

## La inteligencia artificial y los sistemas de vigilancia: un delicado equilibrio entre innovación y protección

### NEREA LUIS MINGUEZA

Doctora en computación cuántica  
Consultora independiente y experta en IA

En el siglo XXI, la adopción de la inteligencia artificial (IA) en las organizaciones empieza a transformar paulatinamente el ámbito laboral. Se han dado a conocer casos de uso que incorporan sistemas de videovigilancia inteligentes para, por ejemplo, monitorizar la productividad de los empleados. El objetivo del uso de estas tecnologías es mejorar su eficiencia y también su seguridad. Sin embargo, esta adopción plantea preguntas cruciales sobre los derechos de los trabajadores y los límites éticos que deben considerarse.

### Wearables, monitorización y la llegada del 5G

El abanico de dispositivos utilizados para la monitorización en el entorno laboral ha crecido exponencialmente con el avance de la tecnología. Desde sensores portátiles (wearables) que miden la actividad física hasta sistemas de geolocalización y cámaras de videovigilancia con reconocimiento facial. Estos dispositivos no solo se limitan a la oficina física; en el caso del teletrabajo, los empleadores pueden utilizar software de monitorización de teclados, grabación de pantallas y seguimiento del uso de aplicaciones.

Por otro lado, la llegada de la tecnología 5G ha acelerado esta adopción de dispositivos, permitiendo una mayor conectividad y transmisión de grandes volúmenes de datos en tiempo real. Con redes más rápidas, los sistemas de monitorización pueden operar de manera más fiable. Este despliegue masivo, si pensamos en los smartphones para rastrear y analizar el comportamiento de una ciudad, permite por ejemplo estudiar la viabilidad del transporte público en los movimientos diarios de las personas.

Volviendo al entorno laboral, la videovigilancia inteligente, por ejemplo, permite el seguimiento en tiempo real de los movimientos de los trabajadores. En teoría, estas herramientas pueden ayudar a mejorar la seguridad laboral, reducir accidentes y aumentar la productividad. Sin embargo, también representan un riesgo considerable

en términos de vigilancia desmedida, violación de la privacidad y creación de entornos laborales opresivos.

Los sistemas de IA basados en monitorización utilizan cámaras de videovigilancia o sensores. Aunque la justificación empresarial se enfoca en mejorar la eficiencia, optimizar procesos y garantizar la seguridad, los riesgos para los derechos fundamentales de los trabajadores son evidentes. ¿Hasta qué punto es legítimo monitorizar a los empleados sin invadir su privacidad?

## **Machine Learning y privacidad y regulación**

Una de las áreas más controvertidas es la utilización de sistemas de Machine Learning, o aprendizaje automático, ya sea en la evaluación del rendimiento, la asignación de tareas, la contratación o incluso la terminación de contratos. Estos sistemas, aunque eficientes, pueden carecer de transparencia y estar sesgados, lo que podría dar lugar a decisiones injustas o discriminatorias. ¿Cómo se asegura que estas decisiones sean objetivas y equitativas? Aquí es donde entra en juego la necesidad de una regulación clara y adecuada

El uso de estas tecnologías, si no se regula correctamente, puede afectar derechos fundamentales como la privacidad y la dignidad de los trabajadores. La recopilación de datos, que va desde la actividad en ordenadores hasta datos biométricos, debe cumplir con normativas como el Reglamento General de Protección de Datos (GDPR). Los trabajadores tienen derecho a ser informados sobre qué datos se recopilan, con qué fines y cómo se utilizan.

Por otro lado, la adopción de tecnologías de monitorización en el lugar de trabajo plantea importantes desafíos en términos de ciberseguridad y protección de datos. Para mitigar estos riesgos, las organizaciones deben asegurarse de que sus sistemas de software cumplen con estándares internacionales de seguridad, como la ISO/IEC 27001, una de las normas más reconocidas para la gestión de la seguridad de la información. Esta norma proporciona un marco sólido para la implementación de controles de seguridad, incluyendo la evaluación de riesgos, la protección de datos sensibles y la prevención de accesos no autorizados.

En el contexto de la monitorización laboral, la ISO 27001 es fundamental para garantizar que los datos recolectados de los empleados, como información biométrica, geolocalización o actividad digital, se almacenen y procesen de manera segura y confidencial. La implementación de esta norma también asegura que las organizaciones lleven a cabo auditorías regulares de sus sistemas, identificando y corrigiendo posibles vulnerabilidades, lo que reduce significativamente los riesgos de violaciones de datos y ciberataques.

Finalmente, el principio de no discriminación es otro factor esencial a tener en cuenta. Los sistemas de IA pueden perpetuar sesgos presentes en los datos con los que fueron entrenados, lo que podría desembocar en prácticas discriminatorias en la contratación o la evaluación del rendimiento. Es fundamental que estos sistemas sean auditados y evaluados para garantizar que no refuercen prejuicios de género, raza o cualquier otra condición.

## **La nueva Ley de Inteligencia Artificial**

En este contexto, la transparencia y la regulación son claves. Los empleados tienen derecho a saber qué herramientas de IA se utilizan en su entorno laboral, cómo se procesan los datos y con qué finalidad. Las empresas deben ser completamente transparentes sobre los algoritmos que aplican, y proporcionar información comprensible sobre cómo se toman las decisiones automatizadas.

Las organizaciones deben implementar políticas claras y garantizar que sus empleados reciban formación sobre estas tecnologías, sus beneficios y riesgos, así como sobre sus derechos y la protección de su privacidad en este nuevo panorama tecnológico.

A nivel internacional, algunos países han comenzado a desarrollar leyes específicas para la IA. En la Unión Europea, la propuesta de la Ley de IA (AI Act) busca establecer un marco regulador que asegure un uso seguro y ético de la inteligencia artificial en diversos sectores, incluido el laboral. Es importante que las empresas comprendan y respeten estas regulaciones, y que los gobiernos proporcionen guías claras para su implementación.

Es fundamental que el despliegue de la IA se realice con un enfoque ético, donde los derechos laborales y la dignidad humana sean priorizados por encima de la eficiencia tecnológica. La tecnología no debe ser una excusa para vulnerar derechos fundamentales, sino una herramienta que mejore tanto las condiciones de trabajo como la productividad empresarial.

## **Caso de uso prohibido: Reconocimiento facial y de emociones**

Entre las tecnologías más controvertidas en el ámbito de la monitorización laboral se encuentran los sistemas de reconocimiento facial y de reconocimiento de emociones. Estas tecnologías, capaces de identificar a los empleados a partir de sus características biométricas o de analizar sus expresiones faciales para inferir estados emocionales, presentan serios riesgos para la privacidad y la dignidad humana. En la

Unión Europea, su uso está restringido por el GDPR, que considera los datos biométricos como una categoría especialmente sensible de información personal.

Además, la Ley de IA de la UE busca imponer límites estrictos sobre el uso de estas tecnologías en entornos laborales, debido a su potencial para generar discriminación o afectar negativamente el bienestar de los trabajadores. Los sistemas de reconocimiento de emociones, en particular, son cuestionados por su falta de precisión y por los peligros que entrañan al intentar evaluar el estado emocional de los empleados para tomar decisiones sobre productividad o comportamiento.

## **Neuroderechos: Nuevos retos en la protección de los ciudadanos**

Con el avance de tecnologías como las interfaces cerebro-ordenador y la inteligencia artificial, surge un nuevo conjunto de preocupaciones éticas y legales conocido como neuroderechos. Estos derechos buscan proteger la integridad mental y la privacidad neuronal de las personas frente a la posibilidad de que sus pensamientos o emociones sean manipulados o monitorizados mediante tecnologías avanzadas. En el ámbito laboral, estas tecnologías podrían ser utilizadas para evaluar la concentración, el cansancio o incluso la predisposición emocional de los empleados, lo que plantea serios riesgos de abuso y discriminación. Algunos países, como Chile, ya han empezado a legislar sobre neuroderechos, y se espera que estas regulaciones se expandan a nivel global.

Los neuroderechos incluyen el derecho a la privacidad mental, el libre albedrío y la protección contra el sesgo cognitivo, asegurando que las empresas no puedan utilizar tecnologías invasivas para acceder o influir en la actividad mental de los empleados. Aún es un tema que genera opiniones de todo tipo, pero sí que es cierto que este tipo de tecnologías tienen el potencial de traspasar los límites físicos del cuerpo y adentrarse en la mente y nuestro comportamiento, como se ha demostrado con el scroll infinito.

## **Conclusiones**

El futuro del trabajo, sin duda, está ligado al desarrollo de tecnologías como la Inteligencia Artificial, pero es nuestra responsabilidad como sociedad garantizar que estas se implementen de manera justa y equitativa.

La adopción de la inteligencia artificial en el ámbito laboral no es una tendencia pasajera, sino una transformación que redefinirá la naturaleza misma del trabajo en las próximas décadas. Sin embargo, para que esta transformación sea exitosa, es imprescindible un enfoque centrado en el ser humano, donde las tecnologías sirvan para empoderar a los empleados en lugar de explotarlos. La IA puede ser una poderosa

# digitales\_

aliada para mejorar la productividad y la seguridad, siempre y cuando se implementen políticas de uso ético y responsable.

Las empresas que lideren el camino hacia una adopción ética de la IA serán aquellas que prioricen la transparencia, la equidad y el respeto por los derechos de sus empleados.



---

*Artículo financiado por la UE-NextGenerationEU. Sin embargo, los puntos de vista y las opiniones expresadas son únicamente los del autor o autores y no reflejan necesariamente los de la UE o la Comisión Europea. Ni la UE ni la Comisión Europea pueden ser consideradas responsables de las mismas.*