consideración por lo que su captación y difusión es un tratamiento de datos que exige cumplir con todas las exigencias de la normativa sobre protección de datos personales. Es importante, no obstante, como nos recuera el Considerando (57) RGPD que: "El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física". De este modo, una fotografía tendrá la consideración de dato biométrico, únicamente, si detrás de la captura de la fotografía se encuentra un sistema de reconocimiento facial que permita identificar de forma única a una determinada persona. Por ello, como recuerda el WP 193 del GT 29, las fotografías que no posean esa consideración "no podrán tratarse con el fin de extraer plantillas biométricas ni registrarse en un sistema biométrico a fin de reconocer a las personas de las imágenes automáticamente (reconocimiento facial) sin una base jurídica específica (por ejemplo, consentimiento) para esta nueva finalidad".

[21] A. ZORRAQUINO, A. MATAS BRANCÓS, S. MURILLO GEISER, *El nuevo criterio de la Agencia sobre el tratamiento de control de presencia mediante sistemas biométricos*, Newsletter de PwC Tax & Legal, 2023, diciembre.

[22] Ampliamente, L. COTINO HUESO, "*Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal*, El Cronista del Estado Social y Democrático de Derecho, 2022, nº 100, (Ejemplar dedicado a: Inteligencia artificial y derecho), pp. 68-79.

El WP 249, Dictamen 2/2017 sobre el tratamiento de datos en el trabajo, del GT 29 (en adelante, "**WP 249 del GT29**"), puso de manifiesto que son muchos los riesgos que plantea el uso de estos sistemas de reconocimiento unidos a los de video vigilancia como, por ejemplo, que el empleador pueda controlar las expresiones faciales de sus empleados o identificar desviaciones de patrones de movimientos predefinidos durante el desarrollo de su actividad laboral. Esto es lo que llevó a llamar la atención sobre la necesidad de que "los empleadores se abstengan de utilizar estas tecnologías pues, aunque podría haber algunas excepciones marginales, éstas no pueden ser utilizadas para invocar una legitimación general que dé cobertura, sin más, al uso de dicha tecnología". El referido WP 249 del GT29 puso de manifiesto que "aunque el uso de estas tecnologías puede ser útil para detectar o prevenir la pérdida de propiedad intelectual y material de la empresa, mejorando la productividad de los trabajadores y protegiendo los datos personales de los que se encarga el responsable del tratamiento, también plantea importantes retos en materia de privacidad y protección de datos. Por consiguiente, se requiere una nueva evaluación del equilibrio entre el interés legítimo del empresario de proteger su empresa y la expectativa razonable de privacidad de los interesados: los trabajadores".

Con posterioridad, el apartado 73 de las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo, señaló que: "*La utilización de datos biométricos y, en particular, el reconocimiento facial conlleva riesgos mayores para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando los principios de legalidad, necesidad, proporcionalidad y minimización de los datos establecidos en el RGPD. Considerando que el uso de estas tecnologías puede percibirse como especialmente eficaz, los responsables deberían, en primer lugar, evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos para lograr su objetivo legítimo de la transformación*".

Particular interés tiene, por todo ello, la Resolución dictada por la AEPD en el PS/00120/2021 en el caso del establecimiento de un sistema de reconocimiento facial en la empresa Mercadona[23]. El referido procedimiento se inició por la directora de la AEPD a la vista de las noticias publicadas en medios de comunicación acerca de la implantación por la cadena de supermercados concernida de un sistema de reconocimiento facial en alguno de sus centros a resultas de una sentencia penal que había condenado a dos personas como autores de un delito intentado de robo con violencia en las personas, siendo condenados cada uno de ellos a la penas de prisión, inhabilitación especial y la prohibición de acceso al centro comercial.

