FACULTAD DE DERECHO

ANÁLISIS JURÍDICO DE LOS SISTEMAS DE RECONOCIMIENTO DE EMOCIONES EN EL ÁMBITO LABORAL

Autora: Irene Rubio Ortega

5º E-3 Analytics

Derecho Laboral

Tutora: Ana Higuera Garrido

Madrid

Marzo 2025

LISTADO DE ABREVIATURAS

- AEPD: La Agencia Española de Protección de Datos
- CDEI: Centre for Data Ethics and Innovation
- CEPD: Comité Europeo de Protección de Datos
- CPP: Colaboración público privada
- DGOI: Dirección General de Ordenación del Juego
- DGOJ: Dirección General de Ordenación del Juego
- DPD: Delegado de protección de datos
- EIPD: Evaluación de impacto relativa a la protección de datos
- ET: Estatuto de los trabajadores
- EDPB: Comité Europeo de Protección de Dato
- EU-OSHA: The European Agency for Safety and Health at Work
- IEEE SA: Institute of Electrical and Electronics Engineers Standard Association
- ITSS: Trabajo y Seguridad Social
- LOPDGDD: Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales
- LPRL: Ley de Prevención de Riesgos Laborales
- RGPD: Reglamento General de Protección de Datos
- RIA: Reglamento de Inteligencia Artificial
- SEPD: Supervisor Europeo de Protección de Datos

ÍNDICE

INTRODUCCIÓN

Cuando empecé a leer sobre los sistemas de reconocimiento de emociones, me sorprendió hasta qué punto estas tecnologías podían llegar a influir, o incluso condicionar, la vida laboral de las personas. No estamos hablando de ciencia ficción, sino de herramientas reales que ya permiten a las empresas interpretar estados emocionales a partir de expresiones faciales, tono de voz o ritmo cardíaco. Esta capacidad de "leer" emociones a través de datos biométricos despierta inevitablemente muchas preguntas jurídicas, éticas y prácticas. ¿Qué ocurre con la intimidad del trabajador? ¿Hasta dónde puede llegar el control empresarial? ¿Qué límites establece la legislación actual?

Este trabajo surge precisamente de esa inquietud. A lo largo de estas páginas, analizo el marco jurídico que regula el uso de estos sistemas en el entorno laboral, centrándome especialmente en el Reglamento Europeo de Inteligencia Artificial de 2024 que a partir de ahora llamaremos RIA, reglamento de IA o reglamento de Inteligencia artificial indistintamente y en las excepciones que abre para su uso. También reviso su encaje con otras normativas relevantes, como el Reglamento General de Protección de Datos (RGPD), la legislación española: la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) y el Estatuto de los Trabajadores (ET), y planteo posibles mejoras legislativas para asegurar una protección efectiva de los derechos fundamentales.

Lejos de limitarme a una exposición teórica, he intentado acercar el tema a la realidad práctica, incorporando ejemplos, propuestas y reflexiones personales sobre cómo podría avanzarse hacia una integración ética y segura de estas tecnologías. El objetivo no ha sido tanto demonizar estas herramientas como entender en qué condiciones podrían utilizarse de forma responsable y garantista.

A lo largo de sus distintos apartados, el trabajo aborda desde la definición y el funcionamiento técnico de estos sistemas hasta su regulación jurídica y las propuestas de mejora normativa, incluyendo un estudio práctico aplicado.

CAPÍTULO I: SISTEMAS DE RECONOCIMIENTO DE EMOCIONES EN EL ÁMBITO LABORAL

1. DEFINICIÓN Y FUNCIONAMIENTO DE ESTOS SISTEMAS

Los sistemas de reconocimiento de emociones son tecnologías basadas en inteligencia artificial que analizan señales biométricas, concepto que será analizado posteriormente en el trabajo, y de comportamiento para deducir el estado emocional de una persona. Utilizan datos como expresiones faciales, tono de voz, gestos, ritmo cardíaco o patrones de respiración para interpretar emociones como alegría, estrés, frustración o ansiedad. *"...incluso hay sistemas que pueden determinar emociones compuestas, por ejemplo, tristemente enojado o alegremente sorprendido".*[1] Incluyen señales como cambios en el rostro que llevan a intuir descontento o felicidad, variación en el habla, un movimiento corporal o la ausencia de este. Estos sistemas combinan sensores avanzados, algoritmos de aprendizaje automático y modelos de reconocimiento para procesar grandes volúmenes de información en tiempo real. *"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".*[2]

Como señala Muños Ruiz en su libro *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*,

> a diferencia de los controles tradicionales, los sistemas de reconocimiento de emociones emplean algoritmos e inteligencia artificial que, como se verá, incrementará la capacidad de análisis y explotación del resultado alcanzado. Lo que va a significar una mayor intromisión en los derechos fundamentales de las personas trabajadoras y producir lesiones indirectas de otros derechos fundamentales (la salud mental y su conexión con la seguridad y salud en el trabajo).[3]

---

[1] Ático, G. (2024, 28 noviembre). *Reconocimiento de emociones y protección de datos ¿Cómo se relacionan?* Grupo Atico34. https://protecciondatos-lopd.com/empresas/reconocimiento-emociones/

[2] Unión Europea. (2024). *Reglamento (UE) 2024/XX del Parlamento Europeo y del Consejo de 29 de abril de 2024 relativo a la inteligencia artificial y por el que se establecen disposiciones sobre transparencia, derechos fundamentales y supervisión.* Diario Oficial de la Unión Europea. Considerando 18.

[3] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch.

En términos operativos, su funcionamiento implica tres etapas principales. Primero, recogen datos mediante cámaras, micrófonos y *wearables* (dispositivos electrónicos que se llevan puestos, como relojes inteligentes) que registran expresiones faciales, tono de voz o movimientos. Después, la IA procesa esa información mediante algoritmos que identifican patrones emocionales como el estrés o la desmotivación. Por ejemplo, si alguien frunce el ceño y eleva la voz con frecuencia, el sistema puede detectar una situación de tensión. Finalmente, los resultados se traducen en acciones: alertas, informes o ajustes en el entorno laboral. Estas herramientas pueden ayudar a prevenir riesgos, mejorar el clima emocional o adaptar la carga de trabajo.[4]

2. EL VALOR ECONÓMICO DE LAS EMOCIONES EN LAS EMPRESAS

Las emociones desempeñan un papel crucial en la dinámica empresarial, no solo desde una perspectiva humana, sino también económica. Según lo analizado en *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*, las emociones de los trabajadores pueden influir directamente en la productividad, la innovación y la cohesión del equipo dentro de una organización. Este impacto convierte a las emociones en un activo intangible con un valor económico significativo para las empresas. Que justifica, por tanto, porque se querrían implementar sistemas de reconocimiento de emociones en el mundo corporativo.

2.1 Emociones positivas y su impacto en la productividad

Las emociones positivas, como la satisfacción, la motivación y el entusiasmo, están asociadas con mejoras en el rendimiento laboral. Estudios citados en el libro de Ana Belén Muñoz Ruiz ya mencionado, destacan que los trabajadores emocionalmente satisfechos tienden a ser más creativos y comprometidos, lo que repercute favorablemente en la consecución de los objetivos empresariales. Además, un ambiente emocionalmente saludable fomenta relaciones interpersonales más fuertes y una menor rotación de personal, lo que reduce los costos asociados al reclutamiento y la formación de nuevos empleados.

[4] Martín de Diego, I., Serrano, A., Conde, C., & Cabello, E. (2006). Definición y tipos de emociones. *Revista Electrónica Teoría de la Educación. Educación y Cultura en la Sociedad de la Información*, 7(2), 1–20. Disponible en: http://www.usal.es/teoriaeducacion

2.2 Emociones negativas y sus costes asociados

Por otro lado, las emociones negativas, como el estrés, la frustración o el agotamiento, representan riesgos significativos para las empresas. Estas emociones no solo disminuyen la productividad, sino que también pueden aumentar el absentismo, las bajas por enfermedad y las tasas de rotación laboral. En términos económicos, Ana Belén Muñoz Ruiz destaca que los costos derivados de la desmotivación y el desgaste emocional pueden ser considerables, afectando tanto al rendimiento individual como al colectivo.[5]

2.3 Gestión emocional a través de la inteligencia artificial

El uso de sistemas de reconocimiento de emociones en el ámbito laboral permite a las empresas identificar y gestionar las emociones de los trabajadores de manera más efectiva. Estos sistemas, al analizar señales biométricas como expresiones faciales o patrones de voz, pueden detectar indicadores tempranos de emociones negativas y activar medidas correctivas. Por ejemplo, al identificar niveles elevados de estrés en un equipo, las empresas pueden redistribuir las cargas de trabajo o implementar programas de bienestar emocional, minimizando así las pérdidas económicas derivadas de la desmotivación o el absentismo.[6]

2.4 Aplicaciones actuales en diferentes sectores

El uso de estos sistemas de inteligencia artificial es clave para una mejor comprensión de la persona trabajadora y de las necesidades que esta demanda pues se centra en movimientos oculares, gestos y tonos vocales. Entre sus posibles aplicaciones se encuentra la identificación de niveles de estrés en los trabajadores para implementar pausas adicionales o proporcionar apoyo psicológico. También puede asignar tareas según el estado emocional, asegurando que las actividades más críticas sean realizadas por quienes estén más motivados. Además, estas herramientas pueden prevenir el agotamiento laboral mediante la detección temprana de señales de fatiga, optimizar la integración de nuevos empleados ofreciendo mentorías o

[5] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch.
[6] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch.

formación específica, y mejorar la comunicación interna al identificar frustraciones o tensiones durante las interacciones.[7]

Otras ventajas incluyen la adaptación del entorno laboral ajustando condiciones como la iluminación o temperatura en función de las emociones detectadas, y la predicción de la satisfacción laboral para implementar estrategias que refuercen el compromiso de los trabajadores. De igual manera, estas tecnologías pueden ser útiles para desarrollar planes de carrera personalizados que se ajusten a las áreas donde el empleado se sienta más motivado. Sin embargo, el uso de estas herramientas plantea importantes retos éticos y legales, especialmente relacionados con la protección de la privacidad y el respeto a los derechos fundamentales de los trabajadores en el ámbito laboral.

Durante la investigación de este trabajo, se ha intentado recopilar ejemplos documentados sobre la implementación real de estas tecnologías. Sin embargo, la mayoría de las referencias encontradas no provienen de estudios académicos revisados, sino de fuentes periodísticas o institucionales. Se ha optado por incluirlas porque ilustran cómo estas tecnologías están siendo experimentadas en contextos reales, aunque muchas veces fuera del control normativo.

El Proyecto iBorderCtrl fue un programa piloto financiado por la Unión Europea (dentro de Horizonte 2020) con un consorcio de países participantes (entre ellos Luxemburgo, Chipre, Reino Unido, Polonia, España, Hungría, Alemania y Letonia)[8], destinado a reforzar el control fronterizo mediante inteligencia artificial. Utilizaba un sistema automatizado en el que un *avatar* virtual actuaba como agente fronterizo, interrogando a los viajeros mientras una IA analizaba sus expresiones faciales, microgestos y lenguaje corporal en busca de indicios de engaño[9], con el fin de evaluar la veracidad de sus declaraciones. Sin embargo, iBorderCtrl generó fuertes críticas éticas y legales debido a sus riesgos de discriminación (por posibles sesgos algorítmicos que podrían perjudicar a ciertos viajeros)[10], su baja fiabilidad técnica (en

---

[7] Business Insider España. (2018, 30 abril). *Así vigilan las empresas chinas las emociones de sus empleados con esta tecnología militar*. https://www.businessinsider.es/empresas-chinas-vigilan-emociones-empleados-tecnologia-militar-402197

[8] Barona. (2024). Título del artículo. *Actualidad Jurídica Iberoamericana*, *21*, 298-331.

[9] Morote. (2024). *Unión Europea: Robots con inteligencia artificial como agentes fronterizos*. Recuperado de https://tec.com.pe/union-europea-robots-inteligencia-artificial-agentes-fronterizos/#:~:text=Esta%20Inteligencia%20Artificial%20se%20encargar%C3%A1,como%20cualquier%20otro%20oficial%20humano

[10] iBorderCtrl. (2024). *iBorderCtrl automates discrimination*. Recuperado de https://iborderctrl.no/blog:iborderctrl_automates_discrimination#:~:text=fund%20iBorderCtrl%20to%20the%20tune,components%E2%80%94that%20make%20automated%20discrimination%20likely

pruebas iniciales solo alcanzó alrededor de un *76%* de acierto)[11]**,** y el temor de que su despliegue derivase en una forma de vigilancia masiva e indiscriminada de la población migrante**.**[12] Estas preocupaciones llevaron al Parlamento Europeo a pronunciarse en contra: en 2021 solicitó dejar de financiar este tipo de sistemas y expresó su inquietud general ante las tecnologías de reconocimiento facial y emocional, dado el potencial impacto negativo que tienen sobre derechos fundamentales.[13]

Ejemplos destacados incluyen el caso de empresas chinas que emplean sensores inalámbricos integrados en gorros para medir actividad cerebral y emociones como la ira, ansiedad o tristeza, en combinación con algoritmos de IA. Esta tecnología permite a los supervisores identificar cambios en los estados emocionales de los empleados, adaptando sus períodos de descanso o incluso interrumpiendo su actividad laboral cuando sea necesario.[14]

> Según el *South China Morning Post*, más de una docena de empresas y cuerpos del ejército en China han utilizado un programa desarrollado por *Neuro Cap*, un proyecto financiado por el gobierno chino y ubicado en la Universidad de Ningbo. Al respecto, Jin Jia, profesor de neurociencia en la Universidad de Ningbo, señaló: "Creían que podíamos leer sus mentes. Esto provocó alguna disconformidad y resistencia al principio, pero después de un tiempo se acostumbraron al dispositivo... Lo llevan todo el día en el trabajo".[15]

Ejemplo similar son las gafas inteligentes de Google que

> permiten encuadrar el rostro y junto a este superponen unas barras con indicadores de distintas emociones a través de la aplicación Shore que ha sido desarrollada en

---

[11]Morote. (2024). *Unión Europea: Robots con inteligencia artificial como agentes fronterizos*. Recuperado de https://tec.com.pe/union-europea-robots-inteligencia-artificial-agentes-fronterizos/#:~:text=Esta%20Inteligencia%20Artificial%20se%20encargar%C3%A1,como%20cualquier%20otro%20oficial%20humano

[12] Barona. (2024). Título del artículo. *Actualidad Jurídica Iberoamericana*, *21*, 298-331.

[13] Barona. (2024). Título del artículo. *Actualidad Jurídica Iberoamericana*, *21*, 298-331.

[14] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch.

[15] Business Insider España. (2018, 30 abril). *Así vigilan las empresas chinas las emociones de sus empleados con esta tecnología militar*. https://www.businessinsider.es/empresas-chinas-vigilan-emociones-empleados-tecnologia-militar-402197

Alemania. A lo que se suman las aplicaciones que analizan los tonos de voz en una conversación o el lenguaje utilizado en un correo electrónico.[16]

Además, estas herramientas pueden utilizarse en la prevención de riesgos laborales mediante sensores corporales que recogen datos sobre postura, cargas, tiempos y estado fisiológico (frecuencia cardíaca, temperatura corporal, etc.). Este tipo de soluciones han sido exploradas en iniciativas como el Proyecto Europeo H2020 Bionic, que busca integrar IA y nanotecnología en prendas de vestir para diagnosticar y prevenir el estrés físico de los trabajadores.[17]

CAPÍTULO II: RIESGOS INHERENTES EN EL USO DE SISTEMAS DE RECONOCIMIENTO DE EMOCIONES

El despliegue de sistemas de reconocimiento de emociones en el ámbito laboral plantea una serie de riesgos éticos y prácticos que no pueden ser ignorados. En primer lugar, la fiabilidad de estas tecnologías es cuestionable, ya que la interpretación emocional no siempre refleja un estado real de la persona. Como señala Muñoz Ruiz, los datos biométricos utilizados en el ámbito laboral, incluyendo expresiones faciales y patrones de voz, pueden ser objeto de interpretaciones erróneas debido a su alta dependencia del contexto y las características individuales.[18] Por ejemplo, una expresión facial que un sistema detecta como enojo podría deberse al cansancio o incluso a factores culturales, poniendo en riesgo decisiones laborales basadas en estas lecturas.

Además, el sesgo algorítmico y la discriminación constituyen uno de los mayores peligros asociados a estas tecnologías. Estudios recientes destacan cómo los algoritmos tienden a reflejar y amplificar sesgos preexistentes en los datos de entrenamiento.[19] Esto resulta particularmente problemático en entornos multiculturales, donde las expresiones emocionales pueden variar significativamente. La reciente sentencia del Tribunal General de la Unión

---

[16]El Foro de Labos. (2022, 4 mayo). *Derecho a la desconexión digital: Comentario a la STSJ de Madrid de 21-2-2022*. https://www.elforodelabos.es/2022/05/derecho-a-la-desconexion-digital-comentario-a-la-stsj-de-madrid-de-21-2-2022/

[17] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch.

[18] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch.pp. 80-85

[19] *Grupo Atico 34 (2023). "Reconocimiento de emociones: riesgos y normativa". Disponible en: https://protecciondatos-lopd.com/empresas/reconocimiento-emociones/.*

Europea (2023)[20] subraya la importancia de la transparencia en el desarrollo y uso de sistemas de reconocimiento de emociones, al destacar cómo la opacidad tecnológica puede amplificar riesgos éticos y jurídicos. La sentencia se refiere a una petición de transparencia hecha por un político sobre el uso de tecnología de reconocimiento de emociones que se probó en el proyecto iBorderCtrl. Como se ha relatado antes en este documento, el proyecto prueba un sistema de inteligencia artificial capaz de analizar microexpresiones faciales para detectar posibles mentiras durante controles fronterizos. A partir del reconocimiento de hasta 38 gestos faciales, el software decide si la persona recibe un código QR para cruzar la frontera o si, por el contrario, debe someterse a una revisión adicional por parte de un agente. En el caso del proyecto iBorderCtrl, se debatió la tensión entre el interés público de saber si estos sistemas eran fiables y éticamente aceptables y la protección de los intereses comerciales del consorcio desarrollador. El fallo diferenció entre la obligación de transparencia en las evaluaciones éticas y jurídicas, y la confidencialidad del desarrollo tecnológico, priorizando esta última. Esto refleja un desafío crítico para la regulación de estos sistemas en el ámbito laboral, donde la falta de fiabilidad y los sesgos algorítmicos podrían generar decisiones discriminatorias y vulnerar derechos fundamentales, como el acceso a promociones o la estabilidad en el empleo.[21]

Siguiendo por esta línea, *"Si estos datos contienen discriminaciones, el algoritmo aprende a discriminar"*[22], señala Ginès i Fabrellas (2022), citando el caso de Amazon, que entrenó un algoritmo de selección de personas que finalmente descartó. Estos sesgos pueden conducir a interpretaciones erróneas y decisiones discriminatorias, especialmente cuando los datos de entrenamiento no representan adecuadamente la diversidad cultural. Por ejemplo, las expresiones faciales de emociones varían considerablemente entre culturas; una sonrisa puede indicar felicidad en una cultura y nerviosismo en otra, lo que complica la precisión de los sistemas de reconocimiento facial. Además, la falta de diversidad en los conjuntos de datos puede perpetuar estereotipos y amplificar desigualdades existentes. Un estudio reciente destaca que los modelos de IA entrenados sin considerar estas variaciones culturales tienden a fallar en

---

[20] Tribunal de Justicia de la Unión Europea (TJUE). (2023). *Sentencia de 30 de marzo de 2023, F.F. contra Data Protection Commissioner, C-34/21, EU:C:2023:250*.

[21] El Foro de Labos (2023). "No digas ni mu: el Tribunal de la UE deniega la transparencia del reconocimiento de emociones". Disponible en: https://www.elforodelabos.es/2023/09/no-digas-ni-mu-el-tribunal-de-la-ue-deniega-la-transparencia-del-reconocimiento-de-emociones/.

[22] *Esade (2023). ¿Cómo pueden los algoritmos perpetuar la discriminación en el trabajo?. Recuperado de https://dobetter.esade.edu/es/algoritmos-discriminacion-trabajo*

contextos multiculturales, subrayando la necesidad de desarrollar sistemas más inclusivos y equitativos.[23] El Dictamen Conjunto del CEPD y el SEPD de 2021 subrayaba la importancia de realizar evaluaciones de impacto que consideren no solo los sesgos potenciales, sino también los efectos desproporcionados sobre grupos vulnerables, proponiendo mecanismos para identificar y mitigar estas problemáticas antes de implementar sistemas de IA.

Otro aspecto crítico es el impacto en la privacidad de los trabajadores. El procesamiento de datos biométricos sensibles, como las expresiones faciales o la tonalidad de la voz, requiere un consentimiento claro y explícito, tal como establece el RGPD en sus artículos 15 a 22.[24] Normativa que será objeto de análisis más adelante. Sin embargo, en el ámbito laboral, el desequilibrio de poder entre empleadores y empleados puede poner en entredicho la validez de dicho consentimiento. Según la empresa Grupo Ático34, es necesario implementar estrictas medidas de proporcionalidad para garantizar que el uso de estas tecnologías no exceda su finalidad declarada.[25]

Adicionalmente, es importante destacar el desafío de la transparencia. La Guía sobre la Protección de Datos en las Relaciones Laborales de la Agencia Estatal de Protección de Datos (AEPD) (2021) subraya que los empleados deben ser informados de manera clara sobre cómo y por qué se utilizan estas tecnologías.[26] No obstante, según El Foro de Labos (2023), muchas empresas aún carecen de políticas claras que permitan a los empleados entender cómo se procesan sus datos y cómo pueden ejercer sus derechos.[27]

Estos riesgos exigen un marco normativo más robusto que aborde no solo la fiabilidad y la precisión técnica de los sistemas, sino también las implicaciones éticas y sociales de su implementación en el entorno laboral. Sin un enfoque integral, estas tecnologías podrían minar

---

[23] Chen, J., Yan, M., Zhao, J., & Wang, Y. (2023). *Ethical Challenges of AI Bias in Workforce Management*. arXiv preprint. Recuperado de https://arxiv.org/abs/2309.10780

[24] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch. p 83.

[25] Grupo Ático34. (s.f.). *Principio de proporcionalidad en protección de datos*. Protección de Datos LOPD. https://protecciondatos-lopd.com/empresas/principio-proporcionalidad/

[26] Agencia Española de Protección de Datos (AEPD). (2021). *Guía sobre la protección de datos en las relaciones laborales*. https://www.aepd.es/sites/default/files/2021-10/guia-proteccion-datos-relaciones-laborales.pdf

[27] El Foro de Labos (2023). "No digas ni mu: el Tribunal de la UE deniega la transparencia del reconocimiento de emociones". Disponible en: https://www.elforodelabos.es/2023/09/no-digas-ni-mu-el-tribunal-de-la-ue-deniega-la-transparencia-del-reconocimiento-de-emociones/.

derechos fundamentales y perpetuar desigualdades, en lugar de contribuir a un entorno laboral más justo y eficiente.

CAPÍTULO III: EL REGLAMENTO DE IA DE 2024: ANÁLISIS DE LAS EXCEPCIONES

El RIA es la primera norma que vamos a abordar pues es aquella normativa europea en la que se definen estos sistemas por primera vez, implementa la novedad de incluir las emociones y su posible monitorización. Es esta norma la que más claridad aporta sobre su marco jurídico completo pues es aquella que los trata propiamente.

A pesar de que el RGPD, que será analizado con posterioridad, regula el tratamiento de los datos biométricos, parte indispensable para procesar las emociones*, "Cuando el reglamento fue redactado no se tenía en mente que las emociones llegarían a ser monitorizadas, por lo que tiene sentido que ahora experimentemos cierta dificultad para encajar el supuesto en la norma"*[28]

A lo largo de este capítulo y posteriormente en el documento se habla de conceptos procedentes del RIA como **proveedor**, aquel que desarrolla el sistema, y **responsable del despliegue**, quien lo utiliza en su empresa.

1. TRATO QUE RECIBEN LOS SISTEMAS DE RECONOCIMIENTO DE EMOCIONES EN EL RIA

El RIA clasifica los sistemas de reconocimiento de emociones dentro de los niveles de riesgo más altos debido a su potencial impacto en los derechos fundamentales. En concreto, el artículo 5.1(f) prohíbe su uso en el ámbito laboral cuando estos sistemas se emplean para actividades como la contratación, selección de personal, supervisión, evaluación de rendimiento o asignación de tareas. Estas tecnologías se consideran de nivel de riesgo 1: inaceptable porque pueden perpetuar patrones de discriminación, afectar las perspectivas laborales y vulnerar

28 Maldita.es. (9 de abril de 2024). *¿Son nuestras emociones datos personales? Qué dice la ley de protección de datos sobre el reconocimiento de emociones y el análisis de sentimientos con IA.* Maldita Tecnología. Recuperado de https://maldita.es/malditatecnologia/20240409/emociones-datos-personales-protegidos/

derechos como la privacidad y la protección de datos personales.[29] A pesar de esta categorización restrictiva, el reglamento reconoce su utilidad en contextos muy específicos y bajo estrictas condiciones.

El artículo 5.1(f) prohíbe explícitamente el uso de estos sistemas en contextos laborales cuando pueden afectar a las perspectivas laborales, a los medios de subsistencia de dichas personas y a los derechos fundamentales de los trabajadores.

Aunque el texto del RIA no detalla una lista exhaustiva de actividades prohibidas, los considerandos y artículos relacionados permiten inferir varias áreas clave en las que su uso es particularmente problemático.

Como sistemas de alto riesgo, el Capitulo III en su sección segunda establece los requisitos

básicos que deben cumplirse cuando se implementan estos sistemas. La mayoría de obligaciones recaen sobre los proveedores que han de

> establecer un sistema de gestión de riesgos; (ii) garantizar la calidad de los datos de entrenamiento, validación y prueba estableciendo prácticas adecuadas de gobernanza y gestión de los mismos; (iii) desarrollar documentación técnica del producto con un contenido específico; (iv) establecer medidas de supervisión humana en los sistemas que desarrollen proporcionales a los riesgos; (v) garantizar que los sistemas funcionen con un nivel de transparencia adecuado y (vi) disponer de disponer de un sistema de gestión de la calidad que garantice el cumplimiento del reglamento.[30]

Entre otros requisitos incluidos en esta sección.

Los responsables del despliegue tienen a su vez una serie de exigencias recogidas en el artículo 26 y que quedan bien reflejadas en el anexo de este trabajo con el estudio del caso práctico.

---

[29] Unión Europea. (2024). *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 se modifican determinados actos legislativos de la Unión*. Diario Oficial de la Unión Europea, L, 168/1, art. 5.1(f). Disponible en: https://data.consilium.europa.eu/doc/document/PE-48-2024-INIT/en/pdf

[30] Mariscal & Abogados. (n.d.). *Códigos de conducta empresariales*. Recuperado de https://www.mariscal-abogados.es/codigos-de-conducta-empresariales

2. PROHIBICIONES GENERALES Y EXCEPCIONES PERMITIDAS

El RIA establece una prohibición general para el uso de sistemas de reconocimiento de emociones en el ámbito laboral, en particular cuando estos sistemas puedan comprometer los derechos fundamentales de los trabajadores, como la privacidad, la protección de datos personales o la dignidad. Esta prohibición, regulada en el artículo 5.1(f), considera que estas tecnologías presentan un nivel de riesgo inaceptable. Sin embargo, el reglamento introduce excepciones limitadas bajo estrictas condiciones, en dos escenarios específicos: motivos médicos y motivos de seguridad.

- **Motivos Médicos:**

  Estos sistemas pueden utilizarse para prevenir riesgos laborales y proteger la salud de los trabajadores. Por ejemplo, la identificación de estrés en empleados como parte de programas de bienestar laboral.[31]

  A pesar de que los sistemas diseñados para identificar señales de cansancio en conductores, como parpadeos lentos o cabeceos, son cruciales para prevenir accidentes, el RIA no los clasifica como sistemas de reconocimiento de emociones. Según el reglamento, estos sistemas no deducen emociones o intenciones, sino que monitorean estados físicos, como el cansancio, quedando fuera del ámbito del reconocimiento de emociones.[32]

  A diferencia de la detección de fatiga, los sistemas que identifican estados emocionales como estrés o ansiedad a partir de datos biométricos sí entran dentro de la definición del reglamento. Por ejemplo, en entornos corporativos, se podrían emplear tecnologías para analizar expresiones faciales o tonos vocales durante reuniones virtuales, identificando indicadores emocionales como frustración o desmotivación. Estas tecnologías, cuando buscan deducir emociones específicas, son consideradas de alto riesgo y están sujetas a estrictas regulaciones.

---

[31] Unión Europea. (2024). *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 se modifican determinados actos legislativos de la Unión*. Diario Oficial de la Unión Europea, L, 168/1, Considerado 18. Disponible en: https://data.consilium.europa.eu/doc/document/PE-48-2024-INIT/en/pdf

[32] Unión Europea. (2024). *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 se modifican determinados actos legislativos de la Unión*. Diario Oficial de la Unión Europea, L, 168/1, Considerado 18. Disponible en: https://data.consilium.europa.eu/doc/document/PE-48-2024-INIT/en/pdf

Al detectar estos patrones, el sistema podría sugerir automáticamente intervenciones como establecer reuniones más cortas, ajustar cargas de trabajo o proponer sesiones de coaching personal. Estas iniciativas no solo buscan mejorar la salud mental de los empleados, sino también optimizar su rendimiento mediante la reducción del estrés acumulado.

Un ejemplo real de la aplicación de inteligencia artificial para monitorear el estrés laboral es la plataforma ifeel. Esta herramienta utiliza IA para evaluar el clima laboral y las necesidades emocionales de los empleados. Analiza datos proporcionados por los trabajadores para identificar signos de estrés, ansiedad o desmotivación, ofreciendo recomendaciones personalizadas y, si es necesario, acceso a terapia en línea con psicólogos colegiados. Además, proporciona a los departamentos de recursos humanos informes agregados y anónimos sobre el estado emocional de sus equipos, permitiendo intervenciones proactivas para mejorar el bienestar en el entorno laboral.[33]

Otro caso es el de Mia Meraki, que ofrece soluciones basadas en IA para mejorar la salud mental en el trabajo. Su plataforma analiza patrones de comportamiento para detectar signos tempranos de agotamiento, ansiedad o desmotivación en los empleados. Al identificar estos indicadores, la herramienta sugiere intervenciones personalizadas, como ejercicios de relajación o ajustes en la carga de trabajo, contribuyendo a crear un entorno laboral más saludable y productivo.[34]

Estas iniciativas reflejan cómo la inteligencia artificial se está integrando en el ámbito laboral para promover el bienestar emocional de los empleados, permitiendo a las empresas adoptar medidas preventivas y de apoyo basadas en datos objetivos. A pesar de no tratarse estos ejemplos mencionados de sistemas de reconocimiento de emociones por no hacer uso de datos biométricos, se encuentran en un escalón muy cercano en cuanto a funcionamiento y capacidades. Sin duda ilustran la cabida que podrían tener estos sistemas en el mundo laboral, su forma de uso y propósito.

- **Motivos de Seguridad:**

  El RIA también permite el uso de sistemas de reconocimiento de emociones en entornos

---

[33] RRHH Press. (2019). *Ifeel lanza una herramienta basada en inteligencia artificial para medir el clima laboral*. Recuperado de https://www.rrhhpress.com/zona-tech/47593-ifeel-lanza-una-herramienta-basada-en-inteligencia-artificial-para-medir-el-clima-laboral?utm_source=chatgpt.com

[34] Mia Meraki. (n.d.). *Entorno laboral y salud mental: Soluciones de IA*. Recuperado de https://miameraki.com/blog/entorno-laboral-y-salud-mental-soluciones-de-ia/?utm_source=chatgpt.com

donde la seguridad es prioritaria, siempre que su aplicación esté destinada a prevenir incidentes graves o proteger la integridad física de las personas involucradas. Estos casos suelen implicar lugares de trabajo de alto riesgo, como cárceles, plantas industriales o zonas de conflicto. Ejemplos incluyen cámaras con IA para analizar comportamientos en cárceles o herramientas que detecten distracciones en operadores de maquinaria pesada.[35]

En sectores como la minería o la construcción, los sistemas de IA pueden identificar distracciones o estados emocionales que comprometan la atención de los operadores de maquinaria pesada. Los operadores de grúas y excavadoras manejan equipos de gran tamaño con alta probabilidad de accidentes si están distraídos o emocionalmente alterados. Un sistema de reconocimiento de emociones podría identificar frustración o distracción en el operador mediante el análisis de expresiones faciales o posturas. Esto permitiría activar un protocolo de descanso obligatorio o reasignar la tarea a otro operador, asegurando un entorno más seguro.

En instalaciones donde los errores humanos tienen consecuencias graves, como plantas químicas o nucleares, estas tecnologías pueden detectar señales de ansiedad o nerviosismo en los trabajadores. Esto permite intervenir rápidamente para evitar situaciones de riesgo. Por ejemplo, si un trabajador muestra señales de estrés extremo mientras realiza el mantenimiento de una válvula de presión, el sistema podría alertar al supervisor para evaluar la situación y garantizar la seguridad del empleado y del entorno.

Un posible uso de los sistemas de reconocimiento de emociones en el ámbito de la conducción profesional, diferente al enfoque previo sobre la detección de cansancio, podría ser su implementación en vehículos de transporte público, como taxis. Estos sistemas tendrían la capacidad de monitorizar al conductor y detectar emociones como el miedo, que podría surgir ante un posible intento de atraco, o la ira, que podría afectar la capacidad de toma de decisiones durante la conducción. Asimismo, podrían identificar signos asociados a estados de embriaguez, lo que permitiría intervenir de manera inmediata para garantizar la seguridad tanto del conductor como de los pasajeros.

[35] El Periódico. *"Cárceles de Cataluña: Inteligencia Artificial para el control de presos." 20 de septiembre de 2023.*

> Cuando el sistema detecte indicadores emocionales o físicos que puedan poner en riesgo la seguridad, podrían activarse diversas acciones automáticas, como notificar a un centro de control, enviar alertas a las autoridades locales, o incluso detener el vehículo de forma segura. Por ejemplo, si un taxista mostrara signos de miedo extremo durante un intento de robo, el sistema podría activar una alarma silenciosa conectada a una central de seguridad, permitiendo una respuesta rápida por parte de las autoridades. Del mismo modo, la detección de ira descontrolada o embriaguez podría desencadenar recomendaciones para cesar la actividad temporalmente o redirigir el vehículo a un punto seguro.
>
> Por ejemplo, en grandes ciudades con altos índices de criminalidad, como algunas áreas metropolitanas de América Latina, estos sistemas podrían integrarse en flotas de taxis para prevenir incidentes, protegiendo tanto a los conductores como a los pasajeros. Este enfoque demuestra cómo los sistemas de reconocimiento de emociones pueden utilizarse de forma responsable en el ámbito laboral, respetando los derechos fundamentales y mejorando la seguridad operativa.
>
> En todos los casos, se exige transparencia y supervisión humana para minimizar riesgos y garantizar la protección de los derechos de los empleados.[36]

Como se establece en el Considerado 54 del RIA, cuando estos sistemas de reconocimiento de emociones no estén prohibidos por estar justificados por estos motivos médicos o de seguridad, estarán en el nivel de riesgo 2. De hecho, en el Anexo III del RIA donde se enumeran los sistemas de IA de alto riesgo aparecen los sistemas de IA destinados a ser utilizados para el reconocimiento de emociones:

> además, deben clasificarse como de alto riesgo los sistemas de IA destinados a ser utilizados para la categorización biométrica conforme a atributos o características sensibles protegidos en virtud del artículo 9, apartado 1, del reglamento (UE) 2016/679 sobre la base de datos biométricos, **en la medida en que no estén prohibidos** en virtud

[36] Unión Europea. (2024). *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 se modifican determinados actos legislativos de la Unión*. Diario Oficial de la Unión Europea, L, 168/1, Art 26.2 y 26.7. Disponible en: https://data.consilium.europa.eu/doc/document/PE-48-2024-INIT/en/pdf

del presente reglamento, así como los sistemas de reconocimiento de emociones que no estén prohibidos con arreglo al presente reglamento.[37]

Existen escenarios en los que los sistemas de reconocimiento de emociones podrían clasificarse dentro del nivel de riesgo 3 (riesgo limitado), particularmente si no se basan en el uso de datos biométricos de los trabajadores. El artículo 50 del RIA aborda sistemas de IA diseñados para interactuar con personas físicas, como los chatbots o robots de software. En casos donde estos sistemas se limitan al uso de lenguaje escrito para deducir emociones o intenciones, se considera que caen bajo las regulaciones menos estrictas del nivel 3, aplicándose las obligaciones de transparencia mencionadas en el artículo 50.[38]

Sin embargo, si el chatbot también procesa la voz del trabajador, un dato biométrico, la clasificación del sistema cambiaría a niveles de riesgo más elevados, como el nivel 1 o 2, dependiendo de las características específicas del sistema y su uso en el entorno laboral. Este cambio se debe a la mayor sensibilidad de los datos biométricos y los riesgos asociados a su procesamiento.[39]

3. PROHIBICIONES EXPLÍCITAS

El artículo 5.1(f) prohíbe los sistemas de IA que se utilizan en los ámbitos del empleo, la gestión de los trabajadores y el acceso al autoempleo, en particular para la contratación y la selección de personal, para la toma de decisiones que afecten a las condiciones de las relaciones de índole laboral. Esto incluye también sistemas utilizados para la supervisión o evaluación de los trabajadores, ya que estas prácticas pueden tener un impacto significativo en sus perspectivas laborales y en la dignidad del trabajo.[40]

---

[37] Unión Europea. (2024). *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 se modifican determinados actos legislativos de la Unión*. Diario Oficial de la Unión Europea, L, 168/1. Disponible en: https://data.consilium.europa.eu/doc/document/PE-48-2024-INIT/en/pdf

[38] Muñoz Ruiz, A. B. (2024, enero 22). *Los sistemas automatizados de reconocimiento de emociones en el Reglamento UE de IA*. Observatorio de Recursos Humanos. https://www.observatoriorh.com/opinion/los-sistemas-automatizados-de-reconocimiento-de-emociones-en-el-reglamento-ue-de-ia.html

[39] Muñoz Ruiz, A. B. (2024, enero 22). *Los sistemas automatizados de reconocimiento de emociones en el Reglamento UE de IA*. Observatorio de Recursos Humanos. https://www.observatoriorh.com/opinion/los-sistemas-automatizados-de-reconocimiento-de-emociones-en-el-reglamento-ue-de-ia.html

[40] Unión Europea. (2024). *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 se modifican determinados actos legislativos de la Unión*. Diario Oficial de la Unión Europea, L, 168/1, art. 5.1(f). Disponible en: https://data.consilium.europa.eu/doc/document/PE-48-2024-INIT/en/pdf

El Considerando 57 del RIA subraya que estos sistemas *"pueden perpetuar patrones históricos de discriminación, como contra mujeres, determinados grupos de edad, personas con discapacidad, u otros colectivos vulnerables"*. También destaca que *"los sistemas empleados para monitorear el rendimiento y el comportamiento de las personas trabajadoras pueden socavar sus derechos fundamentales a la privacidad y la protección de datos personales"*.

Como se establece en el Anexo III del RIA se incluyen como sistemas de alto riesgo aquellos que están destinados a ser utilizados para contratación, selección de personal, supervisión, evaluación de rendimiento y asignación de tareas. Actividades abordadas a su vez en informes complementarios como el Dictamen conjunto del Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD) (2021).[41]

- **Contratación y selección de personal**:
  Estas actividades han sido objeto de análisis en múltiples estudios, que advierten que los sistemas de IA pueden perpetuar sesgos históricos presentes en los datos con los que fueron entrenados. Por ejemplo, el CEPD-SEPD (2021) considera que el uso de IA para evaluar características emocionales durante entrevistas puede discriminar a personas por su tono de voz o expresiones faciales, afectando especialmente a mujeres o minorías étnicas.

- **Supervisión y evaluación del rendimiento**:

  El uso de tecnologías que monitorean emociones en tiempo real durante la jornada laboral podría generar un ambiente de vigilancia constante, afectando la dignidad y privacidad de las personas trabajadoras. Estas preocupaciones han sido abordadas en documentos como el Informe de Impacto de la IA en el Trabajo de *The European Agency for Safety and Health at Work (*OSHA-EU) (2021), [42] que resalta los riesgos de estrés y ansiedad derivados de entornos laborales excesivamente controlados.

- **Asignación de tareas y decisiones laborales automatizadas**:
  El Considerando 54 del RIA plantea una base para reflexionar sobre cómo los sistemas de reconocimiento de emociones utilizados para categorizar o clasificar a trabajadores en función de sus estados emocionales podrían influir negativamente en la asignación de

[41] CEPD-SEPD. *Dictamen conjunto 5/2021 sobre Ley de Inteligencia Artificial,* 18 de junio de 2021.
[42] OSHA-EU. *Impact of Artificial Intelligence on Occupational Safety and Health,* 2021.

responsabilidades, perpetuando desigualdades estructurales. Esta práctica no solo vulnera derechos laborales, sino que también podría afectar la igualdad de oportunidades.[43]

4. ANÁLISIS DE LAGUNAS Y ÁREAS POCO DEFINIDAS EN EL RIA

Una vez visto donde se sitúan los sistemas de reconocimiento de emociones en el RIA, su definición como sistemas de alto riesgo, su prohibición casi completa en el ámbito laboral y sus pequeñas burbujas de actuación bajo motivos médicos o de seguridad, se analizarán ciertos aspectos sin abordar con claridad, que pueden llegar a generar incertidumbre sobre su implementación:

4.1 Ambigüedad en la delimitación de las excepciones

Aunque se mencionan motivos médicos y de seguridad, no se especifica con detalle cómo deben aplicarse estas categorías ni cómo se garantiza su proporcionalidad en entornos laborales. Aunque se menciona que estos sistemas pueden ser utilizados para proteger la salud de los trabajadores, como en la detección de estrés, no se establece cómo medir la proporcionalidad de su implementación. ¿Qué niveles de estrés justificarían su uso? ¿Qué tipo de intervenciones serían aceptables? Estas preguntas quedan abiertas, dejando margen para interpretaciones dispares en distintos sectores.

En lo que respecta a cuando estos sistemas se fundamenten en motivos de seguridad, los casos aceptados, como el análisis de comportamientos en entornos de alto riesgo, tampoco están claramente definidos. ¿Qué constituye un "incidente grave" suficiente para justificar el uso de estos sistemas? Además, no se abordan las posibles repercusiones sobre la privacidad de los trabajadores en entornos donde la vigilancia es constante.

Desde mi punto de vista, la inclusión de ejemplos prácticos y criterios de evaluación específicos, como un listado de indicadores emocionales relevantes (frustración, desánimo, satisfacción…) o protocolos para validar su uso (fase previa, fase de uso, evaluación…) , podría reducir esta ambigüedad.

---

[43] Unión Europea. (2024). *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 se modifican determinados actos legislativos de la Unión*. Diario Oficial de la Unión Europea, L, 168/1, Considerado 54. Disponible en: https://data.consilium.europa.eu/doc/document/PE-48-2024-INIT/en/pdf

4.2 Falta de orientación sobre supervisión y evaluación: Un análisis del artículo 26

- **La Supervisión Humana**

El artículo 26 del Reglamento Europeo de IA de 2024 establece un marco claro y ambicioso para regular el despliegue de sistemas de IA de alto riesgo. Este enfoque demuestra un compromiso con la seguridad, la transparencia y la supervisión humana en el uso de tecnologías avanzadas, especialmente en entornos laborales. Sin embargo, el análisis del artículo también pone de manifiesto ciertos aspectos que podrían fortalecerse para maximizar su efectividad.

El reglamento hace un profundo énfasis en la obligatoriedad de la supervisión humana. La obligación de contar con personas físicas competentes y formadas para supervisar los sistemas de IA (artículo 26.2 RIA) refuerza el papel de los humanos en el control de decisiones automatizadas. Esto asegura que la tecnología no opere de manera independiente en escenarios críticos, lo que protege los derechos fundamentales de las personas trabajadoras.

Aunque el reglamento exige supervisión humana, no detalla las competencias específicas ni los criterios para definir quiénes deben ocupar este rol. Por ejemplo, en un contexto laboral, podría ser crucial especificar si los supervisores deben contar con conocimientos en ética algorítmica o en la interpretación de datos biométricos.

> El modelo regulatorio por el que ha optado la Comisión responsabiliza a los proveedores de los sistemas del cumplimiento de los requisitos obligatorios como la supervisión humana, poniendo definitivamente el enfoque normativo sobre las fases de diseño y desarrollo de estas tecnologías que habían permanecido fuera del análisis doctrinal jurídico y de las iniciativas políticas.[44]

Pues son los proveedores quienes deben definir las medidas adecuadas de supervisión humana antes de su introducción en el mercado o puesta en servicio.[45]

---

[44] Ohm, P., & Lehr, D. (2017). *Playing with the Data: What Legal Scholars Should Learn about Machine Learning.* UC Davis Law Review, 51(2), 655 y ss. Recuperado de UC Davis Law Review pp. 231-232

[45] Unión Europea. (2024). *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 se modifican determinados actos legislativos de la Unión*. Diario Oficial de la Unión Europea, L, 168/1, Art 13.2 d). Disponible en: https://data.consilium.europa.eu/doc/document/PE-48-2024-INIT/en/pdf

Como expresan Obregón Fernández y Lazcoz Moratinos,[46] señala que la introducción de un operador humano en la toma de decisiones automatizadas preserva la dignidad humana y contrarrestar la deshumanización inherente a los sistemas totalmente automatizados. Este *human in the loop* actúa como un contrapeso necesario para evitar el impacto negativo de decisiones automatizadas exclusivas.

Los mecanismos de gobernanza basados en la supervisión humana reflejan una cultura jurídica europea que prioriza la dignidad y los derechos de los individuos sobre la automatización total.[47] Este modelo normativo contrasta con enfoques norteamericanos más permisivos, destacándose el papel crucial del operador humano como elemento protector frente a posibles vulneraciones de derechos fundamentales, tales como la privacidad y la no discriminación.[48]

La supervisión humana no es un concepto nuevo en el ámbito normativo europeo. Por ejemplo, la Directiva (UE) 2016/680 establece el derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de datos, una disposición que se alinea con el enfoque del RIA. Según el Comité Europeo de Protección de Datos, la supervisión debe ser significativa y llevada a cabo por personas autorizadas, capacitadas y competentes para analizar los datos pertinentes.[49]

A pesar de los avances, los autores subrayan que los mecanismos de supervisión humana establecidos en la normativa europea actual son insuficientes en términos legislativos y aplicativos. Obregón Fernández y Lazcoz Moratinos (2024) argumentan que, aunque se reconoce la importancia de la supervisión humana, su regulación específica sigue siendo limitada, dejando espacio para interpretaciones divergentes que pueden comprometer la efectividad de estas disposiciones en la práctica.

- **Incidentes graves**

---

[46] Ohm, P., & Lehr, D. (2017). *Playing with the Data: What Legal Scholars Should Learn about Machine Learning.* UC Davis Law Review, 51(2), 655 y ss. Recuperado de UC Davis Law Review.pp. 231-232
[47] Obregón Fernández, A., & Lazcoz Moratinos, G. (2024). *La supervisión humana de los sistemas de inteligencia artificial de alto riesgo. Aportaciones desde el derecho internacional humanitario y el derecho de la Unión Europea. Dialnet.*
[48] Sheridan. (1995). *Human-Centered Automation: Oxymoron or Common Sense?.* IEEE International Conference on Systems, Man and Cybernetics, pp. 823–828. https://doi.org/10.1109/ICSMC.1995.537867
[49] Obregón Fernández, A., & Lazcoz Moratinos, G. (2024). *La supervisión humana de los sistemas de inteligencia artificial de alto riesgo. Aportaciones desde el derecho internacional humanitario y el derecho de la Unión Europea.* Dialnet. pp 12-13.

El artículo 26.5 RIA establece mecanismos claros para monitorear los sistemas y actuar en caso de detectar incidentes graves, lo que refleja un enfoque preventivo hacia posibles problemas técnicos o éticos. Este requisito es particularmente relevante en sectores sensibles como la salud, la seguridad o la gestión de datos personales.

El artículo menciona la obligación de informar sobre incidentes graves. La definición de "incidente grave" recogida en el Reglamento de Inteligencia Artificial, que abarca desde daños a la salud hasta perjuicios graves al medio ambiente, propiedad, infraestructuras críticas o a derechos fundamentales, presenta importantes lagunas cuando se analiza desde la perspectiva del entorno laboral. Aunque incluye el incumplimiento de obligaciones vinculadas a los derechos fundamentales, omite toda referencia específica a contextos como el trabajo, donde el uso de sistemas de reconocimiento de emociones puede tener impactos severos sin que exista un daño físico inmediato. Un sistema de IA que discrimina sistemáticamente a mujeres embarazadas al asignarles menos turnos o tareas menos cualificadas podría tener efectos graves sobre sus medios de subsistencia, sin que ello encaje claramente en ninguna de las letras a-d.

Además, la ambigüedad de términos como "grave", "irreversible" o "indirectamente" dificulta una aplicación homogénea y genera incertidumbre sobre cuándo debe considerarse activado este umbral.

También se excluyen expresamente los daños psicosociales o emocionales, a pesar de que estas herramientas pueden generar ansiedad o sensación de vigilancia constante en entornos como el teletrabajo o la atención al cliente. Igualmente, no se contemplan situaciones de riesgo inminente que aún no se han materializado: por ejemplo, un algoritmo que empieza a sesgar decisiones en función del género o la edad no tendría por qué ser reportado como incidente grave hasta que el perjuicio sea plenamente visible. Esta visión limitada deja fuera muchos escenarios donde los sistemas de IA pueden vulnerar derechos laborales de forma significativa, pero no entran técnicamente dentro del concepto de incidente grave tal y como está redactado.

- **Transparencia laboral**

EL RIA establece una serie de requisitos de transparencia desde fases previas a la introducción en el mercado o puesta en servicio. Debe asegurarse que los responsables del despliegue

entienden su funcionamiento, evalúan su funcionalidad y comprenden sus fortalezas y limitaciones.[50]

Sin embargo, al estudiar las áreas poco definidas en el reglamento, nos interesa ver como los responsables del despliegue se comunican con los trabajadores. Aunque el artículo 26.7 garantiza el derecho a la información, no especifica qué contenido debe incluirse en estas comunicaciones. La obligación de transparencia establecida en el artículo 26.7 del Reglamento de IA busca proteger a las personas trabajadoras mediante una comunicación abierta sobre los sistemas de IA implementados en el ámbito laboral. Sin embargo, esta disposición carece de precisión sobre los contenidos específicos que deben incluir estas comunicaciones. Según Muñoz Ruiz (2022), la información debe abarcar desde los algoritmos y datos utilizados hasta las medidas de supervisión humana y los impactos potenciales sobre los derechos laborales, siempre presentada de forma clara y comprensible.[51] El tema de los convenios colectivos se estudia más adelante en este trabajo, se incluye esté a continuación para ejemplificar como se aborda los requisitos de transparencia en la práctica. El convenio colectivo de Just Eat con los sindicatos CCOO y UGT destacan la creación de comisiones específicas, como la Comisión Algoritmo, para supervisar el uso de sistemas de IA, garantizando la participación activa de los representantes de los trabajadores y reforzando la confianza en estas tecnologías.[52]

Además, el nuevo artículo 2 bis del Real Decreto 1659/1998 por el que se desarrolla el artículo 8, apartado 5, de la Ley del Estatuto de los Trabajadores amplía las obligaciones del empleador, exigiendo que se detalle la lógica de los algoritmos, los parámetros utilizados y las medidas de corrección adoptadas, con el fin de evitar riesgos como la discriminación o la opacidad en la toma de decisiones automatizadas.[53] Estas propuestas no sólo fortalecen el derecho a la

---

[50] Diario La Ley. (2024). La transparencia en el desarrollo de la IA, ¿cuál es el enfoque del reglamento europeo? Recuperado de https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAAEADVPwU7DMAz9m1yQUNiQEAdfunGYhCY0Ku5uarWWsrg4Tln-nmyDg_X87Gc_-7uQ1p4uBhyZ9CHhiqrick2S6hl6LeQMhwzbZ4fBCsa9BHi65rxSj8O1ITqSdhW8MzGMJ8rwsnV5lp8jrjyhsaQO9b6NxxGOb977zca_NnAraW4C-OKJkpGbeZrfW9hdnwk1zB84ERwSB5ZHzMvlr9wVszY6WPq8cRdiwz0a7TBSGv9NcVliPUlsl934Irn9Uc7N8JB2qFIyRfC_PqN3SQ8BAAA=WKE

[51] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch. pp. 168-174.

[52] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch. p. 178.

[53] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch. pp. 179-180.

información, sino que promueven una integración ética y transparente de la IA en el ámbito laboral.

CAPÍTULO IV: EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

Una vez hecho el análisis del RIA, la norma principal que trata los sistemas de reconocimiento de emociones y por tanto las emociones de las personas trabajadoras, no se puede pasar por alto el análisis del RGPD. Una norma que lleva muchos más años regulando los datos de carácter personal y que además ha sido adaptado al marco legal español a través de la LOPDGDD que será estudiada más tarde en el trabajo. Estos sistemas recogen información sobre nuestras expresiones y rasgos faciales, que están considerados como datos biométricos bajo el RGPD. Este reglamento protege "directamente" nuestros rasgos físicos y por tanto "indirectamente" nuestras emociones.[54] Ambas normas europeas consiguen crear un marco de protección conjunta.

1. INTRODUCCIÓN AL MARCO NORMATIVO DE PROTECCIÓN DE DATOS

1.1 Regulación europea: El Reglamento General de Protección de Datos (RGPD)

El Reglamento General de Protección de Datos (RGPD), adoptado en 2016 y plenamente aplicable desde mayo de 2018, constituye el marco jurídico principal para la protección de los datos personales en el ámbito de la Unión Europea. Este reglamento establece normas claras sobre cómo deben recogerse, procesarse y protegerse los datos personales, con el objetivo de garantizar los derechos fundamentales de las personas en un entorno cada vez más digitalizado.

El RGPD se aplica al tratamiento de datos personales realizado por responsables o encargados establecidos en la Unión Europea, independientemente de si dicho tratamiento tiene lugar dentro o fuera de la UE. Asimismo, se extiende a organizaciones fuera de la UE que traten datos de ciudadanos europeos, siempre que dichas actividades estén relacionadas con la oferta de bienes o servicios o con el monitoreo de su comportamiento dentro de la Unión.[55]

---

54 Maldita.es. (9 de abril de 2024). *¿Son nuestras emociones datos personales? Qué dice la ley de protección de datos sobre el reconocimiento de emociones y el análisis de sentimientos con IA.* Maldita Tecnología. Recuperado de https://maldita.es/malditatecnologia/20240409/emociones-datos-personales-protegidos/

[55]Agencia Española de Protección de Datos [AEPD]. (2024). *¿Cuál es el ámbito de aplicación del RGPD?* Recuperado de https://www.aepd.es/preguntas-frecuentes/2-rgpd/1-de-aplicacion/FAQ-0202-cual-es-el-ambito-de-aplicacion-del-rgpd

El RGPD se sustenta en una serie de principios esenciales, algunos de ellos serán objeto de análisis más adelante, que orientan el tratamiento de los datos personales:[56] [57]

- Tratamiento proporcionado, legal y transparente: El tratamiento debe ser legítimo, claro y acorde a las expectativas del interesado.
- Limitación de la finalidad: Los datos solo pueden recogerse para fines específicos, explícitos y legítimos.
- Minimización de datos: Los datos deben ser adecuados, pertinentes y no excesivos para la finalidad con la que vayan a ser usados.
- Exactitud: Los datos personales deben ser precisos y mantenerse actualizados.
- Limitación del plazo de conservación: Los datos no deben conservarse más tiempo del necesario para los fines del tratamiento.
- Integridad y confidencialidad: Los datos deben tratarse de manera segura, garantizando su protección frente al acceso no autorizado o pérdida.
- Responsabilidad proactiva (*accuntability*): Los responsables o encargados del tratamiento deben no solo cumplir con la normativa, sino también ser capaces de demostrar dicho cumplimiento.

El RGPD presta especial atención a los datos sensibles, como los relativos al origen étnico, la salud, la orientación sexual o los datos biométricos. Estos últimos, utilizados para identificar de manera única a una persona, están directamente implicados en los sistemas de reconocimiento de emociones. Según el artículo 9 del RGPD, el tratamiento de datos sensibles está prohibido salvo que se cumpla alguna de las excepciones previstas, como el consentimiento explícito del interesado o cuando sea necesario para cumplir obligaciones laborales específicas bajo un marco legal.

El RGPD refuerza los derechos de las personas sobre sus datos personales. Entre ellos destacan:

- Derecho de acceso: conocer qué datos están siendo tratados y con qué finalidad.

---

[56] Grupo Adaptalia. (2024). *Principios de la protección de datos*. Recuperado de https://grupoadaptalia.es/blog/principios-de-la-proteccion-de-datos/#:~:text=Los%20principios%20protecci%C3%B3n%20de%20datos,y%20(vii)%20responsabilidad%20Proactiva

[57] Arena. (2024). *¿Cuáles son los 7 principios del RGPD?* Recuperado de https://www.liberties.eu/es/stories/cuales-son-los-7-principios-del-rgpd/44265

- Derecho de rectificación y supresión: corregir errores o eliminar datos cuando ya no sean necesarios.
- Derecho a la portabilidad: solicitar que los datos se transfieran a otro responsable del tratamiento.
- Derecho a la oposición y a la limitación del tratamiento: impedir o restringir el uso de los datos en determinados casos.[58]

En el entorno laboral, el RGPD impone desafíos específicos, especialmente en relación con el equilibrio entre los intereses del empleador y los derechos del trabajador. La recopilación de datos biométricos para herramientas como el reconocimiento de emociones requiere una **base jurídica sólida** y el cumplimiento estricto de los principios de **proporcionalidad y minimización**. Las empresas deben demostrar que el tratamiento es necesario para cumplir una finalidad legítima y que no existen alternativas menos invasivas.[59]

El RGPD establece, además, que las relaciones laborales no deben comprometer los derechos de privacidad del empleado, exigiendo que cualquier tratamiento de datos biométricos esté adecuadamente documentado, incluyendo **evaluaciones de impacto** que identifiquen riesgos y propongan medidas para mitigarlos. Estas evaluaciones de impacto que exige el RGPD no son idénticas a las exigidas por el RIA, difieren en su enfoque, alcance y contenido. Mientras que la evaluación del RIA se centra en los riesgos que un sistema de IA de alto riesgo puede generar sobre los derechos fundamentales en general, incluyendo libertad, dignidad o no discriminación, la del RGPD se limita a los riesgos vinculados al tratamiento de datos personales. Además, la del RIA la realizan proveedores y responsables del despliegue y exige considerar el contexto específico de uso, como el entorno laboral, este estudio se denomina en la práctica FRAIA (*Fundamental Rights and Algorithm Impact Assessment*), mientras que la del RGPD corresponde al responsable del tratamiento de datos y se enfoca en garantizar la privacidad y seguridad de la información personal, conocido en la práctica como DPIA (*Data Protection Impact Asessment*). Aunque pueden coexistir, tienen finalidades distintas y no se sustituyen entre sí. Además, el RIA explica en su artículo 27.3 como ambas se complementan para evitar repetición.

---

[58] Agencia Española de Protección de Datos. (2024). *Ejerce tus derechos*. AEPD. https://www.aepd.es/derechos-y-deberes/ejerce-tus-derechos

[59] Garriga Domínguez, A. (2024). "Los derechos ante los sistemas biométricos que incorporan Inteligencia Artificial." *Derechos y Libertades*, 51, 117-149.

1.2 Legislación española: La Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)

La Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) adapta el Reglamento General de Protección de Datos (RGPD) al marco legal español, estableciendo disposiciones específicas para su aplicación en distintos ámbitos, incluido el laboral. Esta normativa refuerza los derechos de los ciudadanos y regula situaciones específicas que el RGPD deja abiertas a la interpretación de los Estados miembros.[60]

La LOPDGDD se aplica al tratamiento de datos personales de cualquier persona física en territorio español. Además de complementar el RGPD, introduce normas particulares sobre la protección de datos en áreas clave, como las relaciones laborales, el uso de tecnologías de la información y la garantía de los derechos digitales.

La LOPDGDD establece normas específicas para el tratamiento de datos en el ámbito laboral, regulando cuestiones como el uso de sistemas de videovigilancia, la geolocalización y la monitorización de dispositivos electrónicos proporcionados por el empleador.[61] Estas disposiciones son esenciales para garantizar un equilibrio entre el control empresarial y los derechos fundamentales del trabajador.

Este texto legal introduce el reconocimiento de derechos digitales específicos, como el derecho a la desconexión digital en el ámbito laboral y el derecho a la intimidad frente al uso de dispositivos digitales. Estas garantías buscan proteger a los empleados frente a posibles intrusiones en su privacidad derivadas del uso de tecnologías avanzadas.[62]

En línea con el RGPD, la LOPDGDD considera los datos biométricos, como los empleados en sistemas de reconocimiento de emociones cuando se cumplan los requisitos del artículo 4.14

---

[60] España. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Boletín Oficial del Estado. https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

[61] España. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Boletín Oficial del Estado. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673 Artículos 89, 87 y 90.

[62] España. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Boletín Oficial del Estado. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673 arts 87 y 88

del RGPD, como categorías especiales de datos personales que requieren una protección reforzada. Su tratamiento está condicionado a:

- Una base de legitimación sólida de entre las previstas en el artículo 6 del RGPD, como el cumplimiento de obligaciones legales o la protección de intereses vitales que, en el caso de los datos biométricos, al ser considerados de carácter especial, deberá ser acompañada de una de las previsiones del artículo 9.2 del RGPD como, por ejemplo, que el tratamiento sea necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social.
- Proporcionalidad y necesidad: El empleador debe justificar que no existen alternativas menos intrusivas para alcanzar la finalidad legítima perseguida.
- Evaluaciones de impacto: En casos donde se usen tecnologías avanzadas que puedan generar riesgos significativos para los derechos de los empleados, es obligatorio realizar evaluaciones previas.

2. DATOS BIOMÉTRICOS

2.1 Definición y naturaleza de los datos biométricos

Los datos biométricos se definen en el artículo 4.14 del RGPD como aquellos datos personales obtenidos a partir de características físicas, fisiológicas o conductuales de una persona, que permiten o confirman su identificación única. Estos datos incluyen, entre otros, huellas dactilares, rasgos faciales, patrones de voz, iris y, en el caso del reconocimiento de emociones, **expresiones faciales, tono de voz o ritmo cardíaco** derivados de procesos tecnológicos avanzados.[63]

Los datos biométricos presentan características que los hacen especialmente sensibles:[64]

- Unicidad: Son exclusivos de cada individuo, lo que los convierte en una herramienta eficaz para la identificación o autentificación personal.

---

[63] Unión Europea. (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016,*

[64] Asociación de Bancos Múltiples de la República Dominicana (ABA). (2023, 11 de octubre). *El valor de los datos biométricos: ¿Cómo proteger tu identidad digital?* Asociación de Bancos Múltiples de la República Dominicana. https://aba.org.do/articulos-perspectivas/valor-de-los-datos-biometricos-como-proteger-identidad-digital/

- Inmutabilidad: No pueden ser alterados fácilmente sin procedimientos invasivos, a diferencia de contraseñas o claves alfanuméricas.
- Vinculación directa con la persona: Estos datos están intrínsecamente ligados a la identidad del individuo y, en muchos casos, a su privacidad más profunda.

El artículo 9 del RGPD clasifica los datos biométricos como una categoría especial de datos personales cuando se utilizan para identificar a una persona de **manera inequívoca**. Esto incluye cualquier tratamiento relacionado con herramientas de reconocimiento de emociones, ya que suelen analizar rasgos físicos y fisiológicos para interpretar estados emocionales, estableciendo una conexión directa con la identidad del individuo.

El reconocimiento de emociones combina el análisis de datos biométricos con algoritmos de inteligencia artificial para interpretar y categorizar estados emocionales, descripción doctrinal, ampliamente aceptada en documentos de carácter técnico, informes institucionales (como del SEPD, CEPD, IEEE SA, EU-OSHA, todos estos órganos han sido enumerados en la lista de abreviaturas utilizadas). Esto incluye la monitorización de:

- Expresiones faciales: identificación de microexpresiones que reflejan emociones específicas.
- Modulación de voz: análisis de patrones vocales como el tono, la velocidad o el volumen.
- Fisiología corporal: monitoreo del ritmo cardíaco, la presión arterial o la conductancia de la piel mediante sensores.

Estos elementos amplían el alcance de los datos biométricos, situándolos en una posición de alto riesgo para la privacidad debido a su capacidad de inferir aspectos profundamente personales, como emociones o estados mentales.

El uso de datos biométricos, particularmente en sistemas de reconocimiento de emociones, conlleva riesgos significativos:[65]

[65] Audidat. (2024). *Reconocimiento de emociones y protección de datos*. Audidat. https://www.audidat.com/blog/proteccion-de-datos/reconocimiento-de-emociones-y-proteccion-de-datos/

- Vulneración de la privacidad: la naturaleza íntima de estos datos puede exponer aspectos de la vida personal del individuo que exceden el propósito original del tratamiento.
- Uso indebido o excesivo: los datos biométricos pueden ser tratados con fines secundarios o discriminatorios si no se establecen controles estrictos.
- Riesgo de seguridad: una vez comprometidos, los datos biométricos no pueden "cambiarse" como una contraseña, lo que los convierte en un objetivo altamente atractivo para ciberataques.

3. PRINCIPIOS del RGPD APLICABLES AL TRATAMIENTO DE DATOS EN EL ÁMBITO LABORAL

3.1 Licitud, legitimidad y transparencia

El principio de licitud, lealtad y transparencia es uno de los pilares fundamentales del Reglamento General de Protección de Datos (RGPD), establecido en su artículo 5.1(a). Este principio exige que el tratamiento de datos personales sea legítimo, respetuoso con los derechos del interesado y realizado de manera clara y accesible. En el ámbito laboral, cobra especial relevancia debido a la posición de vulnerabilidad del trabajador frente al empleador, especialmente cuando se emplean tecnologías como los sistemas de reconocimiento de emociones.[66]

En el caso de los sistemas de reconocimiento de emociones, es esencial demostrar que su uso es estrictamente **necesario y proporcional** al objetivo declarado, evitando cualquier tratamiento que exceda los fines legítimos.

El tratamiento de datos personales debe realizarse de manera respetuosa con las expectativas razonables del trabajador y evitando cualquier tipo de engaño o abuso. En el ámbito laboral, esto requiere que:[67]

- El empleador explique de forma clara el propósito del tratamiento y su necesidad.

---

[66] Agencia Española de Protección de Datos [AEPD]. (2024). *Principios*. Recuperado de https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/principios

[67] Boletín Oficial del Estado [BOE]. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*. Recuperado de https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

- Se garantice que el tratamiento no se utilizará de manera discriminatoria, intrusiva o perjudicial para el empleado.
- Se limiten las finalidades del tratamiento exclusivamente a aquellas previamente declaradas.

Por ejemplo, si un sistema de reconocimiento de emociones se utiliza para evaluar el desempeño de los trabajadores, no sería leal emplearlo posteriormente para fines disciplinarios sin haberlo comunicado previamente.

La transparencia exige que los trabajadores sean informados de manera clara, accesible y comprensible sobre cómo se tratan sus datos personales. En el caso de herramientas de reconocimiento de emociones, esta transparencia es especialmente crucial, ya que el tratamiento involucra datos biométricos sensibles. Es recomendable que esta información se proporcione mediante cláusulas informativas claras y detalladas, y que se comunique no solo al inicio de la relación laboral, sino también cada vez que se introduzcan nuevos sistemas o se modifiquen las finalidades del tratamiento.

Aplicar estos principios en el uso de sistemas de reconocimiento de emociones presenta varios desafíos:

- Validez limitada del consentimiento: en el entorno laboral, el consentimiento puede no considerarse plenamente válido debido a la relación de subordinación.
- Ambigüedad en las finalidades: el uso de estas tecnologías puede generar confusión si no se delimitan claramente los propósitos.
- Acceso a información comprensible: los sistemas de inteligencia artificial y algoritmos complejos pueden dificultar la comprensión del tratamiento por parte de los trabajadores.

3.2 Minimización y limitación de la finalidad

Los principios de minimización y limitación de la finalidad están consagrados en los artículos 5.1(c) y 5.1(b) del RGPD, y constituyen un pilar esencial para garantizar un tratamiento de datos personales respetuoso con los derechos fundamentales.

La minimización de datos establece que solo deben recopilarse y tratarse los datos estrictamente necesarios para cumplir con la finalidad declarada. Este principio exige:

- Adecuación: los datos recogidos deben ser pertinentes y útiles para el propósito legítimo del tratamiento.
- Relevancia: sólo deben incluirse los datos que sean imprescindibles para alcanzar la finalidad establecida.
- Limitación: se deben evitar recopilaciones excesivas o superfluas de datos personales.

En el caso de los sistemas de reconocimiento de emociones, esto significa que únicamente se deberían procesar las métricas biométricas directamente relacionadas con el objetivo del tratamiento, como, por ejemplo, identificar niveles de estrés en tareas específicas. Pero, en cambio, no estaría justificado registrar expresiones faciales fuera del horario laboral o en contextos ajenos al trabajo.

El principio de limitación de la finalidad establece que los datos personales deben ser recogidos y tratados para fines específicos, explícitos y legítimos, y no podrán ser utilizados posteriormente para otros propósitos incompatibles con los originales. En el ámbito laboral, esto implica que el empleador debe delimitar con claridad las finalidades del uso de herramientas de reconocimiento de emociones. Cualquier cambio en las finalidades del tratamiento deberá ser notificado al trabajador y, en su caso, contar con una nueva base jurídica y no se permitirá el uso de estos datos para fines secundarios no relacionados, como sanciones disciplinarias o análisis personales no autorizados.

Por ejemplo, si un sistema de reconocimiento de emociones se utiliza para analizar el bienestar emocional de los trabajadores, no sería legítimo emplear los datos recopilados para decisiones de despido sin haber comunicado previamente esta finalidad. Todo ello, exclusivamente desde la perspectiva de la regulación de protección de datos y sin entrar en este apartado a analizar las implicaciones del Reglamento de Inteligencia Artificial. Posteriormente, a falta de jurisprudencia actual, se llevará a cabo un análisis conjunto para ver cómo se combina la aplicación de ambas normas.

3.3 Integridad y confidencialidad

El principio de integridad y confidencialidad, recogido en el artículo 5.1(f) del RGPD, exige que los datos personales sean tratados de manera segura, protegiéndolos contra accesos no autorizados, alteraciones indebidas, pérdidas accidentales o destrucción ilícita. En el caso del reconocimiento de emociones, resulta especialmente relevante debido a la sensibilidad de los datos biométricos tratados, los cuales requieren medidas reforzadas de seguridad.

La integridad implica garantizar que los datos recopilados sean precisos y representen fielmente la realidad. Además, deben implementarse mecanismos que eviten manipulaciones indebidas y aseguren que los datos permanecen intactos durante todo el proceso de tratamiento. Por ejemplo, en un sistema de reconocimiento de emociones, es esencial que las métricas recogidas reflejen con exactitud las expresiones faciales o las variaciones fisiológicas sin alteraciones injustificadas.[68]

Por otro lado, la confidencialidad busca restringir el acceso a los datos únicamente a personas autorizadas para fines específicos. Esto requiere establecer sistemas de protección, como el cifrado de la información y protocolos que aseguren la autenticación de usuarios. En el ámbito laboral, los datos emocionales, como registros de estrés o emociones detectadas, deben estar protegidos y accesibles sólo a quienes tengan autorización explícita, previniendo un uso indebido o divulgaciones no autorizadas.

Para garantizar ambos principios, las empresas deben adoptar medidas técnicas y organizativas adecuadas, como realizar evaluaciones de impacto para prever riesgos, almacenar los datos en entornos seguros y formar al personal que los gestiona. El incumplimiento de estos requisitos puede derivar en graves consecuencias, como la filtración de datos sensibles, la pérdida de confianza por parte de los empleados o sanciones legales significativas. En el contexto del reconocimiento de emociones, cumplir con el principio de integridad y confidencialidad no solo protege la privacidad de los trabajadores, sino que también fortalece un entorno laboral ético y respetuoso.

4. BASE JURÍDICA EN EL ÁMBITO LABORAL

El tratamiento de datos personales en el ámbito laboral requiere una **base jurídica sólida**, especialmente cuando se utilizan sistemas de reconocimiento de emociones, debido a la sensibilidad de los datos biométricos involucrados. Aunque el consentimiento del trabajador figura como una de las bases legales previstas en el artículo 6 del RGPD, su validez en este contexto es limitada debido a la relación de subordinación inherente al contrato laboral. Para que el consentimiento sea considerado libre, debe existir una auténtica capacidad de elección por parte del trabajador, sin que su negativa tenga consecuencias negativas. En la práctica, esta

[68] García, A. (2024). *Los derechos ante los sistemas biométricos que incorporan inteligencia artificial*. Recuperado de archivo local.

libertad es cuestionable, ya que los empleados pueden sentirse obligados a aceptar para evitar represalias o conflictos. Por ello, el consentimiento debería emplearse únicamente como última opción y en casos excepcionales donde no existan alternativas viables, acompañándose siempre de garantías reforzadas.

En el ámbito laboral, las bases jurídicas más sólidas y prácticas suelen ser el cumplimiento de una obligación legal, la ejecución del contrato laboral o los intereses legítimos del empleador. El cumplimiento de una obligación legal podría ser aplicable cuando exista una normativa específica que exija el tratamiento de datos, como la prevención de riesgos laborales en sectores de alto estrés o exposición emocional, siempre que se cumplan los principios de proporcionalidad y necesidad.

Los intereses legítimos del empleador podrían también teóricamente justificar el uso de sistemas de reconocimiento de emociones, pero su aplicación está supeditada a la realización de un test de proporcionalidad. Este test debe evaluar si:

1. El tratamiento es adecuado para alcanzar el objetivo perseguido.
2. Es necesario porque no existen medidas menos lesivas que puedan lograr el mismo resultado.
3. Existe un equilibrio entre el interés del empleador y los derechos fundamentales del trabajador.

Por ejemplo, un empleador podría justificar el uso de estas tecnologías para mejorar el bienestar emocional de los empleados en un entorno laboral de alta exigencia, pero sólo si demuestra que no hay otras herramientas menos invasivas que permitan identificar el estrés o la fatiga.

5. EVALUACIONES DE IMPACTO RELATIVAS A LA PROTECCIÓN DE DATOS

La evaluación de impacto relativa a la protección de datos (EIPD) es un requisito establecido en el artículo 35 del RGPD para los tratamientos que, debido a su naturaleza, alcance, contexto o finalidades, puedan generar un alto riesgo para los derechos y libertades de las personas. Se deberán realizar siempre que se haga un tratamiento a gran escala de datos biométricos. Estas evaluaciones de impacto han sido ya brevemente mencionadas en el principio de este capítulo cuando se las ha comparado con las que exige el RIA, a continuación, se analizan más en detalle. La EIPD debe incluir una serie de elementos fundamentales para garantizar un tratamiento seguro y conforme a la normativa:

- Descripción del tratamiento: Debe detallarse cómo se recopilan, procesan y almacenan los datos biométricos, así como las tecnologías empleadas.
- Análisis de la necesidad y proporcionalidad: Es imprescindible justificar que el tratamiento es necesario para alcanzar una finalidad legítima y que no existen alternativas menos intrusivas.
- Identificación de riesgos: Se deben identificar los posibles impactos negativos sobre los derechos de los trabajadores, como la pérdida de privacidad, discriminación o sesgos algorítmicos.
- Medidas de mitigación: Establecer medidas concretas para reducir los riesgos identificados, como la anonimización de datos, el cifrado de información o la implementación de controles de acceso.

El incumplimiento de la obligación de realizar una EIPD puede acarrear sanciones significativas bajo el RGPD, además de daños reputacionales para la empresa. Además, si se detectan vulneraciones de derechos derivadas de un tratamiento no evaluado adecuadamente, los trabajadores afectados podrían reclamar compensaciones económicas o impugnar el uso de estas tecnologías.

Las evaluaciones de impacto relativas a la protección de datos son una herramienta esencial para garantizar que el uso de sistemas de reconocimiento de emociones en el ámbito laboral sea seguro, ético y conforme al marco normativo. Al identificar y mitigar riesgos desde el inicio, las empresas no solo protegen los derechos de los trabajadores, sino que también fortalecen la confianza en estas tecnologías y evitan posibles conflictos legales y laborales.

6. TRANSPARENCIA Y DERECHO A LA INFORMACIÓN DEL TRABAJADOR

Se ha hablado de transparencia previamente en este trabajo al tratarse el RIA. Sin embargo,

> Transparencia-RGPD y la Transparencia-AIA tienen significados diferentes, establecen obligaciones para actores diferentes, se refieren a categorías de información distinta, tanto en contenido como en redacción, y se dirigen a destinatarios diferentes. Por lo tanto, si se proporciona a los interesados la misma información que se elabore desde el

punto de vista de Transparencia-AIA, no se estaría cumpliendo los deberes de Transparencia-RGPD.[69]

La transparencia y el derecho a la información son principios fundamentales del RGPD que garantizan que los trabajadores comprendan claramente cómo y por qué se recopilan y procesan sus datos personales. En el caso de los sistemas de reconocimiento de emociones, este principio adquiere especial relevancia debido a la sensibilidad de los datos biométricos tratados. El empleador está obligado a proporcionar información clara, concisa y accesible al trabajador antes de iniciar cualquier tratamiento.[70] Esta información debe incluir, entre otras cuestiones, la identidad del responsable del tratamiento, las finalidades específicas para las cuales se usarán los datos, la base jurídica que lo sustenta, la existencia de posibles cesiones o transferencias internacionales de datos, las categorías de datos tratados, la duración del tratamiento y los derechos que puede ejercer el trabajador, como el acceso, la rectificación o la supresión.[71]

Es fundamental que esta información se presente en un lenguaje claro, evitando tecnicismos, y a través de medios fácilmente accesibles, como políticas internas, contratos laborales o plataformas digitales. Además, debe ser actualizada cuando se produzcan cambios en las finalidades o condiciones del tratamiento, garantizando que los trabajadores estén siempre al tanto de cómo se gestionan sus datos personales. Por ejemplo, si la empresa decide utilizar el sistema de reconocimiento de emociones para nuevas finalidades, deberá informar previamente a los empleados de forma comprensible y detallada.

La transparencia debe mantenerse durante todo el ciclo de tratamiento, no solo en el momento de la recopilación de los datos. Esto implica establecer canales de comunicación claros para que los trabajadores puedan plantear dudas o ejercer sus derechos, además de informar regularmente sobre el estado del tratamiento y las medidas de protección adoptadas. Asimismo,

---

[69] Agencia Española de Protección de Datos. (2023, 25 de septiembre). *Inteligencia artificial: Transparencia.* https://www.aepd.es/prensa-y-comunicacion/blog/inteligencia-artificial-transparencia

[70]Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), *Diario Oficial de la Unión Europea*, L 119, art. 12.

[71]Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), *Diario Oficial de la Unión Europea*, L 119, Considerando 39.

la supervisión interna por parte del delegado de protección de datos o del área de recursos humanos es clave para garantizar el cumplimiento de este principio.

El incumplimiento del deber de transparencia puede generar desconfianza entre los trabajadores, deteriorar el clima laboral y dar lugar a conflictos legales. Además, las autoridades de protección de datos, como la AEPD, podrían sancionar a la empresa por no cumplir con esta obligación, invalidando incluso el tratamiento realizado. En conclusión, cumplir con la transparencia y garantizar el derecho a la información no solo asegura el cumplimiento normativo, sino que también refuerza la confianza de los empleados en el uso de estas tecnologías, promoviendo un entorno laboral más ético y equilibrado.[72]

7. SUPERVISIÓN Y CUMPLIMIENTO NORMATIVO

La supervisión y el cumplimiento normativo son elementos esenciales para garantizar que el tratamiento de datos personales mediante sistemas de reconocimiento de emociones en el ámbito laboral se ajuste a la normativa vigente. Estos mecanismos aseguran la protección de los derechos fundamentales de los trabajadores y minimizan los riesgos legales y éticos asociados al uso de tecnologías avanzadas.

El delegado de protección de datos (DPD) desempeña un rol crucial en la supervisión desde dentro de la organización de estos sistemas, especialmente cuando se tratan datos biométricos sensibles. Su función incluye asesorar a la empresa en la implementación de medidas adecuadas, supervisar las evaluaciones de impacto y actuar como punto de contacto entre la organización y las autoridades de protección de datos. Además, el DPD debe garantizar que el tratamiento de los datos cumpla con los principios de transparencia, proporcionalidad y limitación de la finalidad, supervisando que las finalidades declaradas se respeten en todo momento.

La Agencia Española de Protección de Datos (AEPD) también juega un papel fundamental como autoridad de control. Su labor incluye la recepción y resolución de denuncias presentadas por los trabajadores, la realización de inspecciones para verificar el cumplimiento normativo y la imposición de sanciones en caso de infracciones. La AEPD, además, suele emitir guías y

[72]Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), *Diario Oficial de la Unión Europea*, L 119, arts. 83, 58, 84.

recomendaciones específicas sobre el uso de tecnologías como el reconocimiento de emociones, facilitando a las empresas la adopción de buenas prácticas.[73]

A nivel autonómico, existen diversas autoridades de protección de datos, cuya competencia se limita al ámbito de actuación de las administraciones públicas de sus respectivas comunidades autónomas. Estas incluyen:[74]

- Autoritat Catalana de Protecció de Dades (APDCAT): Competente en Cataluña.
- Autoridad Vasca de Protección de Datos (AVPD): Competente en el País Vasco.
- Consejo de Transparencia y Protección de Datos de Andalucía (CTPDA): Competente en Andalucía.

Estas autoridades tienen funciones similares a las de la AEPD, pero limitadas a su ámbito territorial y a las administraciones públicas locales, como la resolución de reclamaciones, la realización de inspecciones y la emisión de recomendaciones específicas para sus respectivas comunidades.

Para garantizar el cumplimiento normativo, las empresas deben integrar la protección de datos como un elemento central de su estrategia. Esto incluye la implementación de medidas técnicas y organizativas, como auditorías periódicas, cifrado de datos y controles de acceso, así como la formación continua del personal sobre la normativa aplicable. Además, deben mantener una colaboración activa con las autoridades de protección de datos y documentar todas las actuaciones relacionadas con el tratamiento de datos personales.

El incumplimiento de estas obligaciones puede derivar en sanciones económicas significativas y daños reputacionales, además de vulnerar los derechos de los trabajadores. En conclusión, la supervisión efectiva y la colaboración con las autoridades de protección de datos, tanto estatales como autonómicas, son esenciales para asegurar un uso ético y seguro de los sistemas de reconocimiento de emociones en el ámbito laboral.

---

[73]Agencia Española de Protección de Datos [AEPD]. (2024). *¿En qué podemos ayudarte?* Recuperado de https://www.aepd.es/la-agencia/en-que-podemos-ayudarte
[74]VLEX. (2024). *Autoridades autonómicas de protección de datos*. Recuperado de https://vlex.es/vid/autoridades-autonomicas-proteccion-datos-716170265

CAPÍTULO V: LEGISLACIÓN LABORAL DE INTERÉS

1. EL ESTATUTO DE LOS TRABAJADORES Y LOS SISTEMAS DE RECONOCIMIENTO DE EMOCIONES

El uso de sistemas de reconocimiento de emociones en el entorno laboral genera conflictos con diversos derechos fundamentales protegidos por la Constitución Española (CE), el Estatuto de los Trabajadores (ET) y la normativa de la Unión Europea. Aunque aspectos como la protección de datos personales y la privacidad ya han sido analizados en los apartados relativos al RGPD y la LOPDGDD, aquí se abordará su impacto en el marco regulador del derecho laboral español, con especial énfasis en el Estatuto de los Trabajadores (ET).

1.1 Derecho a la intimidad en el trabajo (art. 18.1 CE y art. 4.2 ET)

El artículo 18.1 CE reconoce el derecho a la intimidad personal, reforzado en el ámbito laboral por el artículo 4.2 ET, que establece el derecho de los trabajadores al respeto de su intimidad y a la consideración debida a su dignidad. En consecuencia, cualquier medida empresarial que implique una monitorización constante del estado emocional de los empleados debe someterse a un análisis de proporcionalidad, como ha señalado el Tribunal Constitucional en la STC 292/2000.[75]

El uso de sistemas de reconocimiento de emociones plantea un riesgo mayor que otras herramientas de control laboral, como la videovigilancia o el registro de jornada, ya que afecta aspectos íntimos del trabajador, como su estado emocional y psicológico, sin que necesariamente exista un consentimiento libre e informado. Como se ha desarrollado en el apartado RGPD, el consentimiento en el ámbito laboral suele ser problemático debido a la relación de poder asimétrica entre empleador y trabajador, lo que refuerza la necesidad de que su uso sea excepcional y debidamente justificado.

1.2 Derecho a la no discriminación y riesgos de sesgo algorítmico (art. 17.1 ET)

El artículo 17.1 ET prohíbe expresamente la discriminación en el empleo por razones como sexo, origen racial o étnico, discapacidad, edad o cualquier otra condición personal o social. Como se ha analizado en el apartado relativo a los sesgos algorítmicos, el uso de estos sistemas

[75]Tribunal Constitucional. (2000). *Sentencia 292/2000, de 30 de noviembre de 2000*.

puede generar discriminaciones indirectas si los algoritmos de reconocimiento de emociones han sido entrenados con sesgos de género, culturales o raciales, afectando desproporcionadamente a ciertos colectivos.

Además, el uso de estos sistemas en procesos de selección o promoción interna podría contravenir la prohibición del uso de criterios subjetivos o no transparentes en la contratación y evaluación del desempeño (artículo 17.1 ET), especialmente si las decisiones empresariales se basan en interpretaciones algorítmicas de emociones sin verificación humana adecuada.

1.3 Derecho a la transparencia y control empresarial sobre la actividad del trabajador (art. 64 ET y art. 20 ET)

El artículo 20 ET otorga al empleador la facultad de organizar y controlar la actividad laboral, pero con límites claros cuando afectan derechos fundamentales. La jurisprudencia ha reiterado que cualquier medida de control sobre los trabajadores debe ser proporcional, necesaria y respetuosa con su dignidad (STC 39/2016).[76]

El artículo 64 ET reconoce el derecho de los representantes de los trabajadores a ser informados sobre los parámetros, reglas e instrucciones de estos sistemas de inteligencia artificial y los algoritmos que se utilicen. En este sentido, la falta de transparencia en la implementación de estos sistemas vulnera las obligaciones de informar a los representantes sindicales, lo que podría invalidar su uso en la práctica.[77]

Como se ha explicado en el apartado sobre transparencia y supervisión, el Reglamento de IA exige la supervisión humana en el uso de estos sistemas, pero no establece criterios claros sobre cómo garantizar la transparencia en el ámbito laboral, lo que genera inseguridad jurídica para empresas y trabajadores.

2. INTERACCIÓN CON LA LEY DE PREVENCIÓN DE RIESGOS LABORALES (LPRL)

El uso de sistemas de reconocimiento de emociones en el ámbito laboral plantea interrogantes sobre su compatibilidad con la Ley 31/1995, de 8 de noviembre, de Prevención de Riesgos

---

[76]Tribunal Constitucional. (2016). *Sentencia 39/2016, de 3 de marzo de 2016*.
[77]Estatuto de los Trabajadores, 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, *Boletín Oficial del Estado*, núm. 255, de 24 de octubre de 2015, art. 64.

Laborales (LPRL). Si bien estos sistemas podrían contribuir a la identificación y mitigación de riesgos psicosociales, su implementación debe evaluarse dentro del marco normativo vigente, garantizando el respeto a los derechos fundamentales y la proporcionalidad en su uso.

2.1 Justificación bajo la LPRL y prevención de riesgos psicosociales

La LPRL establece la obligación del empleador de velar por la seguridad y salud de los trabajadores en todos los aspectos relacionados con su trabajo (art. 14 LPRL). Desde esta perspectiva, se ha identificado que los sistemas de reconocimiento de emociones podrían integrarse en estrategias de prevención mediante:

- Identificación temprana de riesgos psicosociales, como estrés o fatiga, con el fin de adoptar medidas preventivas adecuadas.
- Mitigación de accidentes laborales en sectores donde el factor emocional influye en la seguridad, como el transporte o la atención sanitaria.
- Optimización de entornos laborales, ajustando condiciones de trabajo en función de patrones colectivos de bienestar emocional.

Sin embargo, como ya se ha señalado en otros apartados, estas aplicaciones deben cumplir con estrictos criterios de proporcionalidad y necesidad, evitando el uso desproporcionado de datos biométricos.

2.2 Alternativas menos intrusivas dentro del marco de la LPRL

En línea con lo previamente identificado, la proporcionalidad es clave en la implementación de herramientas de prevención de riesgos. Existen métodos alternativos que cumplen los mismos objetivos sin requerir el uso de datos biométricos, como:

- Encuestas de riesgos psicosociales validadas científicamente para evaluar el estado emocional de los trabajadores.
- Evaluaciones psicológicas periódicas, llevadas a cabo por expertos en salud laboral.
- Análisis de indicadores indirectos, como tasas de absentismo o rotación de personal, que pueden reflejar problemas de estrés o insatisfacción.

Estas opciones deben considerarse prioritarias antes de recurrir a tecnologías de reconocimiento de emociones, salvo en casos donde su valor añadido esté debidamente justificado.

3. NEGOCIACIÓN COLECTIVA Y REGULACIÓN DEL RECONOCIMIENTO DE EMOCIONES

Los convenios colectivos juegan un papel fundamental en la regulación de los sistemas de reconocimiento de emociones, estableciendo límites y garantías para su implementación en el ámbito laboral. En sectores donde la inteligencia artificial ya impacta la gestión del personal, los sindicatos han intervenido activamente para negociar el uso de estas tecnologías, asegurando la protección de los derechos de los trabajadores. Un ejemplo reciente, que ya ha sido previamente mencionado en este trabajo al hablar de transparencia laboral en el RIA, es el convenio colectivo de Just Eat en España, donde CCOO y UGT acordaron la creación de una Comisión Algoritmo para supervisar el impacto de los sistemas de IA en la organización del trabajo y evitar discriminaciones automatizadas.[78]

La Comisión Algoritmo permite canalizar de forma ordenada, continua y verificable el derecho de información sobre sistemas de inteligencia artificial que afectan a las condiciones laborales. Su diseño paritario (dos representantes por parte empresarial y dos por parte sindical), la posibilidad de solicitar la comparecencia de técnicos responsables, y su función específica de seguimiento de los cambios sustanciales en los algoritmos, le otorgan contenido real y capacidad operativa. Además, garantiza que la información técnica no se traduzca en asimetría de poder, ya que empodera a los representantes de los trabajadores para comprender e intervenir en decisiones automatizadas.

Este precedente sugiere que los sindicatos podrían exigir la inclusión de órganos de supervisión específicos en empresas que utilicen reconocimiento de emociones.[79]La existencia de un órgano como la Comisión Algoritmo en el ámbito de los sistemas de reconocimiento de emociones permitiría incorporar una perspectiva preventiva, ofreciendo un espacio de diálogo técnico-jurídico entre la empresa y la representación social para evaluar, por ejemplo, si el uso de estas herramientas responde a criterios de necesidad y proporcionalidad, o si se adecúa a las

[78]FSC-CCOO. (2024). *CCOO, UGT y FETICO firman con Just Eat España un nuevo acuerdo que lidera el diálogo social en el sector de las plataformas de delivery*. Recuperado de https://fsc.ccoo.es/noticia:715603--CCOO_UGT_y_FETICO_firman_con_Just_Eat_Espana_un_nuevo_acuerdo_que_lidera_el_dialogo_social_en_el_sector_de_las_plataformas_de_delivery&opc_id=6a5018a39e084efa266aa087e2cc86d0

[79]Audiolis. (2024). *Reglamento de inteligencia artificial y negociación colectiva*. Recuperado de https://www.audiolis.com/blog/reglamento-inteligencia-artificial-negociacion-colectiva

garantías previstas en el Reglamento Europeo de Inteligencia Artificial y la normativa nacional de protección de datos.[80]

Otro ejemplo de avance en la regulación colectiva del uso de inteligencia artificial es el Convenio Colectivo del Sector de la Banca, que incorpora una cláusula específica sobre la gestión algorítmica en el ámbito laboral. En concreto, el convenio establece que

> las Empresas informarán a la representación legal de los trabajadores sobre el uso de la analítica de datos o los sistemas de inteligencia artificial cuando los procesos de toma de decisiones en materia de recursos humanos y relaciones laborales **se basen exclusivamente en modelos digitales sin intervención humana**. Esta información deberá incluir, al menos, *"los datos que nutren los algoritmos, la lógica de funcionamiento y la evaluación de los resultados"*.[81]

Aunque el uso de sistemas de inteligencia artificial sin supervisión humana no sería admisible bajo el marco normativo europeo, esta cláusula refuerza el control preventivo sindical en los casos en que la automatización tienda a desplazar la intervención directa, y lo hace exigiendo información concreta, técnica y comprensible sobre el funcionamiento de los algoritmos aplicados en decisiones laborales. A diferencia de previsiones más generales, esta cláusula fija el mínimo de contenido que debe facilitarse a la representación de los trabajadores, convirtiéndose en una referencia útil para futuros convenios colectivos, especialmente en sectores donde pudieran aplicarse tecnologías sensibles como el reconocimiento de emociones.

En empresas que implementen estos sistemas, la negociación colectiva podría centrarse en cláusulas que:

- Limiten el uso del reconocimiento de emociones exclusivamente a fines justificados, como la prevención de riesgos psicosociales, excluyendo su utilización para la evaluación del desempeño o la toma de decisiones disciplinarias.

---

[80] CCOO y UGT. (2023). *Acuerdo colectivo de trabajo con Just Eat España*. https://www.ccoo-servicios.es/archivos/Acuerdo%20Sindicatos%20JUST%20EAT(1).pdf

[81] Federación de Servicios Financieros y Administrativos de CCOO. (2021). *Convenio colectivo del sector bancario 2021*. Art 80.5. https://www.ccoo-servicios.es/archivos/financiero/Convenio-Banca-2021.pdf

- Garantías de transparencia, exigiendo a la empresa informar periódicamente a los representantes sindicales sobre el funcionamiento del sistema, los datos recopilados y las medidas de seguridad implementadas.
- Supervisión y auditorías periódicas, permitiendo la intervención de expertos independientes o comisiones sindicales para evaluar el impacto del sistema en la privacidad y bienestar de los trabajadores.
- Derecho a la desconexión emocional, impidiendo la monitorización continua y asegurando que el uso de estos sistemas no implique una vigilancia invasiva fuera del horario laboral.

La negociación colectiva es clave para equilibrar la introducción de estas tecnologías con la protección de los derechos laborales, estableciendo mecanismos de control que eviten abusos y garanticen su uso proporcional y transparente en el entorno de trabajo.[82]

CAPÍTULO VI: RESPONSABILIDADES LEGALES POR USO INDEBIDO

El uso indebido de un sistema de reconocimiento de emociones puede generar múltiples responsabilidades para la empresa. Administrativamente, puede enfrentar sanciones por incumplir el RIA, el RGPD y la normativa laboral. La AEPD puede imponer multas por tratamiento indebido de datos biométricos, mientras que la Inspección de Trabajo y Seguridad Social (ITSS)[83] puede sancionar a la empresa si el sistema vulnera derechos laborales, como la intimidad, la dignidad o la no discriminación. [84]

Civilmente, los trabajadores pueden demandar a la empresa por responsabilidad contractual si el sistema afecta su relación laboral o sus derechos fundamentales, mientras que el fabricante o proveedor del software podría ser demandado por responsabilidad extracontractual si el sistema presenta fallos o sesgos que perjudican a los empleados.[85]

---

[82] UGT. (2024). *Guía web negociación*. Recuperado de https://www.ugt.es/sites/default/files/guiawebnegociacion.pdf

[83]Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, *Boletín Oficial del Estado*, núm. 189, de 8 de agosto de 2000.

[84] Reglamento (UE) 2024/XX del Parlamento Europeo y del Consejo, de [fecha], relativo a la inteligencia artificial y por el que se establecen disposiciones sobre transparencia, derechos fundamentales y supervisión, *Diario Oficial de la Unión Europea*,

[85]España. (1889). *Código Civil* (Real Decreto de 24 de julio de 1889, con sus reformas vigentes). Boletín Oficial del Estado.

Penalmente, si el sistema vulnera la privacidad o se usa para prácticas discriminatorias, la empresa o sus responsables pueden ser investigados por delitos contra la intimidad (art. 197 CP) o contra los derechos de los trabajadores (art. 311 CP), además de enfrentar responsabilidad penal de la persona jurídica si no se han implementado controles adecuados para evitar estos riesgos. [86]

Laboralmente, los trabajadores afectados pueden impugnar decisiones basadas en el sistema, [87] exigir indemnización por daños morales si sufren perjuicios psicológicos o profesionales, e incluso promover demandas colectivas a través de sindicatos si el impacto es generalizado. La empresa debe actuar con diligencia, revisar el cumplimiento normativo, corregir irregularidades y evaluar la posible responsabilidad de los directivos involucrados.[88]

CAPITULO VII: POSIBLES PROPUESTAS DE DESARROLLO LEGISLATIVO Y MEJORA DE LA SEGURIDAD JURÍDICA

Después de haber analizado el marco jurídico de los sistemas de reconocimiento de emociones en el ámbito laboral, este apartado estudia propuestas clave que buscan consolidar un marco normativo más sólido y equilibrado, promoviendo el desarrollo ético de estas herramientas y garantizando la protección de los derechos fundamentales de los trabajadores.

Las iniciativas aquí exploradas ofrecen soluciones pragmáticas y flexibles. Estas propuestas no solo fortalecerán la seguridad jurídica, sino que también asegurarían que la innovación tecnológica se desarrollase de manera ética, alineándose con los valores sociales y las normativas vigentes.

1. AUTORREGULACIÓN MEDIANTE CÓDIGOS DE CONDUCTA EMPRESARIALES

La autorregulación empresarial, basada en la adopción de códigos de conducta específicos, puede ser un mecanismo eficaz para garantizar el uso ético y responsable de los sistemas de inteligencia artificial (IA) destinados al reconocimiento de emociones en el ámbito laboral. Si las empresas desarrollan sus propios códigos de conducta específicos, pueden marcar límites

---

[86]España. (1995). *Código Penal* (Ley Orgánica 10/1995, de 23 de noviembre, con sus reformas vigentes). Boletín Oficial del Estado.
[87]España. (2011). *Ley 36/2011, de 10 de octubre, reguladora de la jurisdicción social*. Boletín Oficial del Estado
[88]España. (2000). *Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social*. Boletín Oficial del Estado.

claros y establecer buenas prácticas que vayan más allá de lo que exige la ley. Esto les da margen para adaptarse mejor a su sector y a cómo funcionan internamente.[89]

Un buen punto de partida es definir con claridad los fines permitidos para el uso de estas tecnologías, evitando la ambigüedad que pueda derivar en abusos o usos desproporcionados. Por ejemplo, el reconocimiento de emociones podría utilizarse legítimamente para mejorar el bienestar de los trabajadores o la experiencia del cliente, pero debería excluirse su implementación para fines disciplinarios o de control excesivo que vulneren la dignidad de los empleados. Este tipo de regulación interna puede permitir alinear el uso de estas tecnologías con los principios de proporcionalidad y necesidad establecidos en el Reglamento Europeo de IA y las normativas laborales nacionales.

La transparencia debería ser otro pilar fundamental de estos códigos. Las empresas deben garantizar que los trabajadores sean plenamente informados acerca del funcionamiento de los sistemas, los datos recopilados, su finalidad y las posibles consecuencias derivadas de su utilización. Esta información debería recogerse en los contratos laborales o en políticas internas claras, junto con canales de comunicación accesibles para resolver dudas o reportar posibles abusos.

La protección de los datos biométricos también debe ocupar un lugar central en los códigos de conducta. Es necesario limitar la recopilación y el tratamiento de información exclusivamente a los fines justificados, asegurando que los datos sensibles sean gestionados de manera segura. Esto incluye la implementación de medidas técnicas como la anonimización y la eliminación de datos una vez cumplido su propósito. [90]

Además, un código de conducta eficaz debería prever la creación de mecanismos internos de supervisión y control. Un comité de ética empresarial, compuesto por expertos en IA, recursos humanos y representantes de los trabajadores, puede desempeñar un rol crucial en la vigilancia del cumplimiento de los principios establecidos. Este comité podría evaluar periódicamente el

---

[89] Mariscal & Abogados. (n.d.). *Códigos de conducta empresariales*. Recuperado de https://www.mariscal-abogados.es/codigos-de-conducta-empresariales

[90]Agencia Española de Protección de Datos (AEPD). (2023). *Guía sobre protección de datos y relaciones laborales*. Agencia Española de Protección de Datos.
Disponible en: https://www.aepd.es/es/documento/guia-proteccion-datos-relaciones-laborales.pdf pp. 7-8, 23

impacto del uso de estas herramientas y proponer ajustes en función de la evolución tecnológica o de las necesidades de la empresa.[91]

Por último, la formación continua en el uso responsable de estas tecnologías es clave. Sensibilizar tanto a directivos como a empleados ayuda a generar confianza y a construir una cultura organizativa basada en el respeto y la responsabilidad. Incluir también consecuencias claras ante un uso indebido refuerza la eficacia del código.

La autorregulación mediante códigos de conducta ofrece múltiples ventajas en el contexto del uso de sistemas de reconocimiento de emociones en el ámbito laboral. Además de proporcionar flexibilidad para adaptarse a las características particulares de cada organización, estos instrumentos permiten una implementación más rápida que la normativa pública y fomentan un entorno de confianza entre empleadores y empleados. En definitiva, los códigos de conducta no solo refuerzan la seguridad jurídica en el uso de estas tecnologías, sino que también posicionan a las empresas como actores responsables y éticamente comprometidos en la transformación digital del entorno laboral.

2. EMISIÓN DE CIRCULARES VINCULANTES POR PARTE DE LA AEPD

El desarrollo y uso de sistemas de reconocimiento de emociones en el ámbito laboral plantea retos normativos que requieren un enfoque legislativo más preciso y adaptado. Aunque el RGPD y la LOPDGDD ofrecen el marco general, su aplicación práctica en este terreno ha dejado al descubierto algunas lagunas, tanto para proteger los derechos de los trabajadores como para dar seguridad jurídica a las empresas.

Una recomendación es que la AEPD priorice el uso de su capacidad para emitir circulares vinculantes, en lugar de apoyarse principalmente en guías y recomendaciones. Estas últimas, aunque puedan tener cierta utilidad, carecen de seguridad jurídica y no están sujetas a control jurisdiccional, lo que genera incertidumbre tanto para las empresas como para los trabajadores. Las circulares, por su naturaleza vinculante y su mayor peso normativo, permitirían establecer directrices claras y exigibles sobre el uso de tecnologías como el reconocimiento de emociones, proporcionando un marco más sólido para su implementación.

---

[91]Agencia Española de Protección de Datos (AEPD). (2023). *Guía sobre protección de datos y relaciones laborales*. Agencia Española de Protección de Datos.
Disponible en: https://www.aepd.es/es/documento/guia-proteccion-datos-relaciones-laborales.pdf, pp. 24, 31

La AEPD tiene por ley la potestad para dictar circulares de carácter vinculante. Esta facultad fue establecida expresamente en la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD) y desarrollada en su Estatuto aprobado por Real Decreto 389/2021. En particular, el artículo 55 de la LOPDGDD dispone que la Presidencia de la AEPD "podrá dictar disposiciones que fijen los criterios a que responderá la actuación de esta autoridad en la aplicación" del Reglamento General de Protección de Datos (RGPD) y de la propia LOPDGDD, las cuales se denominarán "Circulares de la AEPD" .[92] La ley también establece que estas Circulares tendrán carácter obligatorio una vez publicadas en el Boletín Oficial del Estado boe.es. En consonancia, el Estatuto de la AEPD (RD 389/2021) confirma en su artículo 6 la potestad de la Presidencia para dictar tales circulares vinculantes, siguiendo un procedimiento formal (incluyendo informes técnicos y jurídicos, periodo de audiencia pública y dictamen del Consejo de Estado).[93] Se trata por tanto de normas reglamentarias emanadas de la AEPD, con vocación de generalidad y eficacia jurídica obligatoria para sus destinatarios desde su entrada en vigor.

Tras la entrada en vigor del Estatuto de 2021, la AEPD ha comenzado a ejercer esta potestad normativa. Un ejemplo destacado es la Circular 1/2023, primera circular publicada por la Agencia, relativa al derecho de los usuarios a no recibir llamadas comerciales no solicitadas. Esta Circular, publicada en el BOE el 28 de junio de 2023, fija los criterios que aplicará la AEPD al interpretar el nuevo artículo 66.1.b) de la Ley 11/2022 General de Telecomunicaciones.[94] Dicho precepto legal reconoce a los usuarios finales el derecho a no recibir llamadas de prospección comercial no deseadas, salvo que exista consentimiento previo u otra base de legitimación bajo el RGPD. La Circular vino a aclarar las dudas interpretativas sobre ese artículo, estableciendo de forma vinculante cómo debe entenderse la excepción del interés legítimo en estos casos.[95]

---

[92] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *Boletín Oficial del Estado*, núm. 294, de 6 de diciembre de 2018. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

[93] Ley 7/2021, de 20 de mayo, de cambio climático y transición energética, *Boletín Oficial del Estado*, núm. 121, de 21 de mayo de 2021, art. 6.

[94] Agencia Española de Protección de Datos [AEPD]. (2023, 28 de junio). *Circular sobre el derecho de los usuarios a oponerse al tratamiento de sus datos personales para fines de marketing*. https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-la-circular-sobre-el-derecho-de-los-usuarios

[95] Agencia Española de Protección de Datos [AEPD]. (2023, 28 de junio). *Circular sobre el derecho de los usuarios a oponerse al tratamiento de sus datos personales para fines de marketing*. https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-la-circular-sobre-el-derecho-de-los-usuarios

Una posible medida de mejora legislativa sería que la Agencia Española de Protección de Datos (AEPD) emitiera una circular vinculante que aportase criterios específicos para valorar la proporcionalidad en el uso de sistemas de reconocimiento de emociones en el entorno laboral. En particular, esta circular podría establecer que la **finalidad del tratamiento emocional** debe estar definida funcionalmente, es decir, de forma concreta, evaluable y operativa.

No bastaría, por tanto, con invocar propósitos genéricos como "mejorar el bienestar emocional" o "optimizar la motivación", sino que el responsable del tratamiento debería vincular el uso del sistema a una actividad empresarial concreta, como por ejemplo la detección temprana de fatiga en tareas críticas de seguridad. Esta exigencia permitiría descartar usos difusos o estratégicos, que podrían enmascarar objetivos de control o evaluación subjetiva del rendimiento bajo etiquetas aparentemente positivas.

Asimismo, se propone reforzar el rol de las autoridades supervisoras como orientadores de las entidades supervisadas, promoviendo una relación más colaborativa y menos centrada en el carácter sancionador. Esto podría lograrse mediante el desarrollo de mecanismos de consulta vinculantes como los que ya existen en el ámbito tributario. También se sugiere fomentar la elaboración de estándares técnicos específicos en colaboración con el sector privado, que sirvan como referencia práctica para el diseño y la implementación de sistemas de reconocimiento de emociones respetuosos con la normativa.

3. CORREGULACIÓN A TRAVÉS DE ACUERDOS SECTORIALES

La corregulación, entendida como la colaboración entre actores públicos y privados para desarrollar marcos normativos específicos, representa una solución equilibrada y adaptable para el uso de sistemas de reconocimiento de emociones en el ámbito laboral. Este enfoque permite que las partes interesadas, administraciones públicas, empresas y sindicatos, trabajen conjuntamente para establecer acuerdos sectoriales que regulen de manera contextualizada el empleo de estas tecnologías, garantizando tanto la protección de los derechos fundamentales de los trabajadores como la competitividad y eficiencia empresarial.[96]

Ej: ***The updated Digital Education Action Plan*** *will help make better use of data and AI-based technologies such as learning and predictive analytics with the aim to improve education and*

[96] European Commission. (2020)**.** *White Paper on Artificial Intelligence: A European approach to excellence and trust.*

training systems and make them fit for the digital age. The Plan will also increase awareness of AI at all levels of education in order to prepare citizens for informed decisions that will be increasingly affected by AI.[97]

En el contexto laboral, la corregulación puede materializarse mediante la creación de acuerdos sectoriales que definan estándares comunes y buenas prácticas para el uso de sistemas de inteligencia artificial. Estos acuerdos deben abordar aspectos como los fines legítimos de estas herramientas, los límites en su implementación, los procedimientos de supervisión y las garantías necesarias para evitar abusos. Al ser diseñados de forma específica para cada sector, podrían adaptarse a las particularidades de las actividades económicas, como las exigencias de la atención al cliente, la educación o el teletrabajo, en las que estas tecnologías pueden tener un impacto significativo.

Un ejemplo de éxito en el ámbito de la corregulación, aunque ajeno en el ámbito estrictamente laboral, es el convenio firmado en octubre de 2021 entre la Dirección General de Ordenación del Juego (DGOJ) y AUTOCONTROL, que actualizó el marco de cooperación existente desde 2011 para la publicidad, patrocinio y promoción de las actividades del juego de ámbito estatal. Este acuerdo ha permitido un control más eficaz de la publicidad en el sector del juego, demostrando la efectividad de la corregulación en áreas sensibles.[98]

Una de las principales ventajas de la corregulación es su capacidad para fomentar el consenso entre los distintos agentes sociales. Las mesas de diálogo tripartitas, que incluyen a representantes de empleadores, trabajadores y reguladores, son un mecanismo clave para lograr este objetivo. Estas instancias pueden ayudar a discutir y negociar las condiciones bajo las cuales se utilizarán los sistemas de reconocimiento de emociones, asegurando que las medidas adoptadas reflejen un equilibrio justo entre los intereses de las empresas y los derechos de los empleados[99]. Además, la involucración de los sindicatos no solo refuerza la legitimidad de los acuerdos, sino que también favorece su aceptación y cumplimiento.

---

[97] European Commission. (2020)**.** *White Paper on Artificial Intelligence: A European approach to excellence and trust.*

[98]Autocontrol. (2021, 14 de octubre). *La Dirección General del Juego y AUTOCONTROL firman un convenio de corregulación sobre publicidad del juego*. https://www.autocontrol.es/2021/10/14/direccion-general-del-juego-y-autocontrol-convenio-corregulacion-publicidad-juego/

[99]Organización Internacional del Trabajo. *(2018). Informe sobre el diálogo social y las normas internacionales del trabajo. Recuperado de* https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40ed_norm/%40relconf/documents/meetingdocument/wcms_672978.pdf

La transparencia y la rendición de cuentas también deberían ser pilares fundamentales de este modelo. Los acuerdos sectoriales pueden incluir la obligación de realizar auditorías periódicas, evaluar el impacto real de los sistemas implantados y establecer procedimientos claros para resolver controversias o reclamaciones de los trabajadores.[100]

Desde el punto de vista normativo, la corregulación tiene además un valor estratégico: los acuerdos alcanzados pueden convertirse en una base sólida para futuras regulaciones específicas. Al recoger las necesidades reales y los retos concretos de cada sector, ayudan a diseñar políticas públicas más eficaces y alineadas con la evolución tecnológica y las dinámicas del mercado laboral.[101]

En definitiva, la corregulación a través de acuerdos sectoriales permite avanzar hacia un uso más ético y responsable de los sistemas de reconocimiento de emociones. Combinando la capacidad técnica y organizativa de las empresas con la representación democrática de los trabajadores, se promueve una transformación digital equilibrada, que impulse la innovación sin dejar de proteger los derechos fundamentales en el trabajo.

4. DESARROLLO DE ESTÁNDARES TÉCNICOS INTERNACIONALES

El desarrollo de estándares técnicos internacionales puede ser un componente fundamental para garantizar la seguridad, fiabilidad y equidad en el uso de sistemas de reconocimiento de emociones en el ámbito laboral. Estos estándares, promovidos por organismos como la Organización Internacional de Normalización (ISO), pueden ayudar a establecer requisitos mínimos que deben cumplir estas tecnologías antes de su implementación. La estandarización no solo proporciona un marco técnico claro para las empresas, sino que también refuerza la seguridad jurídica y la confianza de los trabajadores en el uso de estas herramientas.

> ISO 45003, Gestión de la Seguridad y Salud en el Trabajo – Salud y Seguridad Psicológicas en el trabajo – Directrices para la gestión de riesgos psicosociales, es la primera norma mundial que aborda la salud psicológica de un trabajador y las áreas que

[100] Edwards, L., & Veale, M. (2017). *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*. Duke Law & Technology Review, 16(1), 18-84.
[101] Centro de Documentación Europea - Universidad de Granada. (2024, 12 de marzo). *Más de 100 empresas firman los compromisos del Pacto sobre la IA de la UE para impulsar un desarrollo fiable y seguro*. https://cde.ugr.es/index.php/union-europea/noticias-ue/1858-mas-de-100-empresas-firman-los-compromisos-del-pacto-sobre-la-ia-de-la-ue-para-impulsar-un-desarrollo-fiable-y-seguro

pueden afectarla, incluidas la comunicación ineficaz, la presión excesiva, el liderazgo deficiente y la cultura organizacional.[102]

Uno de los principales beneficios de adoptar estándares internacionales es la posibilidad de garantizar la interoperabilidad de los sistemas. En un contexto global donde muchas empresas operan en diferentes países, contar con especificaciones comunes ayuda a evitar la fragmentación normativa y permite desplegar estos sistemas sin comprometer su funcionamiento ni generar incertidumbre legal. Además, los estándares actúan como garantía frente a riesgos como el sesgo algorítmico, al exigir pruebas de equidad, transparencia y fiabilidad. En este contexto, la ISO/IEC 42001:2023, el primer estándar internacional para sistemas de gestión de inteligencia artificial, también puede desempeñar un papel crucial. Según la ISO, esta norma *"proporciona un marco para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de IA que aborde los desafíos éticos, técnicos y organizativos"* (*ISO/IEC 42001:2023*, 2023). Su adopción impulsa la aplicación de principios éticos y transparentes en tecnologías avanzadas, incluyendo los sistemas de reconocimiento de emociones, promoviendo una integración responsable en el entorno laboral.

La adopción de estos estándares también promueve la transparencia y el acceso a la información sobre cómo funcionan los sistemas de reconocimiento de emociones. Por ejemplo, las certificaciones técnicas pueden incluir requisitos sobre la explicabilidad de los algoritmos, permitiendo que los usuarios y los trabajadores comprendan las bases de las decisiones automatizadas. Esta transparencia es crucial para proteger los derechos fundamentales y garantizar que las tecnologías no sean utilizadas de manera arbitraria o discriminatoria.

Los estándares técnicos pueden servir como una herramienta para reducir la fragmentación regulatoria entre países o regiones.[103] En lugar de depender exclusivamente de normativas nacionales o supranacionales que pueden diferir significativamente, los estándares internacionales proporcionan un punto de referencia común que armoniza las expectativas de los reguladores y las prácticas de las empresas[104]. Esto no solo facilita el cumplimiento

---

[102] GlobalSTD. (s.f.). *La salud mental en los espacios de trabajo: ISO 45003*. Recuperado de https://www.globalstd.com/blog/salud-mental-en-los-espacios-de-trabajo-iso-45003/

[103] Abriendo Mercados. (2023). *Importancia de armonizar normas y regulaciones en el comercio exterior*. Recuperado de https://abriendomercados.com/importancia-de-armonizar-normas-y-regulaciones-en-el-comercio-exterior/

[104] Abriendo Mercados. (2023). *Importancia de armonizar normas y regulaciones en el comercio exterior*. Recuperado de https://abriendomercados.com/importancia-de-armonizar-normas-y-regulaciones-en-el-comercio-exterior/

normativo, sino que también impulsa la competitividad empresarial al eliminar barreras técnicas al comercio y la innovación.

