

Tendencia T09

Regulaciones emergentes sobre IA datos y vigilancia digital

Código	T09
Categoría	Normativa / Regulatoria
Criterio C2 – Riesgo de desplazamiento ocupacional	2 – Bajo: crea nuevas tareas de gobernanza de datos y protección de privacidad. No desplaza perfiles actuales sino que añade competencias específicas a roles de RRHH y cumplimiento. Ajustes moderados.
Procesos transversales afectados	Principalmente: Gestión de personas y SSO, Gestión del cumplimiento. En forma secundaria: Producción, Compras y abastecimiento.
Nivel de madurez	3-4 – Tendencia madura: marco regulatorio central (EU AI Act) vigente con plazos definidos y enforcement en marcha; proliferación global de marcos equivalentes; enforcement GDPR intensificado. En Uruguay el avance es aún lento.

Definición operativa

Las regulaciones emergentes sobre IA, datos y vigilancia digital constituyen el conjunto de marcos legales —principalmente el Reglamento de IA de la UE (EU AI Act) y el Reglamento General de Protección de Datos (GDPR), junto con sus equivalentes y desarrollos nacionales e internacionales— que establecen obligaciones vinculantes sobre cómo las organizaciones pueden desarrollar, desplegar y gestionar sistemas de inteligencia artificial, recopilar y procesar datos personales, y utilizar tecnologías de monitoreo digital sobre trabajadores y proveedores.

Para la industria manufacturera, esta tendencia tiene tres dimensiones operativas específicas que afectan directamente los procesos de Gestión de personas, Gestión del cumplimiento, Producción y Compras y abastecimiento:

- **Gobernanza de IA en el lugar de trabajo:** el EU AI Act clasifica como de 'alto riesgo' el **uso de IA en contratación, selección, evaluación de desempeño, asignación de tareas y otras decisiones de empleo**. Desde agosto de 2025, los sistemas de IA de propósito general (GPAI) deben documentar datos de entrenamiento y publicar informes de transparencia. Desde agosto de 2026, los sistemas deberán cumplir

requisitos de gestión de riesgos, supervisión humana, documentación técnica y evaluación de impacto de datos. Las multas pueden alcanzar €35 millones o el 7% del volumen de negocio global anual [1][2].

- Privacidad de datos y GDPR aplicado a sistemas IIoT y analítica de personas: la convergencia del IIoT manufacturero con el procesamiento de datos de trabajadores —wearables, sensores biométricos, monitoreo de productividad, geolocalización en planta— crea riesgos de gestión de datos personales (GDPR) significativos. El cumplimiento acumulado de multas GDPR superó los €7,1 mil millones hasta mediados de 2025, con €1,2 mil millones emitidos sólo en 2024. [3][4].
- Regulación de vigilancia digital y wearables en el trabajo: el despliegue de tecnologías de monitoreo —cámaras con IA, gafas inteligentes, wearables con sensores biométricos, sistemas de seguimiento de ubicación, análisis de comportamiento en tiempo real— activa un marco regulatorio crecientemente estricto que combina el EU AI Act (prohibición de ciertas formas de reconocimiento emocional en espacios de trabajo desde febrero de 2025), el GDPR, la legislación laboral nacional y la normativa de SSO [5][6].

Alcance extraterritorial: el EU AI Act como estándar global de facto

Al igual que el GDPR —que se convirtió en el estándar de privacidad de datos global de referencia a pesar de ser una regulación europea— el EU AI Act tiene alcance extraterritorial: aplica a cualquier sistema de IA cuyos outputs sean utilizados en la UE, independientemente de dónde esté establecido el proveedor o el usuario. Esto significa que empresas manufactureras de América Latina, Asia o Norteamérica que vendan a clientes europeos, tengan empleados en la UE o exporten productos allí deben cumplir sus requisitos. El 'Efecto Bruselas' en regulación de IA replica el patrón ya documentado para el GDPR: la regulación más estricta del mercado más grande se convierte en estándar de facto global [2][7].

Nivel de madurez

La tendencia alcanza madurez de nivel 4: el marco regulatorio central está vigente, los plazos de cumplimiento están definidos, el enforcement GDPR opera a escala industrial, y la proliferación global de marcos equivalentes —con distintos enfoques pero objetivos convergentes— da certeza sobre su trayectoria estructural. Los indicadores clave son:

- EU AI Act en vigor con hitos ya cumplidos: el Reglamento entró en vigor el 1 de agosto de 2024. Las prohibiciones (uso de IA con riesgos inaceptables, incluyendo reconocimiento emocional en lugares de trabajo) son vinculantes desde el 2 de febrero de 2025. Los requisitos para modelos GPAI están vigentes desde agosto de

2025. La plena obligatoriedad para sistemas de alto riesgo —incluyendo los de RRHH y gestión del empleo— entrará en vigor el 2 de agosto de 2026 [1][2].

- Enforcement GDPR consolidado a escala industrial: más de 2.800 multas emitidas hasta mediados de 2025; total acumulado €7,1 mil millones; más del 60% de ese total impuesto desde enero de 2023. El GDPR está siendo utilizado como principal herramienta de exigencia de cumplimiento para regulación de IA mientras las normas específicas de IA se implementan progresivamente [3].
- Proliferación de marcos regulatorios equivalentes a nivel global: Brasil aprobó su proyecto de IA en el Senado (diciembre 2024), con modelo de clasificación de riesgo similar al EU AI Act. Japón aprobó la AI Promotion Act (mayo 2025). China actualizó su Ley de Ciberseguridad con referencias explícitas a IA (enero de 2026). El G7 bajo la presidencia de Canadá (2025) desarrolló un compendio de mejores prácticas para IA centrada en las personas en el lugar de trabajo [7][8].
- Regulación de vigilancia en el trabajo en aceleración: la Equal Employment Opportunity Commission (EEOC, EE.UU.) emitió en diciembre de 2024 un comunicado sobre wearables en el lugar de trabajo. La Eurofound³ documenta que el monitoreo digital de trabajadores es un fenómeno de difícil regulación, con múltiples estados miembros de la UE introduciendo salvaguardias nacionales adicionales al GDPR. La National Labor Relations Board (NLRB) en EE.UU. emitió un memorando sobre vigilancia digital que sigue vigente [5][6].

En el Anexo A4.9 se presentan las evidencias empíricas a nivel internacional que justifican el nivel de madurez asignado, incluyendo casos industriales demostrativos.

Análisis prospectivo

Escenario de corto plazo (0-2 años)

El período inmediato está dominado por la preparación para el cumplimiento de la plena obligatoriedad del EU AI Act para sistemas de alto riesgo en agosto de 2026. Para las empresas manufactureras que ya utilizan herramientas de IA en procesos de RRHH —reclutamiento automatizado, evaluación de desempeño, programación de turnos, sistemas de gestión de productividad—, este plazo presiona, ya que la documentación de sistemas, evaluaciones de sesgo, auditorías de sistemas y establecimiento de procesos de supervisión humana demandan meses de trabajo preparatorio.

El cumplimiento de normativas de gestión de datos personales continuará siendo el principal vector regulatorio para IA en este período, dado que las reglas específicas del EU AI Act aún se están consolidando.

Escenario de mediano plazo (3-5 años)

En el mediano plazo, la convergencia regulatoria global se profundizará. Los marcos de Brasil, India, Japón, China y los países del G20 irán progresivamente hacia estándares de riesgo similares a los del EU AI Act, creando un entorno de cumplimiento multi-jurisdiccional complejo para las empresas manufactureras que operan cadenas de valor globales. El 'Efecto Bruselas' garantiza que los estándares más exigentes —los europeos— se convertirán en el mínimo denominador común para cualquier empresa que aspire a operar en mercados internacionales.

La función de cumplimiento en manufactura debe evolucionar desde un enfoque reactivo (responder a auditorías) hacia un enfoque proactivo de gobernanza de IA y datos: políticas internas de uso responsable de IA, registros de inventario de sistemas de IA, procesos de evaluación de impacto antes del despliegue, y mecanismos de supervisión humana documentados para las decisiones de alto riesgo.

Tensión central: los mismos sistemas que mejoran la productividad generan los mayores riesgos regulatorios

Las tecnologías con mayor potencial de mejora de la seguridad y eficiencia en manufactura —wearables biométricos para SSO, sistemas de IA para gestión de productividad, algoritmos de programación de turnos, herramientas de vigilancia de fatiga en operaciones peligrosas— son exactamente las clasificadas como de alto riesgo por el EU AI Act cuando involucran decisiones sobre trabajadores, o como problemáticas bajo el GDPR cuando procesan datos biométricos o de comportamiento. Las empresas manufactureras deben navegar esta tensión estructural: adoptar la tecnología para competir, pero gobernándola adecuadamente para no asumir riesgos regulatorios desproporcionados.

Impacto sobre los procesos transversales de la industria manufacturera

La tendencia tiene impacto concentrado en los procesos de gestión de personas y cumplimiento, con efectos secundarios sobre producción y compras:

Tabla 1. Impacto actual y proyectado de la tendencia T09 sobre procesos críticos

Proceso transversal	Impacto actual	Impacto proyectado	Descripción del impacto
Gestión de personas y SSO	Medio	Alto	Es el proceso más directamente afectado. Actualmente: los sistemas de IA usados en reclutamiento, evaluación de desempeño, programación de turnos y gestión de productividad son clasificados como de alto riesgo por el EU AI Act. Las prohibiciones de reconocimiento emocional en el trabajo entraron en vigor en febrero de 2025. Los wearables de monitoreo biométrico (SSO) activan restricciones GDPR. A futuro (agosto 2026): obligación de informar a los trabajadores sobre el uso de IA de alto riesgo en decisiones que les afectan; supervisión humana demostrable; evaluaciones de impacto de protección de datos; registro de sistemas en base de datos EU.
Gestión del cumplimiento	Medio	Alto	Proceso con mayor crecimiento de carga de trabajo regulatorio. Actualmente: necesidad de inventariar y clasificar todos los sistemas de IA por nivel de riesgo; verificar cumplimiento de proveedores de herramientas de IA con el EU AI Act; gestionar DPIA para sistemas de monitoreo de trabajadores. A futuro: función de cumplimiento que debe integrar tres marcos normativos simultáneos (EU AI Act + GDPR + legislaciones nacionales), con potenciales marcos adicionales en mercados no-UE donde la empresa opera.
Producción	Bajo	Medio	Los sistemas de IA en planta que involucran decisiones que afectan a trabajadores —asignación de tareas mediante IA, sistemas de optimización de mano de obra, wearables de monitoreo de seguridad con IA— activan obligaciones regulatorias. Los sistemas de control de proceso puramente automatizados sin decisiones sobre trabajadores están generalmente en categorías de riesgo más bajas. A futuro: cualquier sistema de 'gestión algorítmica del trabajo' (asignación de tareas, seguimiento de rendimiento en tiempo real) requerirá bases legales documentadas y mecanismos de transparencia ante los trabajadores.

Proceso transversal	Impacto actual	Impacto proyectado	Descripción del impacto
Compras y abastecimiento	Bajo	Medio	Las empresas son responsables del cumplimiento de los sistemas de IA que adquieren a proveedores. El EU AI Act exige verificar que los proveedores de sistemas de alto riesgo cumplan con sus obligaciones (registro en base de datos EU, documentación técnica, declaración de conformidad). A futuro: los contratos de adquisición de herramientas de IA deben incluir cláusulas de garantía de cumplimiento EU AI Act; los equipos de compras estratégicas incorporarán el compliance de IA como criterio de evaluación de proveedores de tecnología.
Logística de entrada	Bajo	Bajo	Si bien los sistemas de gestión de mano de obra en recepción y almacén (asignación de tareas, medición de productividad por operario, geolocalización en planta) que utilizan IA entran en la categoría de alto riesgo del EU AI Act cuando toman decisiones que afectan al trabajador, las regulaciones impactan poco sobre el proceso logístico en sí ya que las responsabilidades recaen en el área de gestión de personas.
Logística de salida	Bajo	Bajo	Los sistemas de gestión de picking asistidos por IA (optimización de rutas de preparación, asignación de órdenes, medición de productividad) tienen el mismo perfil regulatorio que los de entrada: clasificación de alto riesgo cuando toman decisiones que afectan al trabajador, pero que se deriva a gestión de personas

Dimensiones del impacto ocupacional y sobre perfiles (C2 = 2 – Bajo)

El impacto sobre el empleo es principalmente de **adición de nuevas responsabilidades y competencias a los perfiles existentes**, no de desplazamiento. La tendencia crea demanda de nuevos perfiles especializados y amplía el alcance de los roles de cumplimiento y RRHH hacia la gobernanza de tecnologías digitales.

- Perfiles con mayor ampliación de responsabilidades: responsable de RRHH, oficial de protección de datos (DPO), jefe de cumplimiento, responsable de sistemas, responsable de seguridad y salud ocupacional, analista de compras estratégicas (para proveedores de tecnología).
- Nuevas competencias demandadas: conocimiento del EU AI Act y su clasificación de riesgo aplicada a herramientas de RRHH y producción, metodología de Evaluación de

Impacto de Protección de Datos (DPIA), gestión de contratos con proveedores de IA (cláusulas de cumplimiento), diseño de procesos de supervisión humana para decisiones asistidas por IA, comunicación transparente a trabajadores sobre sistemas de IA que les afectan, auditoría de sesgo en sistemas de IA [1][2].

- Nuevos perfiles emergentes: oficial de cumplimiento de IA, especialista en ética de IA, oficial de protección de datos con especialización en IA (el DPO tradicional debe actualizarse en marcos de IA), analista de gobernanza de IA.
- Tensiones organizacionales emergentes: las obligaciones de transparencia del EU AI Act —informar a los trabajadores sobre el uso de IA que les afecta, garantizar supervisión humana de decisiones de alto riesgo— introducen tensiones entre la eficiencia operativa que buscan los sistemas de gestión algorítmica y los derechos de los trabajadores que garantiza la regulación. **La negociación colectiva sobre el uso de IA en el trabajo emerge como un nuevo espacio de relaciones laborales en Europa.**

Anexo A4.9. Evidencia empírica internacional

Cronograma regulatorio clave — EU AI Act y marcos relacionados

Fecha	Hito regulatorio	Implicación para empresas manufactureras
Agosto 2024	EU AI Act entra en vigor (Reglamento UE 2024/1689)	Las empresas deben iniciar una auditoría de sistemas de IA. Período de gracia para la mayoría de obligaciones.
Febrero 2025	Prohibiciones vigentes: reconocimiento emocional en lugares de trabajo, scoring social, vigilancia biométrica masiva	Las empresas manufactureras que usaban IA de reconocimiento emocional en planta deben discontinuarlas. Obligaciones de alfabetización en IA para personal involucrado en operaciones de IA.
Agosto 2025	Obligaciones GPAI: documentación de datos de entrenamiento, informes de transparencia, divulgación de riesgos	Los proveedores de herramientas de IA generativa que las empresas ya usan deben publicar documentación. Los equipos de RRHH e IT deben verificar el cumplimiento de sus proveedores.
Diciembre 2024	Ley de IA de Brasil aprobada en Senado; EEOC (EE.UU.) emite hoja de hechos sobre wearables	Las empresas con operaciones en Brasil preparan adaptación. Las que usan wearables de monitoreo en EE.UU. deben evaluar riesgos ADA/antidiscriminación.
Enero 2026	China: Ley de Ciberseguridad enmendada con referencias explícitas a IA entra en vigencia	Las empresas con operaciones en China deben adaptar sistemas de IA a nuevos requisitos de seguridad y localización de datos.