De las actuaciones previas de investigación, se concluyó que la mercantil realizaba un tratamiento de datos biométricos que no sólo alcanzaba a la identificación de condenados penales con imposición de medidas de seguridad, sino que afectaba a cualquier persona que entrase en uno de sus supermercados (incluidos menores) y a sus empleados. El tratamiento de datos incluía la captación, el cotejo, conservación y la destrucción –en

[23] De esta concreta cuestión y de sus concretos antecedentes me he ocupado en "*El reconocimiento facial como mecanismo de control empresarial a examen*", Nueva Revista Española de Derecho del Trabajo, 2021, nº 252, pp.13-22. En colaboración con I. García-Perrote.

caso de identificación negativa– (tras 0,3 segundos de su recogida) de la imagen biométrica captada de cualquier persona que entrase en el supermercado. En el tratamiento, dice la AEPD, se observa claramente un sistema de reconocimiento facial indiscriminado y masivo ya que "dependiendo de los datos biométricos recogidos, pueden derivarse datos del sujeto como su raza o género (incluso de las huellas dactilares), su estado emocional, enfermedades, taras y características genéticas, consumos de sustancias, etc.".

De lo expuesto por la AEPD concluye, en el caso, que los sistemas de reconocimiento facial no son meros sistemas de videovigilancia y, por tanto, exigen bases de legitimación del tratamiento que van más allá de las establecidas en el art. 6 RGPD y, por tanto, requieren un tratamiento radicalmente distinto al utilizar datos biométricos de forma masiva y remota del tipo "uno-a-varios" debiendo tratarse en el marco del régimen excepcional que proporciona el art. 9 RGPD. Exigencia que no se había cumplido. Las características de estos sistemas imponen un estricto y reforzado cumplimiento de la obligación de información de acuerdo con lo establecido en el art. 13 RGPD cuando estamos en presencia de un tratamiento más invasivo, con riesgos más específicos y mayores, que conlleva la utilización de datos biométricos. Requerimiento al que tampoco se había atendido. Y, en fin, hubiera resultado imprescindible contemplar los riesgos sobre los derechos de los trabajadores en la elaboración del EIPD ex art. 35 RGPD, exigencia que, en el caso, había quedado, también, desatendida. Ello dio lugar a una de las multas más elevadas de las hasta ahora impuestas por la AEPD

La posibilidad de que estos sistemas puedan alcanzar la habilitación requerida por el art. 9.2.b) RGPD, puede venir de la mano de instrumento típicamente laboral: el convenio colectivo. A esta posibilidad hizo mención expresa el Dictamen 2/2022, de 2 de febrero de la APDCAT. En dicho informe se daba respuesta a la consulta planteada por un Ayuntamiento sobre la posibilidad de instalar un sistema de control de presencia en el lugar de trabajo mediante reconocimiento facial. La APDCAT señaló que "a falta de previsión legal, cabe recordar que, de acuerdo con lo que prevé el art. 9.2.b) RGPD, la autorización puede estar prevista en el marco de un convenio colectivo. Por ello, en caso de que el convenio colectivo, el pacto o acuerdo resultante de la negociación, prevea la utilización de datos biométricos a tal fin y establezca garantías adecuadas respecto a los derechos fundamentales y de los intereses de las personas interesadas, este instrumento permitiría concluir la concurrencia de la excepción prevista en el art.9.2. b) RGPD". Como ya hemos justificado en otro lugar, a nuestro juicio, el alcance en nuestro país de la expresión que utiliza el RGPD, "*convenio colectivo (que) con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado*", remite a los convenios colectivos estatutarios, regulados en el Título III ET, que tienen atribuida la condición de norma jurídica, con su correspondiente inserción en el cuadro de fuentes del Derecho (art. 3.1 b) y art. 82.3 ET)[24].

[24] "*Aspectos laborales de la Ley Orgánica 3/2018, de 5 de diciembre: una aproximación desde la protección de datos",* Trabajo y Derecho*,* 2019, nº 52, p. 110 a 118.