El IEEE 7014-2024 exige que los sistemas informen claramente sobre su funcionamiento y metodología de análisis afectivo, asegurando que los usuarios comprendan cómo se interpretan sus estados emocionales y con qué propósito se utilizan dichos datos.[105] Además, refuerza la importancia del consentimiento informado y la veracidad en la identificación de sistemas que analizan estados emocionales, aspectos clave en la protección de los derechos de los trabajadores cuando estas tecnologías se aplican en el ámbito laboral. Relevante en el caso de estudio por sus apartados de su sección sobre transparencia, gestión de riesgos y explicabilidad. Este estándar puede servir como referencia para el desarrollo de futuras regulaciones más específicas en la supervisión de sistemas de reconocimiento de emociones en el entorno de trabajo.

Por último, el desarrollo de estándares técnicos debe ser un proceso inclusivo, que cuente con la participación activa de múltiples actores, incluidos reguladores, empresas, expertos en IA, sindicatos y organizaciones de la sociedad civil.

> El desarrollo inclusivo y la diversidad son aspectos clave para potenciar el impacto positivo de la Inteligencia Artificial (IA) en la sociedad. Las distintas perspectivas y la aplicación de metodologías con equipos multidisciplinares, que incluyan una visión ética y social, determinarán un sistema de IA responsable, justo y equitativo.[106]

La colaboración en este ámbito asegura que los estándares reflejen un equilibrio entre las necesidades de la industria y los derechos de los trabajadores, promoviendo un uso responsable de los sistemas de reconocimiento de emociones en el entorno laboral.

En definitiva, los estándares técnicos internacionales pueden actuar como un **puente entre la innovación y la regulación**, permitiendo que los sistemas de reconocimiento de emociones se integren en el entorno laboral de forma ética, transparente y conforme a principios de justicia, seguridad y respeto por los derechos humanos.

---

[105] IEEE. (2024). *IEEE 7014-2024: Standard for Ethical Considerations in Emulated Empathy in Autonomous and Intelligent Systems*. Institute of Electrical and Electronics Engineers.
[106] *Ciberespiral. (2023). Desarrollo inclusivo y diversidad en la inteligencia artificial. Recuperado de https://ciberespiral.org/es/desarrollo-inclusivo-y-diversidad-en-la-inteligencia-artificial/*

5. INCENTIVOS PARA LA ADOPCIÓN DE BUENAS PRÁCTICAS

La implementación de incentivos específicos para fomentar la adopción de buenas prácticas en el uso de sistemas de reconocimiento de emociones en el ámbito laboral puede ser una estrategia útil de cara a promover un desarrollo ético y responsable de estas tecnologías. Aunque el mecanismo más habitualmente utilizado en España para promover el cumplimiento regulatorio es el de las sanciones, la realidad es que, en un contexto tan cambiante como el de la IA, los incentivos pueden ser de mayor utilidad a la hora de promover un comportamiento ético y responsable por parte de los empleadores.

En línea con la estrategia de incentivos, la administración Biden estableció un marco que vinculaba la contratación pública federal con el cumplimiento de estándares éticos y de seguridad en el desarrollo de inteligencia artificial. Según esta orden ejecutiva, firmada en octubre de 2023, las empresas que deseen trabajar con el gobierno federal deben demostrar que cumplen con criterios estrictos relacionados con la transparencia, la ciberseguridad y la evaluación de riesgos asociados a la IA. Este mecanismo no solo prioriza a las organizaciones que adoptan buenas prácticas, sino que también promueve un mercado más responsable al incentivar a las empresas a adherirse a estándares elevados como condición para acceder a contratos gubernamentales. Este enfoque subraya cómo los incentivos pueden ser una herramienta poderosa para fomentar la innovación ética en sectores estratégicos[107][108].

Estos incentivos pueden tomar diversas formas, desde beneficios fiscales hasta reconocimientos públicos, y tendrían como objetivo recompensar a las empresas que lideren con el ejemplo en la aplicación de estándares técnicos, mecanismos de autorregulación y medidas de transparencia.

Uno de los incentivos más efectivos es el establecimiento de ventajas fiscales para las empresas que demuestren cumplir con estándares de calidad en el diseño e implementación de sistemas de IA. Por ejemplo, aquellas organizaciones que integren auditorías externas, sistemas de evaluación de impacto y medidas de protección de datos biométricos podrían acceder a reducciones impositivas o a programas de financiación pública. Estos beneficios no solo

[107]El Confidencial. (2023). *Biden firma una orden para controlar la inteligencia artificial*. Recuperado de https://www.elconfidencial.com/mundo/2023-10-30/biden-firma-orden-controlar-inteligencia-artificial_3764864
[108] Wired. (2023). *Biden's executive order on cybersecurity, AI, and more*. Recuperado de https://www.wired.com/story/biden-executive-order-cybersecurity-ai-and-more

refuerzan el compromiso de las empresas con el cumplimiento normativo, sino que también generan un atractivo económico que incentiva a otras organizaciones a seguir el mismo camino.

Además de los incentivos fiscales, la creación de sellos de calidad o certificaciones específicas para empresas que implementen buenas prácticas representa una herramienta poderosa para destacar su compromiso ético y diferenciarse en el mercado[109]. Estos reconocimientos, otorgados por organismos reguladores o entidades independientes, no solo mejoran la reputación corporativa, sino que también incrementan la confianza de los trabajadores, consumidores y socios comerciales en el uso de estas tecnologías. [110] Un sello de calidad podría, por ejemplo, certificar que los sistemas utilizados por la empresa son transparentes, equitativos y respetan los derechos fundamentales de los empleados.

Otro mecanismo de incentivo es el acceso prioritario a programas de apoyo gubernamental o colaboraciones público-privadas. Las empresas que lideren en la adopción de buenas prácticas podrían beneficiarse de fondos específicos destinados al desarrollo tecnológico responsable o ser consideradas como socios preferentes en proyectos piloto supervisados por las administraciones públicas. Este tipo de reconocimiento práctico refuerza la competitividad de las organizaciones que actúan de manera ética, al tiempo que establece un estándar aspiracional para el resto del mercado.

Por supuesto, estos incentivos deberían ir acompañados de campañas de sensibilización, formación y divulgación de buenas prácticas. Dar visibilidad a casos de éxito y mostrar los beneficios concretos de adoptar un enfoque ético en el desarrollo de estas tecnologías puede animar a más empresas a seguir este camino.

Los incentivos para la adopción de buenas prácticas son una herramienta esencial para consolidar un marco de seguridad jurídica y equidad en el uso de sistemas de reconocimiento de emociones. Premiar a quienes lideran con responsabilidad no solo refuerza la seguridad

---

[109]*Cadena SER. (2024). La empresa albaceteña Grupo Tecon obtiene la prestigiosa Certificación de Ciberseguridad EMMA/OpenNAC. Recuperado de https://cadenaser.com/castillalamancha/2024/09/27/la-empresa-albacetena-grupo-tecon-obtiene-la-prestigiosa-certificacion-de-ciberseguridad-emma-opennac-radio-albacete/*

[110]*Industrial Mindset. (2024.). Cómo ISO 45001 mejora la reputación corporativa y la confianza de los stakeholders. Recuperado de https://industrialmindset.com/22-como-iso-45001-mejora-la-reputacion-corporativa-y-la-confianza-de-los-stakeholders/*

jurídica y el respeto a los derechos fundamentales, sino que también impulsa una cultura de innovación sostenible y confiable.

CAPÍTULO VIII: NOVEDADES LEGISLATIVAS

El Gobierno de España ha aprobado el martes 11 de marzo de 2025 un anteproyecto de ley para el uso adecuado de la inteligencia artificial (IA), alineándose con el Reglamento Europeo de IA. Esta normativa introduce medidas relevantes para el reconocimiento de emociones y el uso de datos biométricos. Se procede a mencionar los cambios que tendrían un efecto en el objeto de estudio de este trabajo:[111]

1. Se prohíbe el uso de IA para identificar biométricamente a personas en lugares públicos, salvo excepciones para casos específicos bajo control de las fuerzas de seguridad, como investigaciones de redes de trata.
2. Sanciones: Para IA de alto riesgo: Multas de hasta 7,5 millones de euros o entre el 1% y 2% del volumen mundial de negocio de la empresa infractora.
3. Supervisión y control: La Agencia Española de Protección de Datos (AEPD) se encargará específicamente de la regulación del uso de datos biométricos.

"El Consejo de Ministros enviará la norma al Congreso donde empezará el proceso parlamentario habitual para ser tramitada como un proyecto de ley."[112]

CONCLUSIÓN

Trabajar en este TFG me ha hecho ver que la tecnología avanza más rápido que el derecho, pero también que el derecho tiene la capacidad, y la responsabilidad, de marcar los límites del juego. Los sistemas de reconocimiento de emociones en el entorno laboral no son meras herramientas de eficiencia: tocan fibras sensibles como la privacidad, la dignidad o la salud mental de quienes trabajan. Y aunque su uso está mayoritariamente prohibido en el Reglamento Europeo de IA, existen excepciones, por motivos médicos o de seguridad, que, si no se regulan con precisión, pueden abrir la puerta a usos poco controlados.

---

[111]Díaz, M. (2025, 11 de marzo). *El proyecto de ley para adaptar el reglamento europeo de la IA*. Newtral. Recuperado de https://www.newtral.es/reglamento-ia-inteligencia-artificial-gobiern/20250311/?amp
[112]Díaz, M. (2025, 11 de marzo). *El proyecto de ley para adaptar el reglamento europeo de la IA*. Newtral. Recuperado de https://www.newtral.es/reglamento-ia-inteligencia-artificial-gobiern/20250311/?amp

A lo largo del trabajo he analizado el funcionamiento técnico y los posibles beneficios de estos sistemas, pero también he puesto el foco en sus riesgos éticos, jurídicos y prácticos. He examinado su encaje dentro del Reglamento de IA, el RGPD, la legislación laboral española y la normativa de prevención de riesgos, identificando tanto los vacíos legales como las tensiones que generan. Además, he planteado propuestas para mejorar la seguridad jurídica: desde una regulación más clara y sectorial, hasta el refuerzo de mecanismos de control como la negociación colectiva, la supervisión humana efectiva, la emisión de circulares vinculantes por parte de la AEPD, el impulso de códigos de conducta empresariales y la corregulación a través de acuerdos sectoriales. Todas estas medidas apuntan a un mismo objetivo: garantizar que, si estas tecnologías llegan a utilizarse, lo hagan dentro de unos límites bien definidos, con transparencia y pleno respeto a los derechos de las personas trabajadoras.

No se trata de estar a favor o en contra de la tecnología, sino de decidir con sentido y con garantías cómo, cuándo y para qué se puede utilizar. La inteligencia artificial puede tener un papel positivo en el ámbito laboral, pero solo si la persona, y no el algoritmo, sigue estando en el centro.

BIBLIOGRAFÍA

- Abriendo Mercados. (2023). Importancia de armonizar normas y regulaciones en el comercio exterior. Recuperado de https://abriendomercados.com/importancia-de-armonizar-normas-y-regulaciones-en-el-comercio-exterior/
- Agencia Española de Protección de Datos (AEPD). (2021). Guía sobre la protección de datos en las relaciones laborales. https://www.aepd.es/sites/default/files/2021-10/guia-proteccion-datos-relaciones-laborales.pdf
- Agencia Española de Protección de Datos (AEPD). (2023). Guía sobre protección de datos y relaciones laborales. Agencia Española de Protección de Datos. Disponible en: https://www.aepd.es/es/documento/guia-proteccion-datos-relaciones-laborales.pdf
- Agencia Española de Protección de Datos (AEPD). (2023). Guía sobre protección de datos y relaciones laborales. Agencia Española de Protección de Datos. Disponible en: https://www.aepd.es/es/documento/guia-proteccion-datos-relaciones-laborales.pdf
- Agencia Española de Protección de Datos (AEPD). (2024). ¿Cuál es el ámbito de aplicación del RGPD? Recuperado de https://www.aepd.es/preguntas-frecuentes/2-rgpd/1-de-aplicacion/FAQ-0202-cual-es-el-ambito-de-aplicacion-del-rgpd
- Agencia Española de Protección de Datos (AEPD). (2024). Ejerce tus derechos. AEPD. https://www.aepd.es/derechos-y-deberes/ejerce-tus-derechos
- Arena. (2024). ¿Cuáles son los 7 principios del RGPD? Recuperado de https://www.liberties.eu/es/stories/cuales-son-los-7-principios-del-rgpd/44265
- Ático, G. (2024, 28 noviembre). Reconocimiento de emociones y protección de datos ¿Cómo se relacionan? Grupo Atico34. https://protecciondatos-lopd.com/empresas/reconocimiento-emociones/
- Audidat. (2024). Reconocimiento de emociones y protección de datos. Audidat. https://www.audidat.com/blog/proteccion-de-datos/reconocimiento-de-emociones-y-proteccion-de-datos/
- Autocontrol. (2021, 14 de octubre). La Dirección General del Juego y AUTOCONTROL firman un convenio de corregulación sobre publicidad del juego. https://www.autocontrol.es/2021/10/14/direccion-general-del-juego-y-autocontrol-convenio-corregulacion-publicidad-juego/
- Barona. (2024). Título del artículo. Actualidad Jurídica Iberoamericana, 21, 298-331.

- Boletín Oficial del Estado [BOE]. (2018). Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Recuperado de https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf
- Business Insider España. (2018, 30 abril). Así vigilan las empresas chinas las emociones de sus empleados con esta tecnología militar. https://www.businessinsider.es/empresas-chinas-vigilan-emociones-empleados-tecnologia-militar-402197
- Cadena SER. (2024). La empresa albaceteña Grupo Tecon obtiene la prestigiosa Certificación de Ciberseguridad EMMA/OpenNAC. Recuperado de https://cadenaser.com/castillalamancha/2024/09/27/la-empresa-albacetena-grupo-tecon-obtiene-la-prestigiosa-certificacion-de-ciberseguridad-emma-opennac-radio-albacete/
- Centro de Documentación Europea - Universidad de Granada. (2024, 12 de marzo). Más de 100 empresas firman los compromisos del Pacto sobre la IA de la UE para impulsar un desarrollo fiable y seguro. https://cde.ugr.es/index.php/union-europea/noticias-ue/1858-mas-de-100-empresas-firman-los-compromisos-del-pacto-sobre-la-ia-de-la-ue-para-impulsar-un-desarrollo-fiable-y-seguro
- CEPD-SEPD. Dictamen conjunto 5/2021 sobre Ley de Inteligencia Artificial, 18 de junio de 2021.
- Chen, J., Yan, M., Zhao, J., & Wang, Y. (2023). Ethical Challenges of AI Bias in Workforce Management. arXiv preprint. Recuperado de https://arxiv.org/abs/2309.10780
- Ciberespiral. (2023). Desarrollo inclusivo y diversidad en la inteligencia artificial. Recuperado de https://ciberespiral.org/es/desarrollo-inclusivo-y-diversidad-en-la-inteligencia-artificial/
- Comisión de las Comunidades Europeas. (2004). Libro Verde sobre la Colaboración Público-Privada y el Derecho Comunitario de Contratación Pública y Concesiones. Recuperado de https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX%3A52004DC0327
- CCOO y UGT. (2023). Acuerdo colectivo de trabajo con Just Eat España. https://www.ccoo-servicios.es/archivos/Acuerdo%20Sindicatos%20JUST%20EAT(1).pdf
- Datos.gob.es. (2024). Inteligencia artificial para mejorar la interoperabilidad en el sector público europeo. Recuperado de https://datos.gob.es/es/blog/inteligencia-artificial-para-mejorar-la-interoperabilidad-en-el-sector-publico-europeo

- Díaz, M. (2025, 11 de marzo). El proyecto de ley para adaptar el reglamento europeo de la IA. Newtral. Recuperado dehttps://www.newtral.es/reglamento-ia-inteligencia-artificial-gobiern/20250311/?amp
- Edwards, L., & Veale, M. (2017). Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For. Duke Law & Technology Review, 16(1).
- El Confidencial. (2023). Biden firma una orden para controlar la inteligencia artificial. Recuperado de https://www.elconfidencial.com/mundo/2023-10-30/biden-firma-orden-controlar-inteligencia-artificial_3764864
- El Periódico. "Cárceles de Cataluña: Inteligencia Artificial para el control de presos." 20 de septiembre de 2023.
- El Foro de Labos. (2022, 4 mayo). ¿Es legítimo el reconocimiento de emociones en el entorno laboral? El Foro de Labos. Recuperado de https://www.elforodelabos.es/2022/05/derecho-a-la-desconexion-digital-comentario-a-la-stsj-de-madrid-de-21-2-2022/
- El Foro de Labos (2023). "No digas ni mu: el Tribunal de la UE deniega la transparencia del reconocimiento de emociones". Disponible en: https://www.elforodelabos.es/2023/09/no-digas-ni-mu-el-tribunal-de-la-ue-deniega-la-transparencia-del-reconocimiento-de-emociones/.
- European Commission. (2020). White Paper on Artificial Intelligence: A European approach to excellence and trust.
- Federación de Servicios Financieros y Administrativos de CCOO. (2021). Convenio colectivo del sector bancario 2021. Art 80.5. https://www.ccoo-servicios.es/archivos/financiero/Convenio-Banca-2021.pdf
- FSC-CCOO. (2024). CCOO, UGT y FETICO firman con Just Eat España un nuevo acuerdo que lidera el diálogo social en el sector de las plataformas de delivery. Recuperado de https://fsc.ccoo.es/noticia:715603--CCOO_UGT_y_FETICO_firman_con_Just_Eat_Espana_un_nuevo_acuerdo_que_lidera_el_dialogo_social_en_el_sector_de_las_plataformas_de_delivery&opc_id=6a5018a39e084efa266aa087e2cc86d0
- García, A. (2024). Los derechos ante los sistemas biométricos que incorporan inteligencia artificial. Recuperado de archivo local.
- Garriga Domínguez, A. (2024). "Los derechos ante los sistemas biométricos que incorporan Inteligencia Artificial." Derechos y Libertades, 51, 117-149.