Fecha	Hito regulatorio	Implicación para empresas manufactureras
Agosto 2026	EU AI Act: plena obligatoriedad para sistemas de alto riesgo, incluyendo IA en contratación, evaluación de desempeño, gestión de personal	Fecha crítica para empresas que usan IA en RRHH. Se requieren: DPIA, documentación técnica, registro en base de datos EU, supervisión humana demostrable, información a trabajadores.
Agosto 2027	Obligaciones adicionales de transparencia; plena conformidad para modelos GPAI en mercado antes de agosto 2025	Nueva ola de obligaciones; las empresas que adoptaron IA antes del ciclo regulatorio deben adaptar sistemas heredados.
2028-2031	Revisiones y expansiones del EU AI Act; consolidación de marcos en Brasil, India, otros mercados emergentes	El perímetro regulatorio se expande a nuevos sectores y usos. Consolidación del 'efecto Bruselas' como estándar global.

Enforcement regulatorio

- DLA Piper GDPR Fines and Data Breach Survey (enero 2026): multas GDPR acumuladas superan €7,1 mil millones hasta mediados de 2025; €1,2 mil millones emitidos en 2024. Más del 60% del total ha sido impuesto desde enero de 2023 —señalizando aceleración sostenida. El GDPR es actualmente la herramienta primaria de enforcement para IA mientras las normas específicas se implementan [3].
- Kiteworks 2026 Data Security and Compliance Risk Forecast: el 29% de las organizaciones identifica las transferencias transfronterizas via proveedores de IA como su principal exposición de privacidad. El 54% de los consejos de administración no está comprometido con la gobernanza de IA —creando exposición no gobernada en la cima de las organizaciones [3].
- Casos de multas GDPR por uso de IA (2024-2025): LinkedIn fue multada por rastrear señales de comportamiento de usuarios (tiempo en publicaciones, velocidad de desplazamiento) para determinar características personales y usarlas en algoritmos de publicidad predictiva. El caso ilustra cómo los sistemas de analítica de comportamiento —incluidos los de monitoring de productividad en entornos laborales— pueden activar obligaciones GDPR por inferencia de características personales [4].

Vigilancia digital en el trabajo

- Eurofound (2024): el uso de tecnologías de monitoreo digital en el trabajo —IoT/wearables, machine learning, análisis de comportamiento— crea 'desafíos

significativos de cumplimiento' con el principio de minimización de datos del GDPR. Las tecnologías IoT carecen de transparencia en su recopilación y procesamiento de datos, amplificando los riesgos de privacidad. Múltiples estados miembros de la UE han introducido salvaguardias nacionales adicionales [5].

- EEOC, Wearables in the Workplace (diciembre 2024): la Comisión de Igualdad de Oportunidades en el Empleo de EE.UU. emitió una hoja de hechos advirtiendo que la tecnología de rastreo embebida en wearables —localización, frecuencia cardíaca, actividad cerebral eléctrica, fatiga— puede violar la Ley de Americanos con Discapacidades (ADA). El crecimiento en envíos de gafas inteligentes fue del 210% en 2024 [6].
- Marketplace Privacy, AI Round Up 2025/2026 (BCLP): 2025 fue un año definitorio para la privacidad de datos y el paisaje digital. Las gafas inteligentes con IA crean 'un campo minado legal' con riesgos de vigilancia invasiva, potencial violación de derechos de privacidad de terceros en instalaciones industriales y responsabilidad bajo legislación laboral si el monitoreo resulta opresivo [6].