VI. Datos biométricos y artificios adaptados al cuerpo

Los datos biométricos se encuentran vinculados con el uso de la tecnología wearable habitualmente referenciada como WT (Wearable Technology), y los dispositivos asociados como WD (Wearable Devices) o, simplemente, wearables: chaqueta tecnológica, relojes inteligentes, etc. Integrados en estos dispositivos se están desarrollando bioprocesadores para registrar datos biométricos del cuerpo humano (flujo sanguíneo, temperatura de la piel, nivel de grasa corporal, frecuencia cardíaca, etc.). Esta información incorporada a través de una pulsera o reloj inteligente permite ofrecer nuevas formas de autentificación. A título de ejemplo, los datos del electrocardiograma podrían llegar a convertirse en una "firma cardíaca", y, por extensión, en un instrumento de control a través del uso de los latidos de su corazón que son únicos en cada persona. Pero también nos encontramos con los exoesqueletos, una tecnología en constante y rápida evolución, lo que hace que cada día se diseñen y utilicen nuevos modelos con capacidades mejoradas y ampliadas[25].

Como señala el WP 249 del GT29, los riesgos de estos sistemas en el mundo laboral son evidentes dado que "los empleadores están cada vez más tentados de proporcionar dispositivos portátiles a sus empleados con el fin de rastrear y registrar su salud y actividad dentro y algunas veces incluso fuera del lugar de trabajo". Sin embargo, este tratamiento de datos implica el de datos de salud lo que hace necesario recordar su consideración como datos sensibles y, por extensión, las limitaciones que se imponen a su tratamiento[26]. En estos casos, "es altamente improbable que pueda darse un consentimiento explícito válido". Y ello, dice el GT29, porque, en primer lugar, "los trabajadores no son esencialmente «libres» para dar dicho consentimiento. Incluso si el empresario utiliza a un tercero para recopilar los datos de salud, que solo proporcionarían al empresario información agregada sobre la evolución general en este ámbito, el tratamiento seguiría siendo ilegal". Asimismo, por que como se recuerda el WP 216 del GT 29, Dictamen 5/2014, sobre técnicas de anonimización, es técnicamente muy difícil garantizar la misma de forma completa. Y, añade, "incluso en un entorno con más de mil empleados, habida cuenta de la disponibilidad de otros datos sobre los trabajadores, el empresario aún podría distinguir a los trabajadores individuales con indicadores de salud particulares, como hipertensión u obesidad".

En la misma línea, la "*Guía para la protección de datos en las relaciones laborales de la AEPD*" ha señalado que la monitorización de datos de salud a través de dispositivos inteligentes está, por lo general, prohibida, a menos que esté establecida por ley o reglamentariamente, dado que no se enmarca en la vigilancia de la salud; supone el tratamien-

[25] Dentro de las nuevas formas robóticas, el desarrollo tecnológico ha conseguido crear un nuevo tipo de dispositivos, los exoesqueletos, que empiezan a presentarse como una vía de intervención ergonómica y de mejora de las condiciones de trabajo, especialmente en lo que a la carga física se refiere. Las Notas Técnicas de Prevención del Instituto Nacional de Seguridad y Salud en el Trabajo 1162 (*Exoesqueletos I: Definición y clasificación*) y 1163 (*Exoesqueletos II: Criterios para la selección e integración en la empresa*), se ocupan desde la perspectiva preventiva del uso de exoesqueletos.

[26] Extensamente sobre esta cuestión, J. BAZ RODRIGUEZ, *Privacidad y protección de datos de los trabajadores en el entorno digital*, cit., p. 239-242.

to de datos de salud sin una base jurídica (una vez más, se reconoce la imposibilidad de solicitar el consentimiento del trabajador puesto que éste no sería libre para prestarlo); su finalidad es ilegítima y vulnera el principio de proporcionalidad.

VII. La métrica de las emociones

El cuerpo y la conciencia se encuentran implicados en vivencias y sentimientos compartidos, de modo que el sistema nervioso, el cerebro y el modo de comportarse y afrontar el mundo no pueden ser comprendidos como estructuras separadas. Antes, al contrario, como dijo Merlau-Ponty, deben ser entendidos como una estructura sistémica[27]. Entre las manifestaciones del cuerpo figuran la recepción pasiva ante los estímulos del medio y la respuesta activa ante ellos; la interacción global que cohesiona a la psique con el entorno gracias a impulsos como las emociones y los sentimientos. Las emociones, se ha dicho, no son algo que me ocurre, sino algo que yo hago. En suma, son "disposiciones mentales" que generan actitudes y éstas pueden ser objeto de control, valoración y seguimiento.

El RIA define en su art. 3.39 como «sistema de reconocimiento de emociones»: un sistema de IA destinado a distinguir o inferir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos. Mientras que su Considerando (18) clarifica el concepto, al señalar que el mismo se refiere a "emociones o intenciones como la felicidad, la tristeza, la indignación, la sorpresa, el asco, el apuro, el entusiasmo, la vergüenza, el desprecio, la satisfacción y la diversión. No incluye los estados físicos, como el dolor o el cansancio, como, por ejemplo, los sistemas utilizados para detectar el cansancio de los pilotos o conductores profesionales con el fin de evitar accidentes. Tampoco incluye la mera detección de expresiones, gestos o movimientos que resulten obvios, salvo que se utilicen para distinguir o deducir emociones. Esas expresiones pueden ser expresiones faciales básicas, como un ceño fruncido o una sonrisa; gestos como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, como una voz alzada o un susurro".

Un magnífico ejemplo de que estos usos son ya una realidad, es la resolución de la Agencia de Protección de Datos húngara de 8 de febrero de 2022, en la que revisaba la práctica llevada a cabo por un banco durante 45 días y que consistía en utilizar un software de procesamiento de señales de voz basado en IA[28]. El mencionado software analizaba y evaluaba los estados emocionales de los clientes y las palabras clave utilizadas en las llamadas. La finalidad de esta tecnología era gestionar las quejas, controlar la calidad de las llamadas y del trabajo y, además, aumentar la eficiencia de los empleados. A continuación, los resultados de este análisis se almacenaban junto con las grabaciones de las llamadas y estos datos se usaban para clasificar las llamadas en orden de prioridad. La justificación del banco para el procesamiento de datos se basó en su interés legítimo

[27] M. MERLAU PONTY, *La fenomenología de la percepción*, Madrid, Editorial Planeta, 1993.

[28] Un extenso análisis en A. B. MUÑOZ RUIZ, *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*, Valencia, Tirant lo Blanch, 2023, pp. 149-153.

de garantizar buenos niveles de retención de clientes y eficiencia. Sin embargo, el Agencia húngara concluyó que el banco no había considerado adecuadamente los intereses en juego y le sancionó con una multa de 670.000 € obligándole a suspender el uso del sistema de análisis de emociones descrito.

Los inaceptables riesgos que el control de las emociones lleva consigo ha tenido como consecuencia su expresa prohibición por el RIA. Así, tanto "*la introducción en el mercado, la puesta en servicio o la utilización de sistemas de IA para inferir las emociones de una persona física en los ámbitos de la aplicación de la ley (...) en lugares de trabajo* (...)" (art. 5.1 f) RIA), como "*la introducción en el mercado, la puesta en servicio para este fin específico o el uso de sistemas de categorización biométrica que clasifiquen individualmente a las personas físicas sobre la base de sus datos biométricos para deducir o inferir su raza, opiniones políticas, afiliación sindical, convicciones religiosas o filosóficas, vida sexual u orientación sexual* (...)" (art. 5.1 g) RIA) han quedado expresamente prohibidos. El fundamento de tan severa exclusión se encuentra, como expresa el Considerando (48) RIA, en el "desequilibrio de poder en el contexto laboral (…), unido al carácter intrusivo de estos sistemas, dichos sistemas podrían dar lugar a un trato perjudicial o desfavorable de determinadas personas físicas o colectivos enteros". Lo que lleva a prohibir "la introducción en el mercado, la puesta en servicio y el uso de sistemas de IA destinados a ser utilizados para detectar el estado emocional de las personas en situaciones relacionadas con el lugar de trabajo (…)".

