

Inteligencia Artificial y poder

La Ley de Inteligencia Artificial de la Unión Europea (EU AI Act) define ésta como un sistema basado en máquinas que está diseñado para funcionar con distintos niveles de autonomía, que puede mostrar capacidad de adaptación tras su despliegue, y que, para objetivos explícitos o implícitos, infiere, a partir de la información que recibe, cómo generar resultados tales como predicciones, contenidos, recomendaciones o decisiones que pueden influir en entornos físicos o virtuales.

Definición que incluye aportaciones desde sus primeras etapas hasta sus últimos avances en IA física (automatización o robótica autónoma, donde los sistemas actúan pudiendo tomar decisiones autónomas); grandes modelos de lenguaje (*ChatGPT*, *Gemini*, *Grok*, *Claude*, ...); o los sistemas de IA Agente que están cambiando los panoramas laborales o educativos, al permitir pasar a sistemas autónomos en los que la IA deja de ser una herramienta para convertirse en una capa operativa transversal, sustitutiva no ya solo del trabajo que se automatiza, sino también del conocimiento (programadores, abogados, investigadores, etc.), modificando los procesos de apropiación de la plusvalía y las relaciones técnicas y sociales de producción. De esta manera, se mejora la productividad y la toma de decisiones, pero se acelera la sustitución del trabajador con efectos que ya se notan en las grandes tecnológicas (*Big Tech*) y en empresas avanzadas en su

uso. Lo que abre la necesidad de una respuesta urgente de los Estados y de los sindicatos ante unos efectos graves en el empleo, la precariedad laboral y su influencia crítica en la sostenibilidad de la seguridad social.

Paralelamente, la IA genera ventajas comparativas para los que la usan frente a la competencia, pero genera dependencias tecnológicas de estos sistemas (y de las *Big Tech* propietarias) que, una vez implantadas, no se pueden reemplazar fácilmente.

En la actualidad, la seguridad y la defensa ya no se definen solo por la capacidad de disuasión física, sino por la superioridad en el dominio digital. Sistemas de Alerta Temprana, la Logística Inteligente o la Sanidad Militar encuentran en la IA un ins-

trumento fundamental para su optimización, porque es capaz de integrar datos de múltiples fuentes en tiempo real, generar miles de escenarios en los que probar las capacidades de defensa y ataque, simular escenarios de combate y respuesta en solo unos segundos, y proponer acciones en función del riesgo, impacto y recursos disponibles.

En Ucrania, el apoyo de las *Big Tech* y de la IA permitió anticipar e impedir la invasión inicial de Rusia, con fiabilidad y precisión en las respuestas. El sistema Lavender, de Israel, permite, a través de su gran base de datos de la población objetivo, identificar a personas y elaborar prioridades de eliminación. Asimismo, su sistema Gospel identifica edificios o estructuras

La IA puede proporcionar a la humanidad grandes beneficios, pero abre la puerta a unos usos dañinos que dejan clara la necesidad de abordar una regulación con garantías precisas para la población. En particular, en lo que se refiere a la responsabilidad de los que controlan las redes sociales y de los propietarios de sistemas de IA que los usen para cometer o permitir abusos y delitos de diverso tipo.

desde donde puede estar operando el enemigo, para su destrucción, aunque normalmente con "daños colaterales".

La IA confiere poder a los Estados con mayor capacidad de IA aplicada a la defensa, al control social, a la economía o a la inteligencia, reconfigurando el poder global alrededor de la capacidad tecnológica. La IA condiciona la ciberseguridad como pieza central en los sistemas de defensa y en las empresas. La detección de vulnerabilidades en el software se ha convertido en un nuevo elemento de poder de fuerte incidencia para evitar (o desarrollar) aplicaciones fraudulentas y militares. Y cobra relevancia la computación cuántica con algoritmos capaces de romper los sistemas criptográficos seguros de clave pública, o conseguir computadores y comunicaciones cuánticas de seguridad garantizada, ya que el primero que los alcance y utilice tendrá una gran superioridad sobre los demás, estando, por ahora, China en la vanguardia de la producción de nuevos tipos de armas equipados con nuevas tecnologías e IA. China, es dominante en IA aplicada, con cerca del 40% de todas las patentes mundiales en el sistema de IA, frente a aproximadamente el 20% de EEUU. Si bien con un modelo regulatorio inaceptable en su control político-social (sistemas de vigilancia masiva con asignación de "crédito social" personal).

Hoy en día, sabemos que la IA incrementa la capacidad de manipulación de la realidad y desinformación, lo que lleva a riesgos crecientes en materia de seguridad y dependencia social. De hecho, está siendo utilizada para desestabilizar democracias o modelos sociales mediante una desinformación basada en datos falsos y el empleo de bots. Un ejemplo paradigmático es la del "soldado Foster" generada por IA en Instagram y presentada como heroína de la guerra iniciada por EEUU e Israel en Irán, que consiguió en tiempo récord más de un millón de seguidores pensando que era una persona real. O los numerosos deepfakes usados en campañas de desinformación orientadas a influir en las elecciones de los países democráticos, como ha sido el caso de EEUU o el Brexit.

A medida que se recurre a asistentes de IA o a redes sociales para informarse —sobre todo entre los jóvenes— con mensajes en los que es difícil saber qué es real y qué no lo es, las empresas que controlan esos sistemas acumulan un poder político extraordinario, ya que controlan qué información

se ofrece y cómo, qué argumentos se presentan y qué contenidos se ocultan.

Las *Big Tech* dominan infraestructuras, "nubes", algoritmos y datos, con capacidad de control y manipulación social que posibilita una vigilancia eficiente y una predicción efectiva de comportamientos a través del análisis de los datos individuales (firma digital) que aportamos en nuestra vida cotidiana. Y tienen una influencia y control que asumimos en nuestros comportamientos, en lo que vemos y en lo que pensamos, sin ser conscientes de ello, pudiendo generar *mensajes hiper personalizados* e influir sobre cómo pensar o votar.

En paralelo, la expansión de las *Big Tech* y de la IA tiene impactos ambientales crecientes por su desmesurada demanda de energía, agua, la generación de residuos y la dependencia de materiales críticos. Riesgos ambientales crecientemente negativos que tienden a minimizarse aludiendo a los potenciales de la IA para la transición energética, la descarbonización y la sostenibilidad que están lejos de materializarse por ahora.

La Unión Europea cuenta con una regulación sobre el riesgo en el uso de la IA que exige transparencia sobre los grandes modelos de lenguaje, de los que se desconoce la información y entrenamiento en los que se basan, o sobre los criterios de aplicación de sus algoritmos. Pero las *Big Tech* se niegan a proporcionar la información exigida, que consideran secreto comercial. Son apoyadas por Trump, que está impulsando una desregulación federal en EEUU que plantea problemas serios para la seguridad y derechos de las personas. Sirva como ejemplo el avanzado uso de la IA en la edición genética y su uso no ético o para producir armas biológicas letales.

El desafío central es quién y cómo controla a las *Big Tech* y a los Gobiernos que poseen una IA que vigila y condiciona a los ciudadanos y a las empresas, cuyos avances son más rápidos que la capacidad de los Estados para regularla. La IA también puede ser utilizada con fines éticos y al servicio del bien común, por lo que la Unión Europea debería aprovechar su capacidad tecnológica para conseguirlo. Porque la cuestión clave es quién va a determinar su futuro: si los dueños de las Big-Tech, con gobiernos autoritarios tipo Gran Hermano, o los gobiernos democráticos con capacidad de controlar y poner al servicio del bien común los nuevos desarrollos tecnológicos. **TEMAS**