Panorama regulatorio global

- IAPP Global AI Law and Policy Tracker (2025-2026): Japón aprobó la AI Promotion Act en mayo de 2025 — regulación que incentiva la cooperación con medidas de seguridad del gobierno y prevé divulgación pública de empresas que usen IA para violar derechos humanos—. China promulgó sus Reglas de Etiquetado de IA (septiembre 2025) exigiendo etiquetas visibles e invisibles en contenido generado por IA [8].
- Nemko / Atomic Mail, Global AI Regulations 2025: Brasil y Chile están desarrollando modelos de clasificación de riesgo inspirados en la UE. El 'Efecto Bruselas' emerge como el mecanismo dominante de convergencia regulatoria global: los países que operan cadenas de suministro conectadas con la UE adoptan estándares europeos como referencia de facto [7].
- Casa Blanca, Orden Ejecutiva sobre IA (diciembre 2025): EE.UU. adoptó una orden ejecutiva que busca establecer un marco nacional mínimamente restrictivo para política de IA, limitando la divergencia regulatoria a nivel estatal. Representa un viraje desde el enfoque de no intervención federal hacia una postura de 'pro-innovación con gobernanza mínima' [8].

Referencias

- [1] IRIS Global / HR-ON / Boundless (2025-2026). 'EU AI Act HR Compliance: How HR Can Prepare' y 'EU AI Act in HR: Requirements and Compliance'. Disponible en: <https://www.irisglobal.com/blog/eu-ai-act-hr-compliance-guide/> y <https://hr-on.com/eu-ai-act-for-hr-2026/> [Cronograma EU AI Act: prohibiciones feb. 2025; GPAI ago. 2025; alto riesgo ago. 2026; alto riesgo en RRHH: reclutamiento, evaluación desempeño, asignación de tareas; multas hasta €35M o 7% facturación global].
- [2] Ogletree Deakins / Boundless (2025). 'The EU AI Act Is Here—What It Means for U.S. Employers' y 'EU AI Act Employer Compliance Guide'. Disponible en: <https://ogletree.com/insights-resources/blog-posts/cybersecurity-awareness-month-in-focus-part-iii-the-eu-ai-act-is-here-what-it-means-for-u-s-employers/> [Alcance extraterritorial; alto riesgo incluyendo chatbots de selección, software de ranking de CVs, analítica de productividad; información obligatoria a trabajadores; supervisión humana demostrable; DPIA requerida].
- [3] Kiteworks (marzo 2026). 'GDPR Fines Hit €7.1 Billion: Data Privacy Enforcement Trends in 2026'. Disponible en: <https://www.kiteworks.com/gdpr-compliance/gdpr-fines-data-privacy-enforcement-2026/> [Total multas GDPR >€7,1B hasta mediados de 2025; €1,2B en 2024; >2.800 multas; 60%+ desde enero 2023; GDPR como herramienta primaria enforcement IA; 29% cita transferencias via IA como top exposición; 54% boards no comprometidos con gobernanza IA].
- [4] DPO Europe / Secure Privacy (2025-2026). 'Fines for GDPR Violations in AI Systems' y 'Compliance Challenges at the Intersection of AI & GDPR 2025'. Disponible en: <https://data-privacy-office.eu/fines-for-gdpr-violations-in-ai-systems-and-how-to-avoid-them/> [Caso LinkedIn: rastreo señales comportamentales para inferir características personales y uso en algoritmos predictivos; penalidades hasta 4% facturación global GDPR; AI Act hasta 7%].
- [5] Eurofound (julio 2024). 'Employee Monitoring: A Moving Target for Regulation'. Disponible en: <https://www.eurofound.europa.eu/en/resources/article/2024/employee-monitoring-moving-target-regulation> [IoT/wearables, ML y analítica de comportamiento: desafíos GDPR de minimización de datos; falta de transparencia en recopilación; múltiples estados miembros con salvaguardias nacionales adicionales; monitoreo continuo sin límites de tiempo].
- [6] Littler / Jackson Lewis (2024-2025). 'EEOC Fact Sheet on Wearable Technologies Indicates Growing Concern over Employee Monitoring'. Disponible en: <https://www.littler.com/news-analysis/asap/eeoc-fact-sheet-wearable-technologies-indicates-growing-concern-over-employee> [EEOC diciembre 2024: wearables pueden violar ADA; rastreo localización, frecuencia cardíaca, actividad cerebral, fatiga; envíos gafas inteligentes con IA +210% en 2024; NLRB memorando sobre vigilancia digital; leyes estatales de localización/datos biométricos].
- [7] Nemko Digital / FairNow / Atomic Mail (2025-2026). 'Global AI Regulations 2025: Key Frameworks & Compliance Guide'. Disponible en: <https://digital.nemko.com/regulations/global-ai-regulations> [Brasil: Bill 2338/2023 aprobado Senado diciembre 2024; modelo clasificación riesgo similar EU AI Act; Brasil y Chile como pioneros en Latinoamérica; Africa Union Framework; 'Efecto Bruselas' como mecanismo de convergencia global].
- [8] IAPP / Morgan Lewis / GDPR Local (2025-2026). 'Global AI Law and Policy Tracker' y 'The New Rules of AI: A Global Legal Overview'. Disponible en: <https://iapp.org/news/a/global-ai-law-and-policy-tracker-highlights-and-takeaways> [Japón AI Promotion Act mayo 2025; China AI Labeling Rules septiembre 2025; China Cybersecurity Law enmendada con IA en vigor enero 2026; EE.UU. Executive Order diciembre 2025; G7 Canada 2025: compendio buenas prácticas IA centrada en personas en el trabajo].

