Protección de datos y contrato de trabajo

Ignasi Beltran de Heredia Ruiz

Catedràtic de Dret del Treball i de la Seguretat Social

22 abril 2026

Investigació que forma part del projecte de recerca del Ministerio de Ciencia e Innovación titulat “Algoritmos extractivos y neuroderechos. Retos regulatorios de la digitalización del trabajo” ref. PID2022-139967NB-I00

Contexto

NUEVO POLVO DE ORO y CADÁVERES DE ELEFANTES

ENCAPSULA-MIENTO REALIDAD

CORRELACIÓN Y EL SUERO DE LA VERDAD DIGITAL

PRIVACIDAD DEVALUADA

Contexto

Article | Open access | Published: 11 January 2021

Facial recognition technology can expose political orientation from naturalistic facial images

Michal Kosinski

Scientific Reports **11**, Article number: 100 (2021) | Cite this article

234k Accesses | **168** Citations | **2285** Altmetric | Metrics

Journal Information
Journal TOC

APA PsycArticles: Journal Article

Presentation in self-posted facial images can expose sexual orientation: Implications for research and privacy.

© Request Permissions

Wang, D. (2022). Presentation in self-posted facial images can expose sexual orientation: Implications for research and privacy. *Journal of Personality and Social Psychology, 122*(5), 806–824. https://doi.org/10.1037/pspa0000294

Recent research has found that facial recognition algorithms can accurately classify people's sexual orientations using naturalistic facial images, highlighting a severe risk to privacy. This article tests whether people of different sexual orientations presented themselves distinctively in photographs

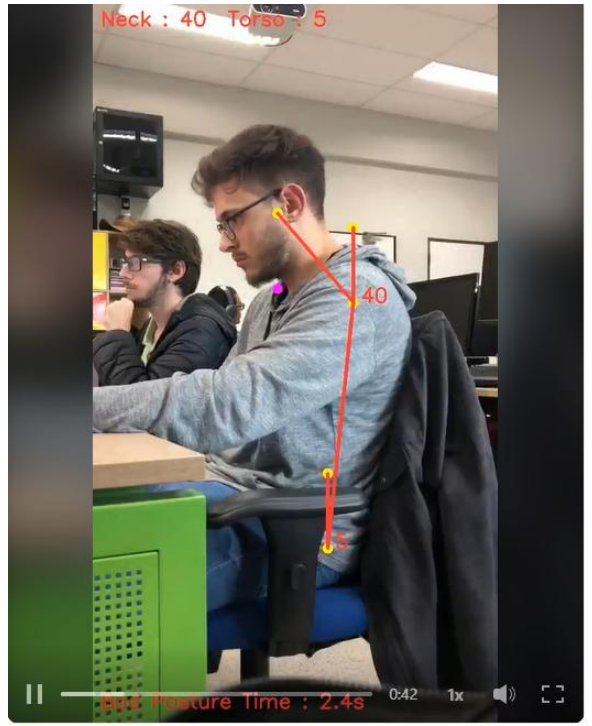
Contexto


Cámaras inteligentes de fatiga y distracción
La solución completa de inteligencia artificial para seguridad vial de las flotas: Su operación más segura a través de la tecnología Trimble de cámaras inteligentes de fatiga y otros comportamientos de riesgo.
Hablar con un experto
Vea la demostración

Contexto

Myontec: ErgoAnalysis lleva la carga física del trabajo a números. Es una solución para aumentar el rendimiento organizacional y el bienestar de los empleados a través del monitoreo y análisis de la carga física relacionada con el trabajo.

La solución basada en ropa inteligente captura la activación de la parte superior del cuerpo y los músculos grandes de las piernas (EMG), los movimientos y la frecuencia cardíaca combinados con video. Los algoritmos analizan la distribución de la carga, la carga estática, las microroturas, la sobrecarga y las posiciones de flexión

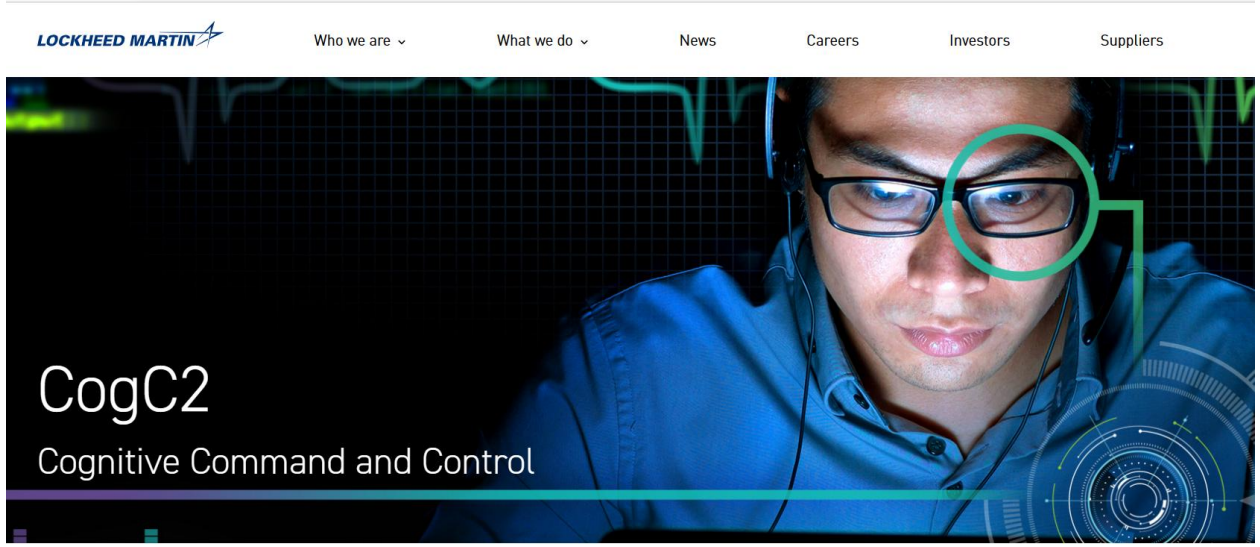


Contexto

Dispositivo con sensores de electroencefalografía (EEG) que permiten a los **empleadores rastrear las ondas cerebrales de los empleados** para detectar niveles de estrés y atención mientras trabajan. El propósito es **medir la productividad mientras se está trabajando**.

