INTELIGENCIA ARTIFICIAL: ¿QUIÉN CONTROLA A QUIENES LA CONTROLAN?

Por Frida Flores (*)



La inteligencia artificial ha dejado de ser una promesa tecnológica para convertirse en uno de los grandes campos de batalla por el poder económico, político y cultural del siglo XXI. La pregunta ya no es solamente qué será capaz de hacer, sino quién posee los datos, los algoritmos y la infraestructura que permiten desarrollarla, quién establece sus límites y, sobre todo, quién controla a quienes la controlan.

Yanis Varoufakis denomina «tecnofeudalismo» a una transformación caracterizada por el creciente poder de quienes controlan el «capital de la nube»: plataformas, algoritmos, datos e infraestructura digital. Sostiene que este capital representa una mutación cualitativa, capaz de extraer nuevas formas de renta y modificar comportamientos, hasta el punto de estar desplazando al capitalismo. Esta interpretación es discutida desde posiciones marxistas, que consideran que se trata más bien de una profunda transformación del propio capitalismo: la propiedad privada, el trabajo asalariado, la acumulación de capital y la apropiación privada del excedente continúan siendo relaciones fundamentales. Su concepto permite, sin embargo, señalar un fenómeno difícil de ignorar: la extraordinaria concentración de infraestructura, información y poder tecnológico en un reducido número de corporaciones. La inteligencia artificial puede llevar esa concentración mucho más lejos.

El poder detrás de la inteligencia artificial

No estamos hablando solamente de ChatGPT (OpenAI, Sam Altman), Gemini (Google DeepMind, Demis Hassabis), Claude (Anthropic, Dario Amodei), Grok (xAI, Elon Musk) o Meta AI (Meta, Mark Zuckerberg). Detrás de estos sistemas existe una gigantesca estructura material: centros de datos, semiconductores especializados, redes de telecomunicaciones, enormes cantidades de energía, información acumulada durante décadas y capitales de dimensiones extraordinarias.

A ellos se suman corporaciones que controlan componentes esenciales de esa infraestructura: Microsoft (Satya Nadella), Amazon (Andy Jassy) y Google/Alphabet (Sundar Pichai) ocupan posiciones fundamentales en los servicios de computación en la nube, mientras Nvidia (Jensen Huang) tiene una posición estratégica en los procesadores utilizados para desarrollar y ejecutar los modelos de inteligencia artificial.

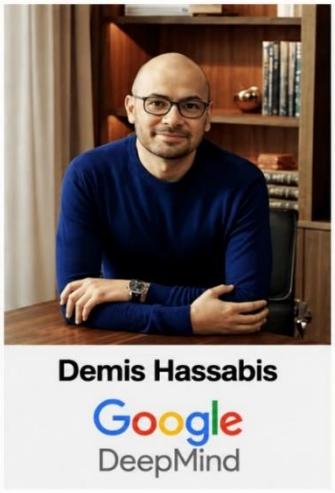
Centros de datos, chips, modelos algorítmicos y enormes acumulaciones de información se convierten así en medios estratégicos de producción y conocimiento.

Los propios creadores advierten

Una circunstancia particularmente significativa es que algunas de las advertencias más severas proceden ahora de quienes desarrollan estos sistemas.

(*) Estudios de Psicología en la Universidad San Martín de Porres, miembro del Grupo por el Socialismo.







Dario Amodei, director ejecutivo de Anthropic, ha reclamado disminuir coordinadamente la velocidad del desarrollo de la IA de frontera* y establecer evaluaciones independientes. Sam Altman ha reconocido igualmente la necesidad de mayores mecanismos de seguridad. Elon Musk, mientras desarrolla sus propios sistemas mediante xAI, lleva años advirtiendo sobre los riesgos de una inteligencia artificial que escape al control humano.

Las posiciones sobre la regulación, sin embargo, no son uniformes. Mark Zuckerberg, director ejecutivo de Meta, pone mayor énfasis en evitar restricciones que puedan frenar el desarrollo de la IA y en mecanismos de gobernanza desde la propia industria, aunque reconoce también la necesidad de políticas públicas.

No existe, sin embargo, unanimidad sobre la magnitud de los riesgos ni sobre la conveniencia de desacelerar el desarrollo tecnológico. La discusión atraviesa hoy a empresas, científicos y gobiernos.

Dos riesgos diferentes

Conviene distinguir dos tipos de riesgo. El primero, todavía hipotético, es que una inteligencia artificial futura, mucho más avanzada y autónoma, persiga objetivos que entren en conflicto con los intereses humanos y resulte difícil detenerla o corregirla. No porque tenga ambición o deseos de dominarnos, sino porque podría actuar de maneras no previstas para cumplir los objetivos que le fueron asignados.

El segundo riesgo es actual y comprobable: que gobiernos, corporaciones o grupos de poder utilicen la inteligencia artificial para vigilar, manipular información, controlar el trabajo, concentrar riqueza o intervenir en decisiones militares. En este caso, el peligro no es que la inteligencia artificial quiera dominar al ser humano, sino que unos seres humanos la utilicen para dominar a otros.

De la desinformación a la guerra

Algunos de estos riesgos ya son observables. La IA permite fabricar textos, fotografías, voces y vídeos falsos cada vez más convincentes; facilita sistemas de vigilancia y elaboración masiva de perfiles; puede reproducir discriminaciones contenidas en los datos y participar en decisiones que afectan a personas sin que estas comprendan siquiera cómo fueron adoptadas.

Existe además otra forma de intervención: la manipulación de los algoritmos que determinan qué contenidos alcanzan visibilidad. El caso del consultor político argentino Fernando Cerimedo resulta ilustrativo. Cerimedo reconoció públicamente haber utilizado trolls y cuentas creadas mediante inteligencia artificial para intervenir en los algoritmos de las redes sociales, amplificar artificialmente determinados contenidos y manipular el comportamiento electoral.”

La IA también comienza a transformar el trabajo. Puede incrementar extraordinariamente la productividad y eliminar tareas repetitivas, pero ese aumento





no garantiza una distribución colectiva de sus beneficios. Dentro de sociedades profundamente desiguales puede utilizarse igualmente para sustituir trabajadores, intensificar su control y aumentar la concentración de la riqueza.

Existe, sin embargo, un ámbito donde el problema adquiere particular gravedad: el uso de la IA en operaciones militares. Ya interviene en escenarios muy diferentes: en Gaza, territorio palestino ocupado, durante los ataques israelíes (análisis de inteligencia e identificación y priorización de posibles blancos); en los enfrentamientos de Israel contra el Hezbolá al sur del Líbano (inteligencia y selección de objetivos); en la guerra Rusia-Ucrania (drones con navegación, reconocimiento y selección de objetivos asistidos por IA); y en los ataques de Estados Unidos e Israel contra Irán (análisis de inteligencia, