Índice Propuesto

1. **Introducción**
    - Contexto sobre el uso de IA y los sistemas de reconocimiento de emociones.
    - Justificación del tema y relevancia del TFG.
    - Objetivo del TFG
2. **Sistemas de reconocimiento de emociones en el ámbito laboral**
    - Definición y funcionamiento de estos sistemas.
    - Aplicaciones actuales en diferentes sectores.
3. **Riesgos inherentes en el uso de sistemas de reconocimiento de emociones**
    - Falta de fiabilidad en la interpretación emocional.
    - Sesgos algorítmicos y discriminación.
    - Impacto en la privacidad, proporcionalidad y consentimiento.
4. **El Reglamento de IA de 2024: Análisis de las excepciones**
    - Trato que reciben en el reglamento
    - Prohibiciones explícitas y actividades relacionadas
    - Prohibiciones generales y excepciones permitidas.
    - Análisis de lagunas y áreas poco definidas en el reglamento.
    - Evaluación de sectores donde estos sistemas podrían tener cabida en el futuro.
5. **RGDPR**
6. **Legislación laboral (Estatuto de los trabajadores y derecho laboral en general).**
7. **Aplicación práctica en el ámbito Español**
    - Criterio de la agencia española de protección de datos
    - Ministerio de trabajo?
    - Convenio colectivo
8. **Posibles propuestas de desarrollo legislativo y mejora de la seguridad jurídica**
    - Autorregulación mediante códigos de conducta empresariales
    - Corregulación a través de acuerdos sectoriales
    - Colaboración público-privada en el diseño de políticas
    - Desarrollo de estándares técnicos internacionales
    - **Procedimientos normalizados para evaluación y supervisión FALTA**
9. **Conclusiones**
    - Resumen de los principales aportes del TFG.
    -
10. **Bibliografía**

1- Introducción

2- Sistemas de reconocimiento de emociones en el ámbito laboral

Definición y funcionamiento de estos sistemas

[incluir definición previa de emociones? página 88 identifica 4 estados]

Se define el sistema de reconocimiento de emociones como un sistema de IA destinado a distinguir o inferir las emociones o las intenciones de las personas físicas a partir de sus datos biométricos (artículo 3 (39) RIA). Los sistemas de reconocimiento de emociones son tecnologías basadas en inteligencia artificial que analizan señales biométricas y de comportamiento para inferir en 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 establece el reglamento, los sistemas de reconocimiento de emociones son un sistema de inteligencia artificial, "diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales"[3]

Como señala Ana Belén 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)."[4]

En términos operativos, su funcionamiento implica tres etapas principales:

---

[1] 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] Art 3 (1) RIA
[4] Muñoz Ruiz, A. B. (2023). *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*. Editorial Tirant lo Blanch.

1. **Captura de datos**: en el entorno laboral, los sistemas recopilan información a través de diferentes dispositivos como cámaras instaladas en espacios de trabajo, micrófonos en reuniones virtuales o sensores biométricos incorporados en wearables. Estos dispositivos registran señales físicas (gestos, expresiones faciales) y vocales (tono de voz, pausas en el habla), proporcionando datos sobre las emociones de los trabajadores. Por ejemplo, una cámara en una sala de reuniones analiza expresiones faciales para evaluar la satisfacción del equipo durante una presentación. La calidad de los datos es esencial para garantizar interpretaciones precisas, por lo que los sistemas incluyen técnicas como la detección de rostros y el filtrado de ruido ambiental.[5]
2. **Procesamiento**: la inteligencia artificial analiza las señales emocionales mediante una variedad de algoritmos avanzados, entrenados con datos específicos del contexto laboral para identificar estados como estrés, desmotivación o entusiasmo. Entre los métodos más utilizados destacan los modelos Markovianos Ocultos (HMM), que permiten identificar transiciones emocionales a lo largo del tiempo, siendo especialmente útiles en el análisis de patrones dinámicos como los cambios en expresiones faciales o en la voz. Las redes neuronales, por su parte, correlacionan características como gestos faciales, tono de voz y postura con emociones específicas en tiempo real, ofreciendo una alta precisión en escenarios complejos. También se emplean máquinas de vector soporte (SVM) para clasificar emociones a partir de datos complejos y separar categorías emocionales en un espacio de características definido. Además, los árboles de decisión construyen estructuras jerárquicas que facilitan la clasificación emocional basándose en variables observadas, mientras que las redes Bayesianas calculan probabilidades de emociones específicas en función de datos como la intensidad de la voz o expresiones particulares. Los algoritmos de votación, como el Bagging y el Boosting, combinan los resultados de múltiples clasificadores para aumentar la precisión, integrando señales provenientes de diferentes fuentes como audio y video. Los métodos no supervisados resultan especialmente útiles para identificar patrones emocionales en entornos no controlados, donde las emociones surgen de manera espontánea. Finalmente, se recurre a técnicas de fusión de información, que integran datos de diversas fuentes a nivel de características o decisiones, para mejorar significativamente la exactitud del reconocimiento emocional. Por ejemplo, un sistema puede detectar niveles elevados de estrés en un empleado al identificar patrones como ceño fruncido recurrente, tono de voz elevado y pausas irregulares en el discurso. Estas señales se procesan combinando redes neuronales y máquinas de vector soporte, lo que permite generar alertas en tiempo real. Este enfoque integral adapta los sistemas a las necesidades del entorno laboral, maximizando su fiabilidad y minimizando posibles sesgos en el análisis emocional.[6]
3. **Resultado**: los datos se traducen en conclusiones emocionales, representadas en reportes o acciones automatizadas según las configuraciones del sistema, esto resulta en diversas aplicaciones en el ámbito laboral. Permiten monitorear el estado emocional de los equipos para identificar patrones como estrés o desmotivación y actuar proactivamente, optimizar la productividad ajustando dinámicamente las condiciones de trabajo, analizar reacciones emocionales en procesos de selección y evaluación de desempeño. Además, contribuyen a prevenir riesgos laborales en tareas críticas al detectar señales de fatiga o distracción, y

---

[5] 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

[6] 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

personalizan programas de formación adaptando el contenido al estado emocional de los participantes, mejorando así el aprendizaje y el bienestar general en el entorno laboral.[7]

Es cierto que ofrecen potenciales beneficios, como la optimización de procesos laborales y la personalización de servicios, también presentan desafíos significativos relacionados con su fiabilidad, la privacidad de los datos y el consentimiento de los trabajadores.