El sistema *Focus UX* **lee «los estados cognitivos humanos en tiempo real** y comparte comentarios personalizados con los empleados, y sus gerentes que los rastrean, sobre su rendimiento cognitivo (carga, estrés, niveles de atención) mientras están en el trabajo».

Contexto



Evaluar la carga de trabajo cognitiva en tiempo real (CogC2 - *Cognitive Command and Control*)

Dispositivo de detección cerebral diseñado por la empresa *SmartCap*. En concreto, evalúa los niveles de fatiga mediante «el monitoreo de las ondas cerebrales de sus usuarios y así detectar la aparición de microsueños y que crean riesgos de seguridad».

Art. 4.1 RGPD. “**Datos personales”**: *toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*;

Art. 4.2 RGPD. “**Tratamiento**”: “*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”.*

Delimitación del concepto “datos personales”: Los servicios de itinerancia de una línea de teléfono móvil, que incluyen la ubicación de su usuario, forman parte del derecho a la intimidad (STEDH 6 de noviembre 2025, Caso Guyvan c. Ucrania)

Trabajador autorizado para emplear el teléfono de la empresa para fines personales (con el compromiso del trabajador de asumir el reembolso de su uso personal). Empresa utiliza los datos de la línea telefónica por ella contratada no sólo para detraer el coste, sino para (entre otros) **extraer datos de localización fuera del país y lo acaba despidiendo**. **Recordatorio Doctrina Barbulescu**:

a) si el empleado **ha sido informado** de la posibilidad de que el empleador pudiera tomar medidas para **monitorizar las comunicaciones** y de la **implementación de dichas medidas**,
b) el **alcance de dicha monitorización** y el **grado de su intrusión** en la privacidad del empleado,
c) si el empleador ha proporcionado **razones legítimas para justificar** la monitorización,
d) si habría sido posible implementar métodos y medidas **menos intrusivos**,
e) las **consecuencias de la monitorización** para el empleado sometido a ella, y si este ha contado con **garantías adecuadas contra la arbitrariedad**; y
f) garantizarle el **acceso a un recurso** ante el órgano judicial competente para valorar los anteriores criterios.

Tal **exceso de información**, no precisa para los fines legítimos autorizados por su recopilación, deviene invasión de la intimidad del empleado (la ubicación en un momento determinado lo es), cuya justificación había de evaluarse por los tribunales nacionales, pero, al no realizarse dicha valoración en su integridad, fallaron en la tutela que debían dispensarle con arreglo al art. 8 CEDH

Delimitación del concepto “datos personales” y seudonimización

STJUE 4 de septiembre 2025 (C-413/23), *Supervisor Europeo de Protección de Datos (SEPT)*: la **seudonimización no constituye un elemento de la definición de "datos personales“**. Se refiere a la adopción de medidas técnicas y organizativas destinadas a **reducir el riesgo de correlación de un conjunto de datos con la identidad de los interesados**; y, según el C17 RGPD, la seudonimización «[solo] puede reducir los riesgos» de correlación para esos interesados y, de este modo, «ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos»

STS 12 de marzo 2026 (rec. 55/2025), “el concepto de «seudonimización» **presupone la existencia de información que permite identificar al interesado y la propia existencia de esa información** impide que los datos que hayan sido objeto de seudonimización puedan considerarse datos anónimos, excluidos del ámbito de aplicación del RGPD”.

> “Ahora bien, en la medida en que se **conserven por separado** la información que permita casar el seudónimo con la identidad real de la persona y se hayan adoptado las medidas técnicas y organizativas necesarias, con ello se evita que el interesado pueda ser identificado solo con los datos seudonimizados”.
>
> **Si las medidas se han adoptado y son suficientes**, la seudonimización afecta al carácter personal de esos datos. Si, a la vista de todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos, se concluye que una persona **no es capaz identificar directa o indirectamente a la persona física oculta tras el seudónimo, esos datos seudonimizados dejan de tener la naturaleza de datos personales** para esa persona física”

Delimitación del concepto “datos personales” y seudonimización

STS 12 de marzo 2026 (rec. 55/2025),

> “la existencia de **información adicional** que permita identificar al interesado no implica, por sí sola, que deba considerarse que los **datos seudonimizados constituyan, de cualquier forma y para cualquier persona, datos personales**”
>
> > **STJUE 7 de marzo 2024** (C-479/22), *OC/Comisión*, “introdujo la diferenciación entre la capacidad de las distintas personas y entidades para **identificar a las personas físicas ocultas detrás del seudónimo**, prestando especial atención a la **posibilidad razonable de que el público interesado identifique a esa persona, en particular mediante una combinación de los datos asociados al seudónimo con la información disponible en internet**.
> >
> > Un **medio no puede ser utilizado razonablemente para identificar** al interesado cuando el **riesgo de identificación resulte, en realidad, insignificante** porque la identificación de esa persona sea prácticamente irrealizable, por ejemplo porque implique un esfuerzo desmesurado en cuanto a tiempo, costes y recursos humanos”

Delimitación del concepto “datos personales” y seudonimización

STS 12 de marzo 2026 (rec. 55/2025), los datos seudonimizados deben considerarse “personales” cuando no pueda excluirse que los terceros a los que se transmitan puedan razonablemente atribuirlos al interesado