VIII. El nacimiento de los neurodatos

Las neurotecnologías se basan en la recolección sin esfuerzo de cantidades masivas de datos, trátese tanto de modelos invasivos, como no invasivos[29]. Debido a las muchas funciones del cerebro y a su intensa actividad las 24 horas del día, los 7 días de la semana, "los dispositivos o servicios relacionados con la neurotecnología tienen el potencial de recopilar muchos neurodatos y, con ellos, las neurotecnologías pueden inferir la salud o el estado físico y mental de las personas (por ejemplo, resolución de problemas, razonamiento, toma de decisiones, comprensión, recuperación de memoria, percepción, lenguaje, emociones)". Por lo tanto, "se trata de un tratamiento muy intrusivo, si no el más intrusivo, que invade la intimidad mental y, en ocasiones, la integridad mental de la persona afectada. La recolección de huellas cerebrales introduce otros elementos de intrusión. Esto se debe a la posibilidad de inferir información relacionada con las experiencias de los interesados sin que estos las compartan explícitamente o a la posibilidad de perfilar a los interesados en función de patrones de ondas cerebrales"[30].

[29] I. BELTRÁN DE HEREDIA RUIZ, *Inteligencia artificial y neuroderechos: la protección del yo inconsciente de la persona*, Pamplona, Aranzadi, 2023, p. 148.

[30] Informe conjunto elaborado por la Agencia Española de Protección de Datos (AEPD) y el Supervisor Europeo de Protección de Datos (EDPS) sobre el tratamiento de neurodatos.

Como señala el informe conjunto elaborado por la Agencia Española de Protección de Datos (AEPD) y el Supervisor Europeo de Protección de Datos (EDPS) sobre el tratamiento de neuro datos, las referidas singularidades se han utilizado en diferentes trabajos de investigación para construir sistemas de autenticación basados en ondas cerebrales, pero pueden servir también para distinguir a los individuos para otros fines, como, por ejemplo, la elaboración de perfiles.

Existe, por ello, un vínculo estrecho entre los sistemas neurotecnológicos y los datos personales de la persona trabajadora en la medida en que los primeros se pueden alimentar de neurodatos. Existe evidencia que indica que estos datos, en tanto que biométricos, permiten identificar de forma única a las personas, por lo que, sin lugar a duda, los neurodatos de los seres humanos son también datos personales. Los mismos que han sido definidos como la información que se recoge del cerebro y/o del sistema nervioso, pueden venir a constituir una categoría diferenciada y cualificada de los datos biométricos en tanto que datos que pertenecen únicamente al dominio del cerebro. En 2019, la OCDE en el primer instrumento jurídico internacional sobre neurotecnología definió los datos cerebrales personales como "datos relacionados con el funcionamiento o la estructura del cerebro humano de un individuo identificado o identificable que incluye información única sobre su fisiología, salud o estados mentales".

La ingente recolección de datos llevada a cabo por las neurotecnologías, junto con su creciente difusión, anticipa la creación de bases de datos masivas de neurodatos. No sorprende por ello que alguna de las primeras respuestas para afrontar este nuevo reto se centre en el control y limitación del tratamiento de esta categoría especial de datos. Así en Brasil, el Projeto de Lei 522/2022 que modifica a Lei n° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), se dirige a regular los límites de este tipo particular de datos biológicos. El proyecto normativo parte de la definición de dato neuronal como "cualquier información obtenida, directa o indirectamente, de la actividad del sistema nervioso central y cuyo el acceso se realiza a través de interfaces cerebro-computadora, o cualquier otra tecnología, invasiva o no invasiva". Sobre esta base, limita el tratamiento estos datos a supuestos muy puntuales y determinados por razones de investigación o clínicas y dentro del ámbito sanitario. Precisando que cuando se necesario el consentimiento para el tratamiento de datos neuronales se debe indicar, de forma clara y destacada, los posibles efectos físicos, cognitivos y emocionales de aplicación, contraindicaciones y las normas sobre medidas de privacidad y seguridad de la información utilizadas