La definición que proporciona el reglamento sobre los sistemas de reconocimiento de emociones establece: "a partir de sus datos biométricos". Cabe preguntarse, ¿Qué cualidades reúnen los datos biométricos? El artículo 3. 34) del Reglamento de Inteligencia Artificial, en virtud de la Resolución del Parlamento Europeo, de 13 de marzo de 2024, sobre la propuesta de Reglamento (P9_TA (2024)0138, dispone que son "datos biométricos", "los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos"

[apartado de definición de datos biométricos interesante incluirlo aquí y no al hablar del RGDPD]

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.

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 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.

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, el libro destaca que los costos derivados de la desmotivación y el desgaste emocional pueden ser considerables, afectando tanto al rendimiento individual como al colectivo.[8]

Gestión emocional a través de la inteligencia artificial

---

[7] 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

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

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 (*Muñoz Ruiz, 2022*).

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 formación específica, y mejorar la comunicación interna al identificar frustraciones o tensiones durante las interacciones.[9]

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.

Ejemplo de este sistema de reconocimiento de emociones fue el Proyecto iBorderCtrl que se establece en la UE para la detección de mentiras en las fronteras, en el que intervenían Luxemburgo, Chipre, Reino Unido, Polonia, España, Hungría, Alemania y Letonia[10], que provocó reacciones en contra, como el Informe de 13 de julio de 2021 de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (A9-0232/2021), que insta a la Comisión para que deje de financiar investigaciones, aplicaciones o programas biométricos que puedan concluir probablemente en una vigilancia masiva e indiscriminada en espacios públicos. El Parlamento Europeo se ha mostrado muy preocupado, especialmente por los efectos de la utilización de los sistemas de reconocimiento facial en sectores como la prevención, investigación, enjuiciamiento y ejecución en materia penal, si bien se recogen como posibles en el texto del reglamento IA. (TECNOLOGÍA BIOMÉTRICA Y DATOS BIOMÉTRICOS. BONDADES Y PELIGROS. NO TODO VALE BIOMETRIC TECHNOLOGY AND BIOMETRIC DATA. BENEFITS AND DANGERS. NOT EVERYTHING IS FAIR)

[9] Así vigilan las empresas chinas las emociones de sus empleados con esta tecnología militar." Publicado el 30 de abril de 2018.

[10]

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 (Muñoz Ruiz, Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales, citando a Business Insider, 2018).

"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' (*Business Insider*, 2018)."

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 (Muñoz Ruiz, citando Proyecto H2020 Bionic, 2022).

[leer página 98 el artículo de la cita 133, hay algún ejemplo más]

Aunque estas aplicaciones demuestran el valor potencial de la tecnología, plantean preguntas sobre la proporcionalidad de su uso y los límites éticos que deben respetarse para garantizar la protección de los derechos fundamentales de los individuos en el entorno laboral. Frente a los controles tradicionales como la videovigilancia, control de ordenadores, internet… Estos sistemas suponen una intromisión mucho más invasiva en la intimidad del empleado. Se consigue obtener un análisis profundo y asegurar la exactitud de un resultado que podría conllevar en lesiones indirectas en derechos fundamentales.

3- 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 (Muñoz Ruiz, 2023, pp. 80-85). 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[11]. Esto resulta particularmente problemático en entornos multiculturales, donde las expresiones emocionales pueden variar significativamente. La reciente sentencia del Tribunal General de la Unión Europea (2023) 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. En el caso del proyecto iBorderCtrl, se debatió la tensión entre el interés público por evaluar la fiabilidad y el impacto ético de estos sistemas 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.[12]

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 (Muñoz Ruiz, 2023, p. 83). 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 (2023), es necesario implementar estrictas medidas de proporcionalidad para garantizar que el uso de estas tecnologías no exceda su finalidad declarada.

Finalmente, es importante destacar el desafío de la transparencia. La Guía sobre la Protección de Datos en las Relaciones Laborales de la AEPD (2021) subraya que los empleados deben ser informados de manera clara sobre cómo y por qué se utilizan estas tecnologías. 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.

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

4. El Reglamento de IA de 2024: Análisis de las excepciones

1. Trato que reciben en el reglamento

El Reglamento de Inteligencia Artificial de 2024 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 derechos como la privacidad y la protección de datos personales (*RIA, artículo 5.1(f)*). A

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

[12] **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/.

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 las perspectivas laborales, los medios de subsistencia y los derechos fundamentales de los trabajadores.

Aunque el texto del reglamento 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.

2. Prohibiciones explícitas y actividades relacionadas

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 (*Reglamento Europeo de Inteligencia Artificial, artículo 5.1(f)*).

El Considerando 57 del reglamento 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"*.

A pesar de que las las actividades como contratación, selección de personal, supervisión, evaluación de rendimiento y asignación de tareas no se enumeran en una lista explícita, son interpretaciones razonables a partir del marco general de prohibiciones y riesgos identificados en el reglamento y en informes complementarios como el Dictamen conjunto del CEPD y el SEPD (2021).

- **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 la OSHA-EU (*2021*), 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 reglamento 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 responsabilidades, perpetuando desigualdades estructurales. Esta práctica no solo vulnera

derechos laborales, sino que también podría afectar la igualdad de oportunidades (*RIA, Considerando 54*).

3. Prohibiciones generales y excepciones permitidas

El Reglamento de Inteligencia Artificial de 2024 (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 (*RIA, Considerando 18*).

  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 Reglamento de IA 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 (*RIA, Considerando 18*).

  (pero podrían detectar en conductores ira, miedo de atraco + alarma , síntomas de alcohol)

  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.

  Al detectar estos patrones, el sistema sugiere 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.[13]

RRHH Press

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.[14]

Mia Meraki

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. (darle una vuelta a esta conclusión que se puede ir más allá)

- **Motivos de Seguridad:**

El RIA también permite el uso de sistemas de reconocimiento de emociones en entornos 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 (*El Periódico, 2023*).

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.

---

[13] RRHH Press. (n.d.). *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

[14] 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

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.

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, consentimiento informado y supervisión humana para minimizar riesgos y garantizar la protección de los derechos de los empleados (*RIA, artículo 26.2 y 26.7*).

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 del presente Reglamento, así como los sistemas de reconocimiento de emociones que no estén prohibidos con arreglo al presente Reglamento”.

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. (misma cita que abajo)

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.[15]

4. Análisis de lagunas y áreas poco definidas en el reglamento

A pesar de las estrictas regulaciones, el reglamento deja ciertos aspectos sin abordar con claridad, lo que genera incertidumbre sobre su implementación:

- **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.

  La inclusión de ejemplos prácticos y criterios de evaluación específicos, como un listado de indicadores emocionales relevantes o protocolos para validar su uso, podría reducir esta ambigüedad.

  (Listado de indicadores emocionales relevantes: emociones críticas en situaciones de riesgo, indicadores de estrés crónico o fatiga, señales de distracción o desmotivación)???

- **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

---

15 https://www.observatoriorh.com/opinion/los-sistemas-automatizados-de-reconocimiento-de-emociones-en-el-reglamento-ue-de-ia.html

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) 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" (Obregón Fernández & Lazcoz Moratinos, 2024, citando a Ohm & Lehr, 2017; Jones, 2017).

Como expresan Obregón Fernández y Lazcoz Moratinos, Jones (2017) 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 (Jones, 2017, p. 231-232).

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 (Obregón Fernández & Lazcoz Moratinos, 2024). 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 (Sheridan, 1995).

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 Reglamento de IA de 2024. 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 (Obregón Fernández & Lazcoz Moratinos, 2024, p. 12-13).

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

El artículo 26.5 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, pero no define qué constituye un "incidente grave". Esto podría dar lugar a interpretaciones diversas. Sin embargo, el reglamento da un paso importante al requerir la suspensión inmediata del sistema en caso de riesgos detectados.

Transparencia laboral

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 de 2024 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 (pp. 168-174). Ejemplos como 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 (Muñoz Ruiz, 2022, p. 178). Además, el nuevo artículo 2 bis del 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 (Muñoz Ruiz, 2022, pp. 179-180). Estas propuestas no sólo fortalecen el derecho a la información, sino que promueven una integración ética y transparente de la IA en el ámbito laboral.

Evaluaciones de impacto

La referencia al RGPD y la obligación de realizar evaluaciones de impacto sobre la protección de datos (artículo 26.9 del Reglamento de IA) refuerzan la coherencia normativa al alinearse con los estándares establecidos en el artículo 35.1 del RGPD. Estas evaluaciones son cruciales cuando los tratamientos de datos, especialmente mediante tecnologías avanzadas, pueden representar un alto riesgo para los derechos fundamentales. En el ámbito laboral, los sistemas de reconocimiento de emociones requieren evaluaciones de impacto particularmente detalladas, dado su uso de datos biométricos y su capacidad para influir en decisiones críticas, como la selección de personal. Tal y como señala Ana Belén Muñoz Ruiz, la AEPD establece que estas evaluaciones no solo deben analizar la proporcionalidad y necesidad del

tratamiento, sino también considerar alternativas menos invasivas que cumplan los mismos fines con menores riesgos (Muñoz Ruiz, 2022, pp. 183-184). Además, se insiste en que las evaluaciones deben abarcar tanto las consecuencias técnicas como éticas, asegurando que el diseño del algoritmo no solo sea funcional, sino también respetuoso con los derechos fundamentales de las personas trabajadoras afectadas. La falta de lineamientos específicos en el Reglamento, por ejemplo, sobre cómo evaluar la proporcionalidad en sectores como la logística o la educación, limita la efectividad de estas disposiciones, dejando un vacío normativo que podría abordarse mediante guías sectoriales más concretas (Muñoz Ruiz, 2022, p. 184).

- **Riesgos éticos y culturales:**
  Los sesgos inherentes en los algoritmos y las diferencias culturales en la expresión de emociones pueden llevar a discriminación o errores en la interpretación de los datos (*CEPD-SEPD, 2021*).

  Los sistemas de inteligencia artificial (IA) destinados al reconocimiento de emociones enfrentan desafíos significativos debido a los sesgos inherentes en los algoritmos y las diferencias culturales en la expresión emocional. "Si estos datos contienen discriminaciones, el algoritmo aprende a discriminar"[16], señala Ginès, 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 contextos multiculturales, subrayando la necesidad de desarrollar sistemas más inclusivos y equitativos.[17] El Dictamen Conjunto del Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (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.