-
- [9] TechClass / GoGlobal (2025-2026). 'The EU AI Act: What HR, IT and Compliance Leaders Need to Know' y 'The EU AI Act in Action: What Employers Must Do Now and Next'. Disponible en: <https://www.techclass.com/resources/learning-and-development-articles/the-eu-ai-act-what-hr-it-and-compliance-leaders-need-to-know-in-2025> [Cuatro categorías de riesgo; prohibiciones específicas en HR; DPIA; bias testing; audit trail obligatorio; framework de implementación por fases hasta 2031].
-
- [10] Secure Privacy (2025-2026). 'GDPR Compliance in 2026: The Complete Guide'. Disponible en: <https://secureprivacy.ai/blog/gdpr-compliance-2026> [Enmiendas GDPR propuestas Q4 2025 (Digital Package); patrones oscuros como prioridad de enforcement; ingeniería de privacidad como estándar; agosto 2026 como fecha crítica convergencia AI Act + GDPR; 3 marcos de compliance separados en una sola fecha].
-
- [11] BigID (2025). '2025 Global Privacy, AI, and Data Security Regulations: What Enterprises Need to Know'. Disponible en: <https://bigid.com/blog/2025-global-privacy-ai-and-data-security-regulations/> [Australia: overhaul GDPR-style con derechos de borrado y portabilidad + limitaciones uso IA de datos; India: Digital Personal Data Protection Act 2023 + consultas regulación IA complementaria; Singapur: Model AI Governance Framework para IA generativa].
-
- [12] The Conversation / TechXplore (marzo 2026). 'Will AI drones, robots and wearable sensors revolutionize workplace safety?'. Disponible en: <https://theconversation.com/will-ai-drones-robots-and-wearable-sensors-revolutionize-workplace-safety-275412> [12,2% de empresas canadienses usando IA para producción en 2025 (doble que el año anterior); Canadá sin ley federal de IA; G7 presidencia canadiense: compendio IA para SSO; brecha de gobernanza en protección de trabajadores].
-
- [13] Christine Carter / SAGE Journals (2025). 'AI Surveillance: Reclaiming Privacy Through Informational Control'. Disponible en: <https://journals.sagepub.com/doi/10.1177/20319525241306327> [Marco conceptual de vigilancia digital del trabajo: wearables, GPS, RFID, cámaras IA, análisis de comportamiento; vigilancia no acotada al lugar de trabajo físico; portabilidad e interoperabilidad del monitoreo; ausencia de límites de duración y frecuencia].
-