- GlobalSTD. (s.f.). La salud mental en los espacios de trabajo: ISO 45003. Recuperado de https://www.globalstd.com/blog/salud-mental-en-los-espacios-de-trabajo-iso-45003/
- Grupo Adaptalia. (2024). Principios de la protección de datos. Recuperado de https://grupoadaptalia.es/blog/principios-de-la-proteccion-de-datos/#:~:text=Los%20principios%20protecci%C3%B3n%20de%20datos,y%20(vii)%20responsabilidad%20Proactiva
- Grupo Atico 34 (2023). "Reconocimiento de emociones: riesgos y normativa". Disponible en: https://protecciondatos-lopd.com/empresas/reconocimiento-emociones/.
- Grupo Ático34. (s.f.). Principio de proporcionalidad en protección de datos. Protección de Datos LOPD. https://protecciondatos-lopd.com/empresas/principio-proporcionalidad/
- iBorderCtrl. (2024). iBorderCtrl automates discrimination. Recuperado de https://iborderctrl.no/blog:iborderctrl_automates_discrimination#:~:text=fund%20iBorderCtrl%20to%20the%20tune,components%E2%80%94that%20make%20automated%20discrimination%20likely
- Industrial Mindset. (2024). Cómo ISO 45001 mejora la reputación corporativa y la confianza de los stakeholders. Recuperado de https://industrialmindset.com/22-como-iso-45001-mejora-la-reputacion-corporativa-y-la-confianza-de-los-stakeholders/
- International Telecommunication Union (ITU).(2025). AI for Good. Recuperado de https://www.itu.int/
- Inneara. (2024). Proyectos de colaboración público-privada. Recuperado de https://www.inneara.com/proyectos-colaboracion-publico-privada/?t&utm_source=perplexity
- Agencia Española de Protección de Datos. (2023, 25 de septiembre). *Inteligencia artificial: Transparencia.* https://www.aepd.es/prensa-y-comunicacion/blog/inteligencia-artificial-transparencia
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Boletín Oficial del Estado, núm. 294, de 6 de diciembre de 2018. https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673
- Ley 7/2021, de 20 de mayo, de cambio climático y transición energética, Boletín Oficial del Estado, núm. 121, de 21 de mayo de 2021.
- Maldita.es. (9 de abril de 2024). ¿Son nuestras emociones datos personales? Qué dice la ley de protección de datos sobre el reconocimiento de emociones y el análisis de sentimientos con IA. Maldita Tecnología. Recuperado de https://maldita.es/malditatecnologia/20240409/emociones-datos-personales-protegidos/

- Mariscal & Abogados. (n.d.). Códigos de conducta empresariales. Recuperado de https://www.mariscal-abogados.es/codigos-de-conducta-empresariales
- Mia Meraki. (n.d.). Entorno laboral y salud mental: Soluciones de IA. Recuperado de https://miameraki.com/blog/entorno-laboral-y-salud-mental-soluciones-de-ia/?utm_source=chatgpt.com
- Moneda Única. (2022). El Foro de Empresas por Madrid es un ejemplo de colaboración público-privada. Recuperado de https://www.monedaunica.net/2022/01/el-foro-de-empresas-por-madrid-es-un-ejemplo-de-colaboracion-publico-privada/?t&utm_source=perplexity
- Monereo, J.L. (2022). La vigilancia digital y el control empresarial: límites derivados del principio de proporcionalidad. Revista de Jurisprudencia Laboral, (4). Recuperado de https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-L-2022-00000001819
- Morote. (2024). Unión Europea: Robots con inteligencia artificial como agentes fronterizos. Recuperado de https://tec.com.pe/union-europea-robots-inteligencia-artificial-agentes-fronterizos/#:~:text=Esta%20Inteligencia%20Artificial%20se%20encargar%C3%A1,como%20cualquier%20otro%20oficial%20humano
- OSHA-EU. Impact of Artificial Intelligence on Occupational Safety and Health, 2021.
- Ohm, P., & Lehr, D. (2017). Playing with the Data: What Legal Scholars Should Learn about Machine Learning. UC Davis Law Review, 51(2), 655 y ss. Recuperado de UC Davis Law Review
- Obregón Fernández, A., & Lazcoz Moratinos, G. (2024). La supervisión humana de los sistemas de inteligencia artificial de alto riesgo. Aportaciones desde el derecho internacional humanitario y el derecho de la Unión Europea. Dialnet.
- Organización Internacional del Trabajo. (2018). Informe sobre el diálogo social y las normas internacionales del trabajo. Recuperado de https://www.ilo.org/sites/default/files/wcmsp5/groups/public/%40ed_norm/%40relconf/documents/meetingdocument/wcms_672978.pdf
- Ramón y Cajal Abogados. (2024). Regulación de los sistemas de IA de alto riesgo en el Reglamento de Inteligencia Artificial. https://www.ramonycajalabogados.com/es/noticias/regulacion-de-los-sistemas-de-ia-de-alto-riesgo-en-el-reglamento-de-inteligencia-artificial

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), Diario Oficial de la Unión Europea, L 119.
- Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, Boletín Oficial del Estado, núm. 260, de 30 de octubre de 2007.
- Real Decreto Legislativo 5/2000, de 4 de agosto, por el que se aprueba el texto refundido de la Ley sobre Infracciones y Sanciones en el Orden Social, Boletín Oficial del Estado, núm. 189, de 8 de agosto de 2000.
- Real Decreto 1393/2007, de 29 de octubre, por el que se establece la ordenación de las enseñanzas universitarias oficiales, Boletín Oficial del Estado, núm. 260, de 30 de octubre de 2007.
- Rodríguez Escanciano, S. (2024). El principio de proporcionalidad como exigencia de la videovigilancia en el marco empresarial. Revista de Jurisprudencia Laboral, (6). Recuperado de https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-L-2024-00000002603
- RRHH Press. (2019). Ifeel lanza una herramienta basada en inteligencia artificial para medir el clima laboral. Recuperado de https://www.rrhhpress.com/zona-tech/47593-ifeel-lanza-una-herramienta-basada-en-inteligencia-artificial-para-medir-el-clima-laboral?utm_source=chatgpt.com
- Sanz, F. (2021, 12 de noviembre). Inteligencia artificial, algoritmos y derecho de información de la representación legal de los trabajadores. Legal Today. Recuperado de https://www.legaltoday.com/practica-juridica/derecho-social-laboral/laboral/inteligencia-artificial-algoritmos-y-derecho-de-informacion-de-la-representacion-legal-de-los-trabajadores-2021-11-12/
- Santos Santana, D. (2018). Derechos de información y consulta de los trabajadores. Universidad de Valladolid. UVaDOC. https://uvadoc.uva.es/bitstream/handle/10324/31718/TFG-D_0621.pdf?sequence=1

- Sheridan. (1995). Human-Centered Automation: Oxymoron or Common Sense?. IEEE International Conference on Systems, Man and Cybernetics, pp. 823–828. https://doi.org/10.1109/ICSMC.1995.537867
- Tribunal Constitucional. (2000). Sentencia 292/2000, de 30 de noviembre de 2000.
- Tribunal Constitucional. (2016). Sentencia 39/2016, de 3 de marzo de 2016.
- Tribunal de Justicia de la Unión Europea (TJUE). (2023). Sentencia de 30 de marzo de 2023, F.F. contra Data Protection Commissioner, C-34/21, EU:C:2023:250.
- UGT. (2024). Guía web negociación. Recuperado de https://www.ugt.es/sites/default/files/guiawebnegociacion.pdf
- Unión Europea. (2024). 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 se modifican determinados actos legislativos de la Unión. Diario Oficial de la Unión Europea, L, 168/1. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32024R1689
- Unión Europea. (2024). Reglamento (UE) 2024/XX del Parlamento Europeo y del Consejo de 29 de abril de 2024 relativo a la inteligencia artificial y por el que se establecen disposiciones sobre transparencia, derechos fundamentales y supervisión. Diario Oficial de la Unión Europea.
- Wired. (2023). Biden's executive order on cybersecurity, AI, and more. Recuperado de https://www.wired.com/story/biden-executive-order-cybersecurity-ai-and-more

ANEXO: ESTUDIO DE UN CASO PRÁCTICO

03:12 a.m. – Daniel avanzaba por el pasillo entre los almacenes con la linterna en una mano y la radio en la otra. Era su tercera ronda de la noche, y aunque todo parecía en calma, un ligero cosquilleo en la nuca le decía que algo no estaba bien. No veía nada, no oía nada, pero algo no encajaba.

Al llegar a la zona de carga, notó una puerta entreabierta. Normalmente, ese acceso siempre estaba cerrado. Quizás alguien la había dejado mal cerrada, o quizás… no estaba solo.

03:14 a.m. – Dio un paso adelante con cautela, forzándose a respirar con normalidad. El silencio era absoluto. Fue entonces cuando un ruido metálico resonó a su izquierda. Giró la linterna justo a tiempo para ver una sombra moverse entre las cajas.

03:15 a.m. – "Aquí Seguridad 3, posible intrusión en el almacén." Apenas pudo terminar de hablar cuando una fuerza brutal lo empujó contra las estanterías. Un segundo asaltante salió de la oscuridad, y antes de que pudiera reaccionar, sintió el impacto de un golpe en el costado.

Intentó soltarse, pero dos contra uno no era una pelea justa. Recibió un puñetazo en la mandíbula, lo suficiente para hacerlo perder el equilibrio. La patrulla tardaría al menos cinco minutos en llegar. Para cuando su compañero lo encontró, los ladrones ya se habían ido, y Daniel estaba en el suelo, aturdido y con la ceja abierta.

En situaciones donde cada segunda cuenta, un sistema de IA no reemplaza el instinto humano, pero sí lo refuerza, permitiendo actuar antes de que el peligro sea inevitable. Si un sistema de reconocimiento de emociones hubiese estado operativo, podría haber detectado los primeros signos de alerta en Daniel mucho antes del enfrentamiento:

- Su frecuencia cardíaca y microexpresiones de estrés y miedo al percibir la puerta entreabierta habrían activado una alerta temprana en la central de seguridad.
- El análisis de su respiración y tensión muscular al escuchar el ruido habría identificado un estado de amenaza inminente.
- Antes del ataque, la IA habría solicitado refuerzos automáticamente, o al menos dado una prealerta, reduciendo el tiempo de respuesta y evitando que Daniel enfrentara el peligro solo.

Contexto del Caso

La empresa ProSegura S.L. es una compañía especializada en seguridad privada y gestión de riesgos corporativos. Su principal actividad es la protección de infraestructuras críticas, como aeropuertos, bancos y centros de datos. La empresa emplea a más de 3.000 vigilantes de seguridad, muchos de los cuales trabajan en situaciones de alta tensión, como la vigilancia de accesos sensibles o la supervisión de zonas con riesgo de ataques o incidentes violentos.

Debido al estrés y la fatiga que enfrentan sus empleados, ProSegura ha identificado un incremento del 20% en los errores de seguridad, un aumento del 35% en bajas médicas por trastornos emocionales y estrés agudo derivado del trato con clientes que deriva en respuestas emocionales inapropiada**s** en situaciones de crisis. Ante esta situación, la dirección ha decidido explorar la implantación de un sistema de reconocimiento de emociones para detectar signos tempranos de estrés, ansiedad, desmotivación, apatía, ira o agresividad entre otras en los vigilantes y prevenir riesgos laborales.

Paso 1: Justificación Legal para la Implementación del Sistema

- Objetivo principal: Reducir errores de seguridad provocados por ansiedad, estrés extremo, reacciones de pánico… en vigilantes de seguridad.
- Justificación bajo el Reglamento de IA (RIA): El sistema se implantaría bajo la excepción de motivos de seguridad (art. 5.1(f) del RIA), ya que su finalidad es proteger la integridad física de los empleados y del público.
- Base jurídica en el RGPD: Se fundamenta en la licitud del tratamiento al cumplir obligaciones de seguridad laboral (art. 6.1.c RGPD y 9.2 b. RGPD) y prevención de riesgos laborales (art. 14 de la Ley de Prevención de Riesgos Laborales, LPRL).
- Test de Proporcionalidad:

  Es necesario: No existen alternativas menos invasivas que permitan detectar en tiempo real emociones críticas que pueden comprometer la seguridad en situaciones de crisis, de forma tan efectiva como lo hace un sistema de IA. Métodos tradicionales como la formación en gestión emocional, las evaluaciones psicológicas periódicas o la supervisión hermana pueden ser útiles para la prevención a largo plazo, pero no garantizan una intervención inmediata cuando un vigilante experimenta un estado emocional que afecta su capacidad de respuesta.

Es idóneo (juicio de adecuación): El sistema es adecuado para el objetivo de prevenir fallos de seguridad en situaciones críticas. Detectar emociones como miedo, pánico, ira o confusión en tiempo real permite a los supervisores actuar preventivamente, evitando reacciones impulsivas o bloqueos que pongan en riesgo a los empleados o al público. Los estados emocionales pueden cambiar en segundos y cualquier retraso en su identificación podría acarrear consecuencias graves. En este caso, la restricción del derecho a la privacidad se justifica porque su utilidad es real y directamente vinculada con la protección de la seguridad.

Es limitado y garantista: Se han implementado medidas estrictas para minimizar el impacto en la privacidad y evitar el uso indebido del sistema. "*el empresario tendrá que restringir el tratamiento de los datos de sus empleados, manejando los estrictamente necesarios por el tiempo imprescindible*"[113]

El reconocimiento de emociones solo se activa en momentos de alto riesgo, no se utiliza para evaluación de desempeño ni sanciones disciplinarias, quedando así fuera de la controversia jurisprudencial que analiza si la video vigilancia de los trabajadores está justificada y como esto lo modula la existencia o no un carácter sancionador o el nivel de transparencia (STS de 7 de julio de 2016, rec. 3233/2014, TS en fecha 31 de enero de 2017, recurso 3331/2015, TS de 21 de julio de 2021, recurso 4877/2018.)[114] Los **datos generados** por el sistema no se almacenan más que el **mínimo legal de 6 meses.** [115][116] Dicho almacenamiento se realizará con las medidas de seguridad apropiadas.

Se informará al trabajador de que los sistemas están siendo utilizados de forma clara, concisa y accesible a lo largo de todo el ciclo, además, la ubicación de las cámaras respeta la intimidad del trabajador, cumpliendo con los requisitos de transparencia del

---

[113]Rodríguez Escanciano, S. (2024). *El principio de proporcionalidad como exigencia de la videovigilancia en el marco empresarial*. Revista de Jurisprudencia Laboral, (6). Recuperado de https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-L-2024-00000002603
[114]Monereo, J.L. (2022). *La vigilancia digital y el control empresarial: límites derivados del principio de proporcionalidad*. Revista de Jurisprudencia Laboral, (4). Recuperado de https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-L-2022-00000001819
[115]Unión Europea. (2024). *Reglamento (UE) 2024/1684 del Parlamento Europeo y del Consejo, de 13 de marzo de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de IA)*. Diario Oficial de la Unión Europea, L, 7.5.2024. Art 26.6.
[116]Rodríguez Escanciano, S. (2024). *El principio de proporcionalidad como exigencia de la videovigilancia en el marco empresarial*. Revista de Jurisprudencia Laboral, (6). Recuperado de https://www.boe.es/biblioteca_juridica/anuarios_derecho/articulo.php?id=ANU-L-2024-00000002603

artículo Art. 89 LOPDGDD y amparado su uso por los Art. 22.4 de la LOPDGDD, Art. 20.3 del ET y Art. 22.8 de la LOPDGDD.

Además, la empresa ha establecido un sistema de supervisión humana obligatoria para revisar cada alerta antes de tomar decisiones, se aconseja aquí al cliente colocar a una persona con las habilidades técnicas en materia de Inteligencia artificial y conocimientos algorítmicos necesarios, a pesar de no ser esto una exigencia del reglamento. Se ha negociado con los representantes de los trabajadores garantías adicionales, como la creación de un comité de seguimiento sindical.

Paso 2: Evaluación de Impacto en la Protección de Datos (EIPD)

Antes de implantar el sistema, ProSegura debe realizar una Evaluación de Impacto en la Protección de Datos (EIPD) para cumplir con el artículo 35 del RGPD ya que el sistema cumple con los tres criterios del art 35.3 RGPD Esta evaluación debe responder a:

1. Descripción del tratamiento y su finalidad
2. Evaluación de la necesidad y proporcionalidad
3. Identificación y evaluación de riesgos para los derechos y libertades de los trabajadores (Uso indebido, Posibilidad de decisiones injustificadas, falta de transparencia…)
4. Medidas para mitigar los riesgos, medidas de seguridad y cumplimiento del RGPD

¿Porqué no se realiza evaluación de impacto bajo el artículo 27 del RIA?

Esto no ocurre por no estar ProSegura incluida en la lista de responsables del despliegue que enumera este artículo, que va dirigido principalmente a organismos de derecho público o que presten servicios públicos. Se puede ver cómo el RIA exige un escalón más de garantías para estas entidades.

Paso 3: Consulta con Representantes de los Trabajadores

Antes de poner en marcha el sistema, la empresa deberá consultar a los representantes de los trabajadores conforme al artículo 33 de la LPRL.

Además, existe el deber de transparencia algorítmica del artículo 64.4 d) ET, donde se deberá trasladar "parámetros, instrucciones o reglas"[117] de estos sistemas de inteligencia artificial.

Por último, el propio reglamento de inteligencia artificial en su artículo 26.7 establece la obligación de informar *"a los representantes de los trabajadores y a los trabajadores afectados de que estarán expuestos a la utilización del sistema de IA de alto riesgo".*

Mientras que los artículos 64 y 26 hablan del deber de informar, el artículo 33 de la LPRL habla de un deber de consulta. Cabe aquí preguntarse cuál es la diferencia entre ambos.

"El artículo 2 de la Directiva 2002/14/CE expone una serie de conceptos, llamando la atención la aportación del concepto de información y consulta, ya que para que sea un derecho efectivo debemos conocer previamente en qué consiste esa información y esa consulta. El precepto establece que se entiende por ***información*** *la "transmisión de datos por el empresario a los representantes de los trabajadores para que pueden tener conocimiento del tema tratado y examinarlo". Y seguidamente se establece la* ***consulta*** *como "el intercambio de opiniones y la apertura de un diálogo entre los representantes de los trabajadores y el empresario".*"[118]

La trasposición de la normativa internacional exige que al hablar de consulta se "*deberán incluir, en su caso, la emisión de informe previo".* [119]

Paso 4: Implementación Técnica con Garantías[120]

Para cumplir con la normativa, la empresa debe adoptar medidas adicionales:

- Adoptar medidas técnicas y organizativas adecuadas para garantizar que los sistemas se utilicen de acuerdo con las instrucciones proporcionadas. (26.1 RIA)

[117]Sanz, F. (2021, 12 de noviembre). *Inteligencia artificial, algoritmos y derecho de información de la representación legal de los trabajadores*. Legal Today. Recuperado de https://www.legaltoday.com/practica-juridica/derecho-social-laboral/laboral/inteligencia-artificial-algoritmos-y-derecho-de-informacion-de-la-representacion-legal-de-los-trabajadores-2021-11-12/
[118]Santos Santana, D. (2018). *Derechos de información y consulta de los trabajadores*.Universidad de Valladolid. UVaDOC. https://uvadoc.uva.es/bitstream/handle/10324/31718/TFG-D_0621.pdf?sequence=1
[119]Santos Santana, D. (2018). *Derechos de información y consulta de los trabajadores*.Universidad de Valladolid. UVaDOC. https://uvadoc.uva.es/bitstream/handle/10324/31718/TFG-D_0621.pdf?sequence=1
[120]Ramón y Cajal Abogados. (2024). *Regulación de los sistemas de IA de alto riesgo en el Reglamento de Inteligencia Artificial*. https://www.ramonycajalabogados.com/es/noticias/regulacion-de-los-sistemas-de-ia-de-alto-riesgo-en-el-reglamento-de-inteligencia-artificial

- Supervisión humana (art. 26.2 RIA): Se designa un responsable de IA que verificará alertas y evitará falsos positivos a una persona física que tenga la competencia, la formación y la autoridad necesarias.
- Asegurar que los datos de entrada sean pertinentes y suficientemente representativos en vista de la finalidad prevista del sistema (art. 26.4 RIA)
- Vigilar el funcionamiento del sistema de IA de alto riesgo, basándose en las instrucciones de uso (art. 26.5 RIA). Esta obligación puede implicar informar a los proveedores, importadores, distribuidores y autoridades competentes e, incluso, suspender el uso del sistema.
- Conservar registros generados automáticamente por los sistemas (art. 26.6 RIA).
- Informarán a los representantes de los trabajadores y a los trabajadores afectados de que estarán expuestos a la utilización del sistema de IA de alto riesgo.