> **SSTJUE 19 de octubre 2016** (C-582/14), *Breyer*; y **7 de marzo 2024** (C-604/22), *IAB Europe*: unos **datos que por sí solos serían impersonales, pero relacionados de hecho con una persona física identificable, pasan a ser datos personales** si existen vías legales para obtener de otros información adicional que permita identificar a esa persona.
>
> El hecho de que la información que permita identificar al interesado se encuentre en manos de diferentes personas **NO** determina que no estemos dante datos personales cuando no impida efectivamente la identificación.
>
> **STJUE 9 de noviembre 2023** (C-319/22), *Gesamtverband Autoteile-Handel*: **los datos que por sí mismos son impersonales** pueden adquirir carácter «personal» cuando el responsable del tratamiento los pone a disposición de otras personas que dispongan de medios que puedan permitir razonablemente la identificación del interesado.

“**Debe hacerse una valoración dinámica de los datos para determinar si se trata de datos personales**. **No hay un concepto absoluto de los mismos**, sino que unos datos seudonimizados o que de otra forma no aparezcan vinculados directamente a una persona física concreta e identificada serán considerados o no como personales **en función de que la concreta persona que los reciba tenga medios para, de forma razonable, realizar una atribución de los datos a personas físicas concretas**. Según dicho concepto dinámico (…) unos mismos datos pueden ser personales para unos destinatarios y no serlo para otros, en función de los medios que cada destinatario tenga para realizar la atribución”

Art. 88 RGPD y los CCOL como títulos legitimadores (como la ley - *ex* art. 6.1.c RGPD) para el tratamiento de datos personales

STS 12 de marzo 2026 (rec. 55/2025): el **art. 88 RGPD permite que sean los convenios colectivos los que establezcan disposiciones sobre tratamiento de datos** en el ámbito laboral. No obstante (ex **STJUE 19 de diciembre 2024**, C-65/23, *MK c. K GmbH*) esto **NO** les **exima del cumplimiento de las exigencias derivadas del art. 5** (principios relativos al tratamiento, como la limitación de la finalidad y minimización de datos), **art. 6.1** (condiciones de licitud del tratamiento) y **art. 9** (categorías especiales de datos)

La obligación empresarial de **publicar los escalafones** previstos en el art. 12 del II convenio colectivo de Tripulantes de Cabina de Pasajeros (TCP) de EasyJet Airlines Spain **NO** puede entenderse debidamente cumplida en el caso de que la **empresa publique en su intranet un listado de trabajadores con los datos de identidad sustituidos por un código numérico de doce dígitos** (exigiéndose, por tanto, que determinados datos personales – como el nombre y apellidos – no sean seudonimizados).

> «dado que se trata de **datos generales que no pertenecen a categorías especiales** (nombre y apellidos, antigüedad en la empresa y en la base), **no existe motivo para magnificar la transcendencia de los mismos**, dado que se trata exclusivamente de **datos puramente laborales y con un impacto menor en la vida del interesado**. No existe desproporción alguna por tanto en el derecho informativo previsto en el convenio colectivo cuando sus destinatarios son los trabajadores que potencialmente pueden participar en los procedimientos competitivos, esto es, los restantes TCP.

Protección de datos y derecho de información

STS 8 de marzo 2022 (rec. 130/2019) (1 de 2)

una entidad bancaria **no puede utilizar su conocimiento de los datos de la cuenta corriente de una trabajadora para configurar prueba de los posibles incumplimientos laborales realizados por la empleada titular de la referida cuenta**. Declarado el despido procedente en suplicación (corrigiendo la improcedencia declarada en la instancia porque estima que se ha acreditado la vulneración de la normativa interna y el uso inadecuado de los aplicativos del Banco), la empresa interpone recurso de casación porque entiende que, al declararse inválida (en la instancia y suplicación) la prueba de auditoria sobre las cuentas de las que esta era titular, se han vulnerado los arts. 6.2 LOPD en relación con los artículos 18.1 y 18.4 CE y con el artículo 90.2 LRJS; así como del art. 20.3 ET en relación con los mencionados preceptos constitucionales.

El TS entiende que «**datos de la cuenta corriente de la trabajadora fueron usados, sin autorización ni información previa de la trabajadora, para fines distintos de los que podrían derivarse de una legitima finalidad, anudada al contrato mercantil sobre cuenta corriente bancaria existente entre las partes**».

> "es complemento indispensable del derecho fundamental del art. 18.4 CE la facultad de **saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo**.
>
> En consecuencia, constituye elemento caracterizador de la definición constitucional del art. 18.4 CE , **de su núcleo esencial, el derecho del afectado a ser informado de quién posee los datos personales y, especialmente por lo que a los presentes efectos interesa, con qué fin son utilizados**"

Protección de datos y excepción del consentimiento (art. 6.2 LOPD)

STS 8 de marzo 2022 (rec. 130/2019) (2 de 2):

La excepción del **consentimiento del art. 6.2 LOPD, no es extensible a los datos de una cuenta corriente** del empleado de un banco.

La **excepción debía aplicarse** única y exclusivamente a los supuestos de tratamiento de datos referido a los que son indispensables e imprescindibles para el mantenimiento o ejecución de la relación contractual, sin perder de vista que, en todo caso, **sería indispensable el cumplimiento del deber de información previa a la interesada sobre la finalidad o finalidades del tratamiento**. Y, en segundo lugar, porque la **mayoría de los datos contenidos en la cuenta corriente, nada tienen que ver con el mantenimiento o cumplimiento del contrato de trabajo**, sino con el contrato mercantil a que se ha hecho referencia

> "el conocimiento extracontractual laboral de los datos de la cuenta corriente, inevitable por la existencia de la relación mercantil entre las partes, ya situaba, legítimamente, en una posición privilegiada a la empresa que derivaba de dicho conocimiento, por lo que podía, bien intentar probar las presuntas irregularidades cometidas a través de otros medios de prueba, bien solicitar del órgano judicial autorización, al amparo del artículo 90.4 LRJS , para el acceso y utilización de los datos de la cuenta corriente, previo cumplimiento de las exigencias que dicho precepto establece".

Videocámara

STSJ Galicia 6 de marzo 2026 (rec. 4788/2025), despido disciplinario improcedente porque la prueba de la conducta imputada (apropiación de un bloc de notas por valor de 2,65 €) se ha obtenido mediante imágenes captadas por una cámara que no cumple con requisitos de **art. 89 LOPD**:

> "no se acredita por la empresa ni que las cámaras fueran visibles, ni que se hubiera informado a los trabajadores de su utilización de videovigilancia con finalidad de control y disciplina laboral, ni que siquiera estén debidamente señalizadas, por lo que ha de considerarse incumplidos los requisitos exigidos en el art. 89 LOPD, razón por lo que **no podrá ser tenido en cuenta el visionado de dichas grabaciones para resolver la presente litis**, al no hacer plena válida en juicio, debido a que la parte demandada no acredita el legítimo uso de las cámaras con fines de videovigilancia de los trabajadores, no solo no lo acredita, sino que ni siquiera propone ninguna prueba en tal sentido".

1. Los empleadores podrán tratar las imágenes obtenidas a través de sistemas de cámaras o videocámaras para el ejercicio de las funciones de control de los trabajadores o los empleados públicos previstas, respectivamente, en el art. 20.3 ET y en la legislación de función pública, siempre que estas funciones se ejerzan dentro de su marco legal y con los límites inherentes al mismo. Los empleadores habrán de informar con carácter previo, y de forma expresa, clara y concisa, a los trabajadores o los empleados públicos y, en su caso, a sus representantes, acerca de esta medida. En el supuesto de que se haya captado la comisión flagrante de un acto ilícito por los trabajadores o los empleados públicos se entenderá cumplido el deber de informar cuando existiese al menos el dispositivo al que se refiere el art. 22.4 de esta ley orgánica.

2. En ningún caso se admitirá la instalación de sistemas de grabación de sonidos ni de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores o los empleados públicos, tales como vestuarios, aseos, comedores y análogos.

3. La utilización de sistemas similares a los referidos en los apartados anteriores para la grabación de sonidos en el lugar de trabajo se admitirá únicamente cuando resulten relevantes los riesgos para la seguridad de las instalaciones, bienes y personas derivados de la actividad que se desarrolle en el centro de trabajo y siempre respetando el principio de proporcionalidad, el de intervención mínima y las garantías previstas en los apartados anteriores. La supresión de los sonidos conservados por estos sistemas de grabación se realizará atendiendo a lo dispuesto en art. 22.3 LOPD

Videocámara + audio

Uso de sistema de videovigilancia en el centro de trabajo que, además de imagen, incorpora captación de sonido. La empresa utilizó una de las grabaciones para proceder al despido de una trabajadora por criticar a la empresa en la conversación que mantuvo con una clienta. La trabajadora denuncia a la empresa, quien fue sancionada por la AEPD al considerar que la grabación de audio carecía de base jurídica suficiente y resultaba desproporcionada.

SAN\C-A 29 de septiembre 2025 (rec. 1913/2022) confirma la sanción e indica que la captación de voz implica una intromisión significativamente más intensa que la imagen (exige una justificación reforzada que en el caso no concurría)

Tanto la imagen como la voz constituyen datos de carácter personal (art. 4.1 RGPD y **SSAN\C-A 19 de diciembre 2018**, rec. 286/2017, **27 de diciembre 2019**, rec. 786/2018; y **9 de enero de 2023**, rec. 1716/2021) en la medida en que permite identificar a la persona afectada (STJUE 11 de diciembre 2014, C-212/13, *František Ryneš*)

> STC 119/2022 (licitud de prueba videográfica) establece que, en el ámbito laboral, el tratamiento de datos personales puede entenderse implícitamente consentido si es necesario para la ejecución del contrato. El deber de información sigue siendo esencial y debe ser previo, claro y expreso. La instalación de cámaras es constitucional si se encuentra justificada por indicios de irregularidades, y resulte idónea, necesaria y proporcionada, y no se coloca en espacios de especial intimidad ni con uso generalizado. La STC 98/2000, relativa a la grabación de audio: tal medida solo es legítima si existe una necesidad empresarial acreditada y si no hay medios menos invasivos

[**OJO** futuro/Presente: con captación de imágenes y uso de la IA (posible transcripción mediante “lectura” labios)]

Grabación indiscriminada

STSJ Canarias 15 de junio 2021 (rec. 52/2021): Responsable de comunicación de grupo parlamentario. Grabación de conversaciones telefónicas que mantiene. La grabación sistemática de conversaciones por parte del trabajador es motivo de despido disciplinario

Despido disciplinario: ilicitud de la prueba y confesión

STS 28 de enero 2026 (rec. 1947/2024), recogiendo el criterio de la **STC 86/1995**, entiende que, aunque se hubiera declarado la ilicitud de una prueba (en ese caso, de intervención telefónica), si posteriormente se produce la confesión del acusado, este medio de prueba sí que es válido.

Control jornada laboral – control de la asistencia y acceso laboral a las dependencias - y huella dactilar

AEPD / EXP202304834 / 30/10/24 (colegio notarial Aragón)

Art. 4.14 RGPD: **datos biométricos**: *datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la* ***identificación única*** *de dicha persona, como imágenes faciales o datos dactiloscópicos*

Los datos biométricos tratados (recogida o captura de datos, registro, almacenamiento, procesamiento, comparación, autenticación, conservación, supresión, limitación…etc) se consideran datos de carácter personal siempre y cuando la finalidad del tratamiento sea la identificación o autenticación de una persona- *que permitan o confirmen la identificación única de dicha person*

> **Plantillas biométricas que se generan en los sistemas de control de acceso** (*software de gestión del sistema almacena el hash (patrón o plantilla biométrica) que proporciona el terminal de huella dactilar, el cual se relaciona con el usuario final con el id de usuario del empleado en una tabla para los datos biométricos)* **constituyen datos de carácter personal** dado que el proceso se basa en asignar un identificador (la plantilla biométrica obtenida al recoger las muestras de huella dactilar de los trabajadores en el momento en que se produzca su acceso a las dependencias de la parte reclamada) que permite singularizar a un individuo- el trabajador- y, distinguirlo frente a otros, a través de "*elementos propios de la identidad física, fisiológica, genética, psíquica*", gracias a su cotejo con la muestra previamente guardada.

Impresiones dactilares describen **datos únicos**, permanentes o definitivos en el tiempo, ya que permanecen invariablemente unidos a una persona: por tanto, tienen un impacto más significativo en el derecho fundamental a la protección de datos de su titular en comparación con otro tipo de datos personales. De ahí la especial relevancia que ha otorgarse a las garantías que se adopten en su tratamiento debido que la incidencia, especialmente significativa, en el derecho fundamental a la protección de datos personales de su titular (así lo recoge el art. 9 RGPD).

Control jornada laboral – control de la asistencia y acceso laboral a las dependencias - y huella dactilar

AEPD / EXP202304834 / 30/10/24 (colegio notarial Aragón)

STJUE 1 de agosto 2022 (C-184/20), *Vyriausioji tarnybinės etikos komisija*: **fija una interpretación amplia del concepto categorías especiales de datos personales: *una interpretación amplia de los conceptos de «categorías especiales de datos personales» y de «datos sensibles»*** *se ve respaldada por el objetivo de la Directiva 95/46 y del RGPD (…), de asegurar un alto nivel de protección de las libertades y de los derechos fundamentales de las personas físicas, en particular, de su intimidad, en relación con el tratamiento de los datos personales que las afectan*

STJUE 4 de julio 2023 (C-252/21), *Meta c. Bundeskartellamt:* "**cuando se recoge en bloque un conjunto de datos que contiene tanto datos sensibles como no sensibles sin que sea posible separar los datos entre sí en el momento de la recogida, el tratamiento de ese conjunto de datos debe considerarse prohibido,** en el sentido del art. 9.1 RGPD, si contiene al menos un dato sensible y no se aplica ninguna de las excepciones del art. 9.2, de dicho Reglamento" y destacó que "a los efectos de la aplicación de la excepción

Control jornada laboral – control de la asistencia y acceso laboral a las dependencias - y huella dactilar

AEPD / EXP202304834 / 30/10/24 (colegio notarial Aragón)

Art. 9.2.b RGPD el levantamiento de la prohibición de tratar categorías especiales de datos exige:

1. El tratamiento ha de ser ***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*

2. El tratamiento **ha de ser autorizado –** ***en la medida en que así lo autorice*** por el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros

3. El instrumento a través del cual se articule dicha autorización deberá establecer ***garantías adecuadas*** del respeto de los derechos fundamentales y de los intereses del interesado

4. El responsable debe acreditar también que su tratamiento se puede realizar porque **concurre una de las bases jurídicas legitimadoras del tratamiento *ex* art. 6.1 RGPD**, que son requisito general para el tratamiento de cualquier dato de carácter personal.

Control jornada laboral – control de la asistencia y acceso laboral a las dependencias - y huella dactilar

STJUE 4 de julio 2023, C-252/21, *Meta Platforms Inc.*: **las excepciones a la prohibición de tratamiento de las categorías especiales de datos deben ser interpretadas restrictivamente**.

AEPD / EXP202304834 / 30/10/24 (colegio notarial Aragón): **Una normativa estatal como el ET que obliga al registro horario (sin indicar que deba hacerse mediante un control biométrico) no es una habilitación suficiente subsumible en el art. 6.1.b RGPD**

> (se aparta de **STS\C-A 2 de julio 2007,** Rec. 5017/2003: considera legítimo el tratamiento de los datos biométricos para el control horario de los empleados públicos, sin que fuese necesario un consentimiento previo de los afectados. La tecnología empleada, así como la matemática primitiva que desarrolla la captura, garantiza una protección ante falsificaciones, robos o reversibilidad en la replicación de la huella)

SAN\C-A 11 de febrero 2026 (rec. 65/2022), **lectores de huella tanto para la entrada y salida de la nave como para el acceso a vestuarios y aseos**, justificando la medida en razones de seguridad y control de accesos. La AEPD sancionó esta medida empresarial por vulneración del principio de minimización de datos. La AN confirma la infracción, pero reduce la sanción (a apercibimiento). Que sea útil (en términos de seguridad) no significa que sea necesario (debe acreditarse que no hay una alternativa menos intrusiva – especialmente porque el registro es continuo)

Control jornada laboral – control de la asistencia y acceso laboral a las dependencias - y huella dactilar

SJS\3 Coruña 24 de julio 2025 (núm. 370/2025), validez registro con huella dactilar: “el uso del sistemas biométricos como el control de acceso mediante huella dactilar a un hospital sigue siendo un medio seguro y adecuado para garantizar la protección de bienes, personas y servicios esenciales, y no vulnera ninguno de los derechos fundamentales consistente privacidad, a la intimidad contenido en el art. 18 CE; vulneración del derecho a la salud contenido en el art. 43 CE; vulneración del derecho a libertad a la libertad sindical, art. 28 CE”

Informe AEPD REGAGE25e00024730156 (Julio 2025): tratamiento de datos personales mediante biometría que tiene por finalidad el **control de acceso basado en información biométrica a unas instalaciones de las Fuerzas y Cuerpos de Seguridad del Estado** que incluían diferentes tipologías de instalaciones, bienes y personas.

El sistema biométrico respecto del que se formula la consulta se enmarca en un contexto especialmente sensible como es el de la protección de instalaciones concretas de las Fuerzas y Cuerpos de Seguridad del Estado. Se da una importante concurrencia de **intereses legítimos dignos de protección** alrededor de la seguridad pública, así como la protección de infraestructuras o materias clasificadas, todos estos intereses de especial relevancia. Se afirma la **justificación objetiva y necesidad concreta** de la implantación del sistema de autenticación biométrica, ya que permite verificar con mayor fiabilidad que otros mecanismos quién accede a los espacios protegidos, evita suplantaciones de identidad y permite restringir accesos no autorizados.

Los **desarrollos recientes en tecnologías biométricas**, como la consultada, por cuanto permiten reducir significativamente el impacto sobre los derechos de los interesados, lo cual tiene especialmente en cuenta en el análisis de la proporcionalidad del tratamiento de autenticación

Control jornada laboral – control de la asistencia y acceso laboral a las dependencias / reconocimiento facial

STSJ Galicia 15 de enero 2026 (rec. 144/2026) declara que se produce una **violación del derecho a la propia imagen en relación con la protección de datos, si la empresa utilizar el reconocimiento facial** para el registro de jornada. Especialmente porque «en este caso el tratamiento no era necesario, pues existían otros medios para el registro de jornada y horario sin injerencia en derechos fundamentales, como el control mediante una tarjeta, opción que la propia empresa señaló en el acta de la reunión»

SJS\2 Alicante 15 de septiembre 2023 (rec. 489/2023): sistema de registro de jornada basado en **reconomiento facial** supone una **violación de la intimidad de las personas trabajadoras**, dado su carácter desproporcionado.

Dictamen 11/2024 del CEPD se analiza **el uso del reconocimiento facial para agilizar el paso de pasajeros en aeropuertos**, concluyendo que puede ser compatible con los artículos 5.1.e) y f), 25 y 32 del RGPD en dos escenarios: uno en el que la plantilla biométrica se almacena en un dispositivo del propio pasajero y otro en el que hay almacenamiento centralizado, dentro del aeropuerto, de una plantilla biométrica de forma encriptada con una clave/secreto únicamente en poder del pasajero. En ambos casos, el tratamiento puede considerarse necesario si no existen alternativas menos intrusivas igual de eficaces y se aplican garantías descritas en dicho Dictamen. Entre estas garantías cabe destacar la existencia de alternativas viables o soluciones de respaldo; que el punto de control requerirá una acción positiva antes de iniciar la captura de fotos o vídeos; la prohibición de acceso externo a la identificación y a los datos biométricos; garantizar que el tratamiento se realice localmente en las fases de inscripción, transmisión y emparejamiento; aislar los puntos de control (único punto donde evaluar la coincidencia biométrica) de la red cuando estén en funcionamiento, conservar los datos biométricos en el punto de inscripción y en el punto de control solo durante un período muy breve y eliminarlos tan pronto se haya pasado por el punto de control, etc.

Informe de evaluación de impacto en la protección de datos – EIPD (C84 y 90 + 35 RGPD)

AEPD / EXP202304834 / 30/10/24 (colegio notarial Aragón)

> *EIPD: "en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo"*
>
> *"el responsable debe llevar a cabo, **antes del tratamiento**, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo"*

el tratamiento de datos biométricos se considera de alto riesgo (tratamientos que impliquen el uso de categorías especiales de datos; el uso de datos biométricos y los que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas) y consta entre los tratamientos incluidos en el documento "Listas de tipos de tratamiento de datos que requieren evaluación de impacto relativa a protección de datos"

Informe de evaluación de impacto en la protección de datos (C84 y 90 + 35 RGPD)

AEPD / EXP202304834 / 30/10/24 (colegio notarial Aragón)

> Las EIPD tienen como objetivo último la identificación de los riesgos que llevan aparejados determinados tratamientos personales en atención a su incidencia en el derecho fundamental a la protección de datos personales de sus titulares (…),
>
> > ha de entenderse que se configura como una obligación del responsable- en atención al principio de responsabilidad proactiva-
> >
> > ha de optarse por un enfoque de análisis de riesgos desde el diseño y por defecto, para poder identificarlos, determinar la probabilidad de materialización y su impacto, y prever medidas y garantías que eliminen o, cuando menos, mitiguen los riesgos detectados, evitando su materialización-
> >
> > debe realizarse con carácter previo al tratamiento y
> >
> > adaptarse continuamente en atención a la evolución de los riesgos y amenazas que puedan afectar al tratamiento

Informe de evaluación de impacto en la protección de datos (C84 y 90 + 35 RGPD)

AEPD / EXP202304834 / 30/10/24 (colegio notarial Aragón)

no basta con realizar formalmente una EIPD, sino que la misma, además de contener como mínimo la información del art. 35.7 del RGPD, deberá superarse y ser considerada válida.

Es decir, **no se trata de una obligación formal**, que se entienda cumplida con la mera realización de una EIPD, **sino material**, garantizando que la misma contenga un análisis sólido y exhaustivo

del tratamiento previsto,
de los riesgos que el mismo puede implicar y
de las medidas que se consideren convenientes para evitarlos o, al menos, minimizarlos.

Debe hacerse **con carácter previo al tratamiento**, de tal manera que las conclusiones de la EIPD puedan tenerse en cuenta en su diseño, cumpliendo así el principio de protección de datos desde el diseño y por defecto que contempla el artículo 25 RGPD.