5. Evaluación de sectores donde estos sistemas podrían tener cabida en el futuro (FALTA POR HACER)

[16] *Esade (2023). ¿Cómo pueden los algoritmos perpetuar la discriminación en el trabajo?. Recuperado de https://dobetter.esade.edu/es/algoritmos-discriminacion-trabajo*
[17] 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

5- RGDPD

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.[18]

El RGPD se sustenta en una serie de principios esenciales que orientan el tratamiento de los datos personales:[19]

- [20]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 (accountability): 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.

---

18 https://www.aepd.es/preguntas-frecuentes/2-rgpd/1-de-aplicacion/FAQ-0202-cual-es-el-ambito-de-aplicacion-del-rgpd

19 https://grupoadaptalia.es/blog/principios-de-la-proteccion-de-datos/#:~:text=Los%20principios%20protecci%C3%B3n%20de%20datos,y%20(vii)%20responsabilidad%20Proactiva.

20 https://www.liberties.eu/es/stories/cuales-son-los-7-principios-del-rgpd/44265

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.
- 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.[21]

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.[22]

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.

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.[23]

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.[24] Estas disposiciones

---

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

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

[23] 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

[24] 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.

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.[25]

En línea con el RGPD, la LOPDGDD considera los datos biométricos, como los empleados en sistemas de reconocimiento de emociones, 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.[26]

Los datos biométricos presentan características que los hacen especialmente sensibles[27]:

- Unicidad: Son exclusivos de cada individuo, lo que los convierte en una herramienta eficaz para la identificación o autentificación personal.
- Inmutabilidad: No pueden ser alterados fácilmente sin procedimientos invasivos, a diferencia de contraseñas o claves alfanuméricas.

---

[25] 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

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

[27] https://aba.org.do/articulos-perspectivas/valor-de-los-datos-biometricos-como-proteger-identidad-digital/

- 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. 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:[28]

- 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 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.[29]

---

[28] 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/

[29] https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/principios

El tratamiento de datos personales debe basarse en una base jurídica válida según lo establecido en el artículo 6 del RGPD. En el ámbito laboral, las bases más comunes son:[30]

- Cumplimiento de una obligación legal: Por ejemplo, la recopilación de datos para garantizar la seguridad laboral.
- Ejecución de un contrato: Cuando el tratamiento es necesario para la relación laboral.
- Consentimiento explícito: La validez de esta base de legitimación es muy limitada en el contexto laboral debido a la relación jerárquica entre empleador y empleado que hace que, a juicio del legislador, el consentimiento pueda no ser libremente otorgado.
- Intereses legítimos del empleador: Esta base requiere un análisis de proporcionalidad para garantizar que los derechos del trabajador no se vean comprometidos.

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:[31]

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

---

[30] Agencia Española de Protección de Datos. (2021). *La protección de datos en las relaciones laborales* (pp. 9, 74). AEPD. https://www.aepd.es/guias/la-proteccion-de-datos-en-las-relaciones-laborales.pdf

[31] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

- 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.**

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.[32]

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 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 exiga 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 teoricamente 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:

---

32 file:///C:/Users/irene/Downloads/8585-Texto%20del%20art%C3%ADculo-16293-1-10-20240610%20(1).pdf

1. El tratamiento es adecuado para alcanzar el objetivo perseguido.
2. Es necesario porque no existen medidas menos intrusivas 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. 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 económcas 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

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.[33] 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.[34]

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, 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.[35]

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.

---

[33] art 12
[34] https://www.boe.es/doue/2016/119/L00001-00088.pdf considerado 39 entre otros arts
[35] art 83,58,84…

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 recomendaciones específicas sobre el uso de tecnologías como el reconocimiento de emociones, facilitando a las empresas la adopción de buenas prácticas.[36]

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:[37]

- 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.

8. Propuestas de mejora legislativa en materia de protección de datos

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 ámbito ha evidenciado lagunas que podrían abordarse con medidas específicas para fortalecer la protección de los derechos de los trabajadores y proporcionar seguridad jurídica a las empresas.

Una primera recomendación es que la Agencia Española de Protección de Datos (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,

[36] https://www.aepd.es/la-agencia/en-que-podemos-ayudarte
[37] https://vlex.es/vid/autoridades-autonomicas-proteccion-datos-716170265

permitirían establecer directrices claras y exigibles sobre el uso de tecnologías como el reconocimiento de emociones, proporcionando un marco más sólido para su implementación.

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.

Además, sería óptimo impulsar programas de formación y sensibilización para las empresas, facilitando su comprensión de las obligaciones legales y las mejores prácticas en materia de protección de datos.

Finalmente, se debería establecer un sistema de evaluación periódica de impacto regulador, que permita adaptar las normas existentes a los avances tecnológicos y a las necesidades específicas de los sectores laborales donde estas tecnologías tienen mayor impacto. Este enfoque dinámico garantizaría que la regulación no solo sea clara y precisa, sino también flexible y capaz de responder a nuevos desafíos.

Por tanto, fortalecer el papel orientador y regulador de la AEPD mediante el uso de circulares vinculantes, el desarrollo de estándares técnicos y la promoción de mecanismos de consulta contribuiría a un marco normativo más efectivo. Estas medidas permitirían equilibrar la innovación tecnológica con la protección de los derechos de los trabajadores, promoviendo un entorno laboral más seguro y respetuoso con la privacidad.

8- Posibles propuestas de desarrollo legislativo y mejora de la seguridad jurídica

El avance en la regulación y supervisión de los sistemas de inteligencia artificial, específicamente aquellos destinados al reconocimiento de emociones en el ámbito laboral, demanda un enfoque legislativo innovador y adaptado a los retos que plantean estas tecnologías. Este apartado analiza 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.

Desde mecanismos de autorregulación, como los códigos de conducta empresariales, hasta modelos de corregulación y colaboración público-privada, las iniciativas aquí exploradas ofrecen soluciones pragmáticas y flexibles. Por otro lado, se aborda la importancia del desarrollo de estándares técnicos internacionales y la implementación de incentivos específicos para fomentar buenas prácticas, subrayando el rol de las auditorías, la transparencia y la supervisión humana como pilares esenciales. 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.

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. Estos códigos, diseñados e implementados por las propias empresas, pueden servir para establecer límites claros, procedimientos operativos y principios éticos que complementan la normativa vigente, proporcionando mayor flexibilidad y adaptabilidad a las particularidades de cada organización y sector.[38]

Un código de conducta específico para el uso de estas herramientas debe priorizar la definición clara de los fines permitidos, 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. Para ello, es imprescindible incluir cláusulas específicas en los contratos laborales o políticas internas que detallen estos aspectos. Además, el establecimiento de canales de comunicación efectivos entre la empresa y los empleados es clave para resolver dudas, atender preocupaciones y reportar posibles abusos relacionados con estas herramientas.

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. Estas garantías son esenciales para respetar los derechos fundamentales de los trabajadores y evitar un uso indebido de la información[39].

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, además de evaluar periódicamente el impacto de las tecnologías en el entorno laboral, puede emitir

---

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

[39] Agencia Española de Protección de Datos, 2023, pp. 7-8, 23

recomendaciones para ajustar su uso en función de las necesidades cambiantes de la empresa o los avances tecnológicos.[40]

La formación y la sensibilización de empleados y directivos sobre el uso ético y legal de estas herramientas deben ser componentes esenciales de los códigos de conducta. La capacitación continua no solo contribuye a reducir el desconocimiento y la desconfianza hacia estas tecnologías, sino que también promueve una cultura de respeto y responsabilidad dentro de la organización. Por último, los códigos deberían incluir medidas disciplinarias claras para sancionar el uso indebido de las herramientas de reconocimiento de emociones, reforzando así su aplicación responsable y ética.

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.

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.[41]

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 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* Misma cita

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**

[40] Agencia Española de Protección de Datos [AEPD], 2023, pp. 24, 31
[41] European Commission. (2020)**.** *White Paper on Artificial Intelligence: A European approach to excellence and trust.*

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 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.[42]

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[43]. Además, la involucración de los sindicatos en este proceso puede ayudar a fortalecer la legitimidad de los acuerdos alcanzados y contribuir a garantizar su aceptación y cumplimiento.

Otra dimensión esencial de la corregulación es su capacidad para promover la transparencia y la rendición de cuentas. Los acuerdos sectoriales pueden incluir la obligación de realizar auditorías periódicas para verificar el cumplimiento de las disposiciones pactadas y evaluar el impacto de las tecnologías en los entornos laborales. Estos acuerdos pueden establecer procedimientos claros para gestionar posibles controversias o reclamaciones, asegurando que existan vías efectivas de resolución de conflictos entre las partes.[44]

Desde el punto de vista normativo, los acuerdos sectoriales también pueden servir como una base sólida para la futura elaboración de legislación específica. Al identificar y consensuar las necesidades y desafíos propios de cada sector, estos acuerdos pueden proporcionar información valiosa para el diseño de políticas públicas más efectivas y **adaptadas a la realidad del mercado laboral.** Este enfoque dinámico y participativo permite que la regulación **evolucione al mismo ritmo que las innovaciones tecnológicas, e**vitando la obsolescencia de las normas frente a los rápidos avances de la inteligencia artificial y de los propios ecosistemas laborales.[45]

---

[42] https://www.autocontrol.es/2021/10/14/direccion-general-del-juego-y-autocontrol-convenio-corregulacion-publicidad-juego/

[43] (Organización Internacional del Trabajo, 2018)

[44] 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.

[45] 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?utm_source=chatgpt.com

En definitiva, la corregulación a través de acuerdos sectoriales no solo fortalece la seguridad jurídica en el uso de sistemas de reconocimiento de emociones, sino que también fomenta un entorno laboral más equilibrado y colaborativo. Al combinar la flexibilidad del sector privado con la supervisión y orientación del sector público, este modelo puede ayudar a garantizar una implementación ética y eficiente de estas tecnologías, promoviendo al mismo tiempo la innovación y el respeto por los derechos fundamentales de los trabajadores.

Colaboración público-privada en el diseño de políticas

La colaboración público-privada emerge como un enfoque estratégico clave para garantizar el uso ético, eficiente y seguro de los sistemas de reconocimiento de emociones en el ámbito laboral. Este modelo de cooperación permite combinar l**a experiencia y los recursos del sector privado con la legitimidad, el marco normativo y la capacidad supervisora del sector público,** logrando así un diseño de políticas más inclusivo, efectivo y alineado con las necesidades reales del mercado laboral y los derechos de los trabajadores.[46]

En el contexto del reconocimiento de emociones, esta colaboración puede manifestarse en la creación de **consorcios público-privado**s dedicados al desarrollo de marcos regulatorios específicos para estas tecnologías. Estos consorcios, integrados por representantes de empresas, sindicatos, reguladores y expertos en inteligencia artificial, pueden trabajar en el diseño de políticas y estrategias que regulen su implementación. Al incluir a todos los agentes implicados, se fomenta un proceso de **diálogo y consenso** que resulta esencial para abordar los riesgos, beneficios y desafíos asociados con el uso de estas herramientas.[47]

Una de las formas más efectivas de aplicar esta colaboración es a través de **proyectos piloto** supervisados por las autoridades públicas y cofinanciados por empresas privadas.[48] Estos proyectos pueden permitir la evaluación en entornos controlados del impacto de los sistemas de reconocimiento de emociones en aspectos clave como la productividad, el bienestar de los trabajadores y la protección de sus derechos fundamentales. Los resultados de estas pruebas pueden servir como base para desarrollar políticas públicas informadas y prácticas, ajustadas a las particularidades de cada sector o actividad económica.