En Estados Unidos esta senda es seguida por una la enmienda a la California Consumer Privacy Act, actualmente en tramitación, que incorpora el concepto de "datos neuronales", entendiendo por tales: "la información generada por la medición de la actividad de los sistemas nerviosos centrales o periféricos de un individuo". De igual modo, el 17 de abril de 2024, la Cámara de Representantes y el Senado de Colorado aprobaron un proyecto de ley para proteger la privacidad de los datos biológicos y neuronales de las personas. La futura modificación de la "Colorado Privacy Act", amplía la definición de "datos sensibles" para incluir los datos biológicos, que son "datos que proporcionan una

caracterización de las propiedades, composiciones o actividades biológicas, genéticas, bioquímicas o fisiológicas del cuerpo o las funciones corporales de una persona". Los datos biológicos incluyen los datos neuronales, definidos como la "información relativa a la actividad del sistema nervioso central o de los sistemas nerviosos periféricos de una persona, incluidos el cerebro y la médula espinal, y que pueden procesarse mediante un dispositivo o con su ayuda".

La configuración de los datos neuronales como una categoría diferenciada o cualificada de los datos biométricos, así como la búsqueda de un adecuado punto de equilibrio entre la prohibición radical y la admisión de determinados usos, requerirá de una profunda reflexión.

IX. ¿Datos del cuerpo imagen?

Se ha dicho con acierto que el futuro de la protección de la privacidad "quizá deba aspirar a la superación de las actuales categorías (datos personales, datos no personales, datos sensibles, datos no sensibles), que solo reflejan los datos en el momento de su recogida, pero ignoran los usos subsiguientes y sus potenciales transformaciones"[31]. Probablemente, la categoría de los datos sintéticos (art. 10.5 a) RIA) que ahora incorpora el RIA se dirige a dotar de cobertura a esos espacios, hasta ahora, vacíos. En todo caso, las particularidades del uso del Big Data y sus riesgos exigen seguir desarrollando "técnicas de protección sistémica de los datos"[32], más allá de la que proporciona en la actualidad la normativa para la protección de los datos personales.

Pero los retos a los que nos enfrentamos no paran aquí. En un libro de lectura esencial[33] se señala cómo "millones de imágenes capturadas por cámaras ajenas o servidas por nuestros propios teléfonos móviles han acabado por depositarse en un mundo paralelo mucho más poblado y mucho más frecuentado que el de nuestros espacios corporales, y ello, añade, hasta el punto de que puede decirse sin exagerar que hoy son mucho más visibles nuestras imágenes que nuestros cuerpos". El resultado es que "el espejo ha triunfado sobre el cuerpo y se ha emancipado de él". Este nuevo dualismo entre el "cuerpo físico" (con su parte física y su dimensión emocional) y el "cuerpo imagen" nos debe hacer reflexionar sobre el alcance de los retos que tenemos por delante y en los que el "cuerpo" en sus más diversas y plurales dimensiones cobra y cobrará un protagonismo esencial. Estamos, probablemente, asistiendo al nacimiento y primeras etapas de una realidad que alcanzará dimensiones difícilmente imaginables en los próximos tiempos. El universo de la biometría sigue avanzando hacia su irrefrenable expansión…

[31] J. BAZ RODRIGUEZ, *Privacidad y protección de datos de los trabajadores en el entorno digital*, cit., p. 242.
[32] W. HOFFMANN-RIEM, W., *Big Data. Desafíos también para el Derecho*, cit., p. 152.
[33] S. ALBA RICO*, Ser o no ser (un cuerpo)*, Barcelona, Seix Barral, 2017, pp. 277-278.