La EIDP debe hacer **un análisis de la concurrencia de los preceptivos criterios de necesidad, idoneidad y proporcionalidad del tratamiento**. Y ello por cuanto el responsable que pretenda instaurar un tratamiento de datos personales de esta naturaleza ha de asegurarse que se supera lo que se ha denominado en la jurisprudencia "**el triple juicio de proporcionalidad**", planteándose en especial si el tratamiento de datos biométricos es necesario, idóneo y proporcional

Informe de evaluación de impacto en la protección de datos (C84 y 90 + 35 RGPD)

AEPD / EXP202304834 / 30/10/24 (colegio notarial Aragón)

> **STC 14/2003:** *"si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"*

Si existen otros sistemas no biométricos que permitan conseguir la misma finalidad de identificar-verificar la identidad de las personas con eficacia-, no será necesario iniciar tratamientos biométricos, y, por tanto, implantar este sistema se considerará contrario al RGPD.

Este juicio debe ser el punto de partida de su análisis, pues sólo en caso de que estos métodos superen el citado triple juicio, se exigirá el cumplimiento de otros requisitos o garantías.

En definitiva, el tratamiento de datos biométricos nunca podrá iniciarse de no haber elaborado una EIPD válida y previa al tratamiento

> "necesidad no debe confundirse con conveniencia y que no puede articularse una medida consistente en un tratamiento de datos personales de alto riesgo con base en la satisfacción de los intereses de una sola de las partes"

Directiva 2023/970 del Parlamento Europeo y del Consejo de 10 de mayo de 2023 por la que se refuerza la aplicación del principio de igualdad de retribución entre hombres y mujeres por un mismo trabajo o un trabajo de igual valor a través de medidas de transparencia retributiva y de mecanismos para su cumplimiento

Protección de datos (art. 12)

En la medida en que implique el tratamiento de datos personales, toda información proporcionada con arreglo a las medidas adoptadas en virtud de los artículos 7 (“Derecho a la información”), 9 (“Información sobre la brecha retributiva entre trabajadores y trabajadoras”) y 10 (“Evaluación retributiva conjunta”) se facilitará de conformidad con el RGPD.

Ningún dato personal tratado con arreglo a los artículos 7, 9 o 10 podrá utilizarse con fines distintos de la aplicación del principio de igualdad de retribución.

Los Estados miembros podrán decidir que, cuando la divulgación de información con arreglo a los artículos 7, 9 y 10 dé lugar a la divulgación, directa o indirecta, de la retribución de un trabajador identificable, solo tengan acceso a dicha información los representantes de los trabajadores, la inspección de trabajo o el organismo de fomento de la igualdad.

> Los representantes de los trabajadores o el organismo de fomento de la igualdad asesorarán a los trabajadores acerca de la posibilidad de interponer una demanda al amparo de la presente Directiva sin revelar los niveles retributivos efectivos de cada uno de los trabajadores que realizan el mismo trabajo o un trabajo de igual valor. A los efectos de seguimiento con arreglo al artículo 29, la información estará disponible sin restricciones.

Protección de datos (art. 12)

STS 21 de noviembre 2024 (rec. 218/2023), discrepando de lo apuntado por la **SAN 23 de febrero 2023** (rec. 355/2022) establece que el registro es de los valores medios de los salarios desagregados por sexo, por lo que en principio no es obligado incluir datos que permitan identificar la retribución individualizada de una persona trabajadora

STS 15 de enero 2025 (rec. 136/2023): “La ausencia de concreción en los casos en los que hay muy pocos trabajadores del mismo sexo no comporta la quiebra del art. 28 ET y su desarrollo reglamentario, pues no cabe olvidar el objetivo perseguido por el legislador que ahora reiteramos: identificar las discriminaciones, directas e indirectas dimanantes de una incorrecta valoración de los puestos de trabajo cuando se desempeñe un trabajo de igual valor, y erradicar las desigualdades retributivas».

Protección de datos y decisiones automatizadas (¿una selección de un candidato / despido?)

Anexo III del RIA: "**alto riesgo**" determinados sistemas de IA utilizados para, entre otras dimensiones laborales, el despido

> estos sistemas de IA están sujetos a requisitos legales relativos a la gestión de riesgos (art. 9), la calidad de los datos y la gobernanza de datos (art. 10), la documentación y la conservación de registros (arts. 11 y 12), la transparencia y la comunicación de información a los usuarios (art. 13), la supervisión humana (art. 14), la precisión, la solidez y la ciberseguridad (art. 15), y la información sobre la utilización de IA de alto riesgo en el lugar de trabajo, so pena de multa administrativa de hasta 15.000.000 EUR o de hasta el 3 % del volumen de negocios mundial total anual. [art. 99, ap. 4, letra g)]

Art. 22 RGPD: "admitiría" el uso de decisiones automatizadas para despedir (el "despido" sería subsumible en el concepto de "ejecución" de un contrato - **STJUE 7 de diciembre 2023**, C-634/21, *SCHUFA Holding, Scoring*) **si se cumplen todos estos condicionantes:**

- **art. 64.4.d ET** + **DDFF** + **art. 23 Ley 15/2022** (para el sector público)

- **Uso** debe ser **"necesario"**:

> (GT'29) "teniendo en cuenta si se puede adoptar un método menos invasivo para la intimidad" (volumen de datos a procesar es muy elevado – p.ej.: proceso de selección masivo; el "ruido" existente; el riesgo a la concurrencia de sesgos humanos; o bien, sea un método con menos margen de error – que el humano - para alcanzar un juicio predictivo).

Protección de datos y decisiones automatizadas (¿una selección de un candidato / despido?) **Condicionantes:**

STJUE 7 de diciembre 2023 (C-634/21), *SCHUFA Holding (Scoring)*, el art. 22 RGPD dispone que, en los casos a que se refiere la letra a), deben cumplirse las siguientes reglas acumulativas:

> "el responsable del tratamiento adoptará como mínimo medidas en relación con el **derecho del interesado a obtener intervención humana, a expresar su punto de vista y a impugnar la decisión**".

En la medida que los datos de entrenamiento y/o bien la propia configuración del algoritmo pueden arrojar **potenciales resultados discriminatorios**, también menciona requisitos más estrictos para riesgos específicos.

> Deben establecerse "garantías adecuadas y garantizar un **tratamiento leal y transparente** respecto del interesado".
>
> El responsable del tratamiento está obligado:
>
> - a "utilizar procedimientos matemáticos o estadísticos adecuados";
> - a "aplicar las medidas técnicas y organizativas apropiadas para garantizar que se reduzca al máximo el riesgo de error y se corrijan errores"; y
> - a "asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los intereses y derechos del interesado e impedir, entre otras cosas, los efectos discriminatorios en las personas físicas".

Protección de datos y decisiones automatizadas (¿una selección de un candidato / despido?) **Condicionantes:**

STJUE 7 de diciembre 2023 (C-634/21), *SCHUFA Holding (Scoring)*

GT29: el responsable del tratamiento garantiza la **intervención humana en el tratamiento** si se cumplen cuatro requisitos:

- primero, **intervención humana por parte del responsable**;

- segundo, la supervisión humana de la **decisión ha de ser significativa** y no un simple gesto simbólico;

- tercero, ha de llevarse a cabo por una **persona autorizada, con competencia para modificar la decisión**; y,

- cuarto, dicha revisión implica la necesidad de una evaluación completa de todos los datos pertinentes, incluida cualquier información adicional facilitada por el interesado".

Protección de datos y decisiones automatizadas (¿una selección de un candidato / despido?) **Condicionantes:**

art. 14 RIA: "*sistema de IA de alto riesgo se ofrecerá al responsable del despliegue de tal modo que **las personas físicas a quienes se encomiende la supervisión humana puedan**, según proceda y de manera proporcionada a:*

*a) **entender adecuadamente las capacidades y limitaciones** pertinentes del **sistema de IA** de alto riesgo y **poder vigilar debidamente su funcionamiento**, por ejemplo, con vistas a detectar y resolver anomalías, problemas de funcionamiento y comportamientos inesperados;*

*b) **ser conscientes** de la posible tendencia a confiar automáticamente o en exceso en los resultados de salida generados por un sistema de IA de alto riesgo ("**sesgo de automatización**"), en particular con aquellos sistemas que se utilizan para aportar información o recomendaciones con el fin de que personas físicas adopten una decisión;*

*c) **interpretar correctamente los resultados de salida** del sistema de IA de alto riesgo, teniendo en cuenta, por ejemplo, los métodos y herramientas de interpretación disponibles;*

*d) **decidir, en cualquier situación concreta, no utilizar el sistema de IA** de alto riesgo o **descartar**, **invalidar** o **revertir los resultados de salida** que este genere;*

*e) **intervenir en el funcionamiento** del sistema de IA de alto riesgo o **interrumpir el sistema pulsando un botón de parada** o mediante un procedimiento similar que permita que el sistema se detenga de forma segura*".

Protección de datos y decisiones automatizadas (¿una selección de un candidato / despido?) **Condicionantes:**

Art. 10 Directiva (UE) 2024/2831 del Parlamento Europeo y del Consejo, de 23 de octubre de 2024, relativa a la mejora de las condiciones laborales en el trabajo en plataformas:

> "*Toda decisión de restringir, suspender o poner fin a la relación contractual o a la cuenta de una persona que realice trabajo en plataformas, o cualquier otra decisión que cause un perjuicio equivalente,* ***será adoptada por un ser humano***"

Protección de datos y decisiones automatizadas (¿una selección de un candidato / despido?) **Condicionantes:**

Una vez tomada la decisión automatizada, **STJUE 27 de febrero 2025** (C-203/22), *Dun & Bradstreet Austria,* en aras a poder expresar su punto de vista sobre esa decisión e impugnarla,

> "el interesado **puede exigir** al responsable del tratamiento, como «**información significativa sobre la lógica aplicada**», que este le explique, mediante información pertinente y en forma concisa, transparente, inteligible y de fácil acceso, el **procedimiento y los principios aplicados** concretamente para explotar, de forma automatizada, los datos personales relativos al interesado con el fin de obtener un resultado determinado, como [de acuerdo con el asunto controvertido] un perfil de solvencia".

TJUE hace **2 advertencias**:

> "**la mera comunicación de una fórmula matemática compleja, como un algoritmo, ni la descripción detallada de todas las etapas de la adopción de una decisión automatizada cumple tales requisitos**, en la medida en que ninguna de estas modalidades puede considerarse una explicación suficientemente concisa e inteligible".

> "**la complejidad de las operaciones que deban realizarse para la adopción de una decisión automatizada [no puede] exonerar al responsable del tratamiento de su deber de explicación**". Debiéndose añadir que, además de este "genuino derecho de explicación", "esta información constituye solo una parte de la información a la que atañe el derecho de acceso previsto por dicho artículo [art. 15], ya que este también se refiere a la **información sobre la importancia y las consecuencias previstas del tratamiento en cuestión para el interesado**".

Protección de datos y contrato de trabajo

¡Muchas gracias!

Ignasi Beltran de Heredia Ruiz

Catedràtic de Dret del Treball i de la Seguretat Social

22 abril 2026

Investigació que forma part del projecte de recerca del Ministerio de Ciencia e Innovación titulat "Algoritmos extractivos y neuroderechos. Retos regulatorios de la digitalización del trabajo" ref. PID2022-139967NB-I00