La colaboración público-privada es un instrumento eficaz para promover la adopción de **estándares técnicos y garantizar la interoperabilidad de los sistemas**[49]. Los organismos reguladores pueden trabajar en conjunto con el sector privado para definir **requisitos**

---

[46] (Comisión de las Comunidades Europeas, 2004).
[47] Organisation for Economic Co-operation and Development (OECD). (2021). *Public-Private Partnerships for Policy Design in AI*. Recuperado de https://www.oecd.org/
[48] International Telecommunication Union (ITU). (2025). *AI for Good*. Recuperado de https://www.itu.int/
[49] Datos.gob.es. (s.f.). *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

mínimos de calidad, fiabilidad y transparencia que deban cumplir estas tecnologías antes de ser implementadas. Esta estandarización no solo incrementará la confianza de los usuarios y trabajadores, sino que también facilita el cumplimiento normativo por parte de las empresas.[50]

Otro beneficio significativo de este enfoque es la posibilidad de **compartir recursos y conocimientos** entre el sector público y privado. Mientras las empresas aportan su experiencia técnica y operativa, las administraciones públicas pueden proporcionar orientación regulatoria y supervisión, asegurando que las tecnologías se desarrollen e implementen de acuerdo con los principios éticos y legales.[51] Esta sinergia contribuye a la creación de un entorno de innovación responsable, donde los avances tecnológicos se alineen con los valores sociales y los derechos laborales.

Iniciativas que demuestran cómo la colaboración entre el sector público y privado puede conducir al desarrollo de políticas y estándares son por ejemplo El Centre for Data Ethics and Innovation (CDEI) del Reino Unido ha liderado iniciativas para promover el uso ético de tecnologías de inteligencia artificial (IA) y datos. Por ejemplo, ha desarrollado herramientas y marcos de gobernanza para garantizar que las tecnologías de IA funcionen de manera confiable y transparente, fomentando la confianza pública en su uso.[52]

Otro ejemplo relevante de colaboración público-privada es el Foro de Empresas por Madrid, una iniciativa impulsada por el Ayuntamiento de Madrid que reúne a empresas privadas y actores públicos con el objetivo de desarrollar proyectos que beneficien a la ciudad y sus ciudadanos. Este foro se ha destacado por fomentar la innovación, la sostenibilidad y la mejora de diversos entornos, incluyendo el ámbito laboral, mediante la creación de sinergias entre los sectores público y privado.[53] No cabe duda de que este ejemplo ilustra cómo la cooperación entre sectores puede ser una herramienta eficaz para equilibrar la innovación tecnológica con la protección de los derechos fundamentales, generando beneficios tanto para las empresas como para la sociedad en general.

El programa de Proyectos de Colaboración Público-Privada (CPP) de la Agencia Estatal de Investigación en España es otro ejemplo al que se merece hacer mención. Este programa fomenta alianzas entre empresas y organismos de investigación, financiando iniciativas que aborden retos tecnológicos y sociales. La convocatoria de 2023 asignó hasta 360 millones de euros para proyectos innovadores con impacto en áreas como tecnología, medio ambiente y salud. Este modelo impulsa el diseño de soluciones éticas y sostenibles, asegurando que los recursos del sector privado se combinen con la supervisión y el marco regulatorio del sector público para maximizar su beneficio social.[54]

---

[50] (Catalá Pérez, 2019, pp. 109-134, 223-256).
[51] (Comisión de las Comunidades Europeas, 2004, pp. 3, 6, 9).
[52] https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about?utm_source=chatgpt.com
[53] https://www.monedaunica.net/2022/01/el-foro-de-empresas-por-madrid-es-un-ejemplo-de-colaboracion-publico-privada/?t&utm_source=perplexity
[54] https://www.inneara.com/proyectos-colaboracion-publico-privada/?t&utm_source=perplexity

Además, el CDEI ha publicado una hoja de ruta para construir un ecosistema de aseguramiento de IA en el Reino Unido, estableciendo pasos para verificar que los sistemas de IA sean efectivos, confiables y cumplan con las normativas, lo que impulsa una adopción más amplia y responsable de estas tecnologías.

En conclusión, la colaboración público-privada en el diseño de políticas ofrece una solución robusta para abordar los desafíos que plantea el uso de sistemas de reconocimiento de emociones en el ámbito laboral. Este modelo no solo permite un desarrollo normativo más dinámico y adaptado a las realidades tecnológicas, sino que también garantiza que las medidas adoptadas sean equilibradas, inclusivas y efectivas. Al combinar los esfuerzos de los sectores público y privado, se fomenta un entorno laboral donde la innovación tecnológica y la protección de los derechos fundamentales puedan coexistir de manera armoniosa y sostenible.

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 pueden afectarla, incluidas la comunicación ineficaz, la presión excesiva, el liderazgo deficiente y la cultura organizacional*".[55]

Uno de los principales beneficios de adoptar estándares internacionales es la posibilidad de garantizar la **interoperabilidad de los sistemas**. En un mercado globalizado, donde las empresas operan en múltiples jurisdicciones, contar con especificaciones técnicas unificadas facilita el despliegue de estas tecnologías en diferentes contextos sin comprometer su funcionalidad ni generar incertidumbre regulatoria. Los estándares internacionales actúan como un mecanismo para mitigar los riesgos asociados al sesgo algorítmico, exigiendo que los sistemas sean sometidos a pruebas rigurosas que certifiquen su equidad 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 garantiza 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.

---

[55] 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/

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.[56] 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[57]. Esto no solo facilita el cumplimiento normativo, sino que también impulsa la competitividad empresarial al eliminar barreras técnicas al comercio y la innovación.

Por último, el desarrollo de estándares técnicos debe ser un proceso inclusivo, que cuente con la participación activa d**e 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"* (Ciberespiral, 2023). 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.

Los estándares técnicos internacionales pueden ser una herramienta clave a la hora de asegurar el desarrollo y la implementación ética de los sistemas de reconocimiento de emociones en el ámbito laboral. Al proporcionar un marco técnico unificado, fomentan la transparencia, la equidad y la interoperabilidad, contribuyendo a un entorno laboral donde la innovación tecnológica se alinee con los principios de justicia, seguridad y respeto por los derechos humanos.

[Falta incluir un poco que tendrían que ser respaldados por los supervisores/reguladores de inteligencia artificial para que cumplieran con su función de mejora de la seguridad jurídica y mejora de la eficiencia en el modelo regulatorio]

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,

---

[56] 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/

[57] misma cita

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 (por si la derogan) 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[58][59].

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 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[60]. 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[61]. 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.

---

58 https://www.elconfidencial.com/mundo/2023-10-30/biden-firma-orden-controlar-inteligencia-artificial_3764864/?utm_source=chatgpt.com

59 https://www.wired.com/story/biden-executive-order-cybersecurity-ai-and-more/?utm_source=chatgpt.com

60 (Cadena SER, 2024).

61 Industrial Mindset, 2024.

Estos **incentivos deben ir acompañados de campañas de sensibilización y educación que resalten la importancia de las buenas prácticas en el uso de sistemas de reconocimiento de emociones**. La promoción de casos de éxito y la divulgación de los beneficios tangibles asociados al cumplimiento de estándares éticos pueden motivar a más empresas a invertir en el desarrollo responsable de estas tecnologías. Este enfoque no solo contribuye a la creación de un ecosistema de IA más seguro y transparente, sino que también fomenta la competitividad sostenible y la innovación.

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. Al recompensar a las empresas que actúan con responsabilidad y ética, estos mecanismos no sólo promueven un entorno laboral más respetuoso con los derechos fundamentales, sino que también impulsan una cultura de innovación sostenible y alineada con los valores sociales.

Procedimientos normalizados para evaluación y supervisión FALTA

Que todo el mundo entienda el reglamento de la misma manera, que ponga evaluaciones de impacto y que todo el mundo entienda lo mismo, que se estandarice la manera de llevarlas a cabo. Que se establezcan normas técnicas que ayuden a entender de una misma manera. A todas las empresas que aplica como se hacen esas evaluaciones de impacto] (comisión europea buenas prácticas)

Conclusión

El desarrollo legislativo y la mejora de la seguridad jurídica en torno a los sistemas de reconocimiento de emociones en el ámbito laboral requieren un enfoque integral que priorice la protección de los derechos fundamentales de los trabajadores y fomente una implementación ética de estas tecnologías. Estos sistemas, al evaluar características emocionales y personales, plantean riesgos significativos en términos de privacidad, proporcionalidad y transparencia, por lo que es crucial establecer mecanismos regulatorios que aborden estas preocupaciones de manera efectiva.

La autorregulación mediante códigos de conducta proporciona a las empresas herramientas específicas para definir los fines legítimos de estas tecnologías, evitando usos abusivos o desproporcionados que puedan vulnerar la dignidad de los empleados. Paralelamente, la corregulación y la colaboración público-privada permiten un marco adaptativo y consensuado que garantiza el equilibrio entre los intereses empresariales y la protección de los derechos laborales.

El desarrollo de estándares técnicos internacionales y la creación de incentivos específicos, como beneficios fiscales o certificaciones de calidad, son esenciales para promover la transparencia, la interoperabilidad y la confianza en los sistemas de reconocimiento de emociones. Además, los procedimientos normalizados para la evaluación y supervisión de estas herramientas aseguran que se utilicen de manera responsable, mediante auditorías periódicas, protocolos de supervisión humana y registros detallados de decisiones.

En definitiva, las propuestas planteadas no solo fortalecen la seguridad jurídica, sino que también establecen un camino claro hacia la integración de los sistemas de reconocimiento de emociones en el entorno laboral, garantizando que estos se utilicen como herramientas que respeten la privacidad, la

equidad y la dignidad de los trabajadores. Este marco no solo contribuye a un entorno laboral más justo y transparente, sino que también posiciona a estas tecnologías como un motor de innovación responsable y sostenible.

Bibliografía:

- https://www.elforodelabos.es/2024/11/algoritmos-sesgados-y-seleccion-de-personas/
- https://iamasigual.eu/que-dice-la-ley-de-ia-sobre-los-sistemas-automatizados-de-control-de-emociones/#:~:text=El%20sistema%20de%20reconocimiento%20de,3%20(39)%20RIA).
- Martín de Diego, I., Serrano, A., Conde, C., y Cabello, E. (2006). Técnicas de reconocimiento automático de emociones. [Versión electrónica]. "Teoría de la Educación : educación y cultura en la sociedad de la información", 7 (2), 92-106.
- https://www.businessinsider.es/ia-evaluara-felicidad-trabajadores-empresas-chinas-883859
- https://brand24.com/blog/es/software-de-deteccion-de-emociones/
- **https://revista-aji.com/wp-content/uploads/2024/07/AJI21_Art11.pdf**
- *Biometría y sistemas automatizados de reconocimiento de emociones: Implicaciones Jurídicos-Laborales*
- *https://www.fundacionlaboral.org/actualidad/noticias/fundacion/bionic-ropa-inteligente-para-la-prevencion-de-riesgos-laborales-en-tiempo-real*
- *Wilkins, N. (2019). Inteligencia artificial : una guía completa sobre la IA, el aprendizaje automático, el Internet de las cosas, la robótica, el aprendizaje profundo, el análisis predictivo y el aprendizaje reforzado. [Bravex Publications].* **NO LO TENGO**
- *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024.*
- *CEPD-SEPD. Dictamen conjunto 5/2021 sobre Ley de Inteligencia Artificial, 18 de junio de 2021.*
- *El Periódico. "Cárceles de Cataluña: Inteligencia Artificial para el control de presos." 20 de septiembre de 2023.*
- *MDPI. "Speech Emotion Recognition in Healthcare: Enhancing Doctor-Patient Empathy." 2021.*
- *CEPD-SEPD. Dictamen conjunto 5/2021 sobre Ley de Inteligencia Artificial, 18 de junio de 2021.*
- *OSHA-EU. Impact of Artificial Intelligence on Occupational Safety and Health, 2021.*
- *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*
- *RRHH Press. (n.d.). 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
- *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*
- *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.*
- *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*
- *Jones, M. L. (2017). The Right to a Human in the Loop: Political Constructions of Computer Automation and Personhood. Social Studies of Science, 47(2), 220 y ss. https://doi.org/10.1177/0306312717699716*
- *Sheridan, T. B. (1995). Human-Centered Automation: Oxymoron or Common Sense?. IEEE International Conference on Systems, Man and Cybernetics, 823–828. https://doi.org/10.1109/ICSMC.1995.537867*
- *Esade (2023). ¿Cómo pueden los algoritmos perpetuar la discriminación en el trabajo?. Recuperado de https://dobetter.esade.edu/es/algoritmos-discriminacion-trabajo*
- *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*
- ***Grupo Atico 34** (2023). "Reconocimiento de emociones: riesgos y normativa". Disponible en: https://protecciondatos-lopd.com/empresas/reconocimiento-emociones/.*
- ***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/.*
- ***Agencia Española de Protección de Datos (AEPD)** (2021). Guía sobre la Protección de Datos en las Relaciones Laborales. Disponible en: https://www.aepd.es/.*
- ***Tribunal General de la Unión Europea (2023).** Sentencia de 7 de septiembre de 2023. Asunto T-158/19, Patrick Breyer/Agencia Ejecutiva de la Innovación y de las Redes (INEA). Disponible en: https://curia.europa.eu.*
- *Mariscal & Abogados. (n.d.). Códigos de conducta empresariales. Recuperado de https://www.mariscal-abogados.es/codigos-de-conducta-empresariales*
- *Agencia Española de Protección de Datos (AEPD). (n.d.). Códigos de conducta. Recuperado de https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/codigos-de-conducta*
- *Agencia Española de Protección de Datos (AEPD). (2023). Guía sobre tratamientos de control de presencia mediante sistemas biométricos (versión noviembre 2023). Recuperado de https://www.aepd.es/guias/guia-control-presencia-biometrico.pdf*
- *European Commission. (2020). White Paper on Artificial Intelligence: A European approach to excellence and trust. Recuperado de https://ec.europa.eu*
- *Agencia Española de Protección de Datos (AEPD). (n.d.). Códigos de conducta. Recuperado de https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/codigos-de-conducta*

- *Organización Internacional del Trabajo. (2016). Manual para el diálogo social eficaz: Manual y guía práctica para los interlocutores sociales. Recuperado de https://www.ilo.org/sites/default/files/wcmsp5/groups/public/@ed_dialogue/@dialogue/documents/publication/wcms_548547.pdf*
- *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*
- *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.*
- *Ministerio de Trabajo y Economía Social. (s.f.). La negociación colectiva y los conflictos colectivos. Recuperado de https://www.mites.gob.es/es/Guia/texto/guia_12/contenidos/guia_12_24_3.htm*
- *Organisation for Economic Co-operation and Development (OECD). (2021). Public-Private Partnerships for Policy Design in AI. Recuperado de https://www.oecd.org/*
- *Catalá Pérez, D. (2019). La colaboración público-privada como instrumento de intervención pública para el impulso de la innovación: Un análisis del sistema español de ciencia, tecnología e innovación (Tesis doctoral). Universitat Politècnica de València. Recuperado de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://riunet.upv.es/bitstream/handle/10251/139096/Catal%C3%A1%20-%20La%20colaboraci%C3%B3n%20p%C3%BAblico-privada%20como%20instrumento%20de%20intervenci%C3%B3n%20p%C3%BAblica%20para%20el%20impulso....pdf?utm_source=chatgpt.com*
- *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*
- *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/*
- *Global Suite Solutions. (2024). ¿Qué es y para qué sirve la norma ISO 42001:2023 de inteligencia artificial? Recuperado de https://www.globalsuitesolutions.com/es/que-es-y-para-que-sirve-la-norma-iso-42001-2023-inteligencia-artificial/*
- *nternational Organization for Standardization. (2023). ISO/IEC 42001:2023: Artificial Intelligence Management Systems — Requirements. Recuperado de https://www.iso.org/standard/81230.html*
- *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/*
- *Ciberespiral. (s.f.). Desarrollo inclusivo y diversidad en la inteligencia artificial. Recuperado de https://ciberespiral.org/es/desarrollo-inclusivo-y-diversidad-en-la-inteligencia-artificial/*
- *Datos.gob.es. (s.f.). 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*
- *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/

- *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/*
- *Agencia Española de Protección de Datos. (2024). Ejerce tus derechos. AEPD. https://www.aepd.es/derechos-y-deberes/ejerce-tus-derechos*
- *Garriga Domínguez, A. (2024). "Los derechos ante los sistemas biométricos que incorporan Inteligencia Artificial." Derechos y Libertades, 51, 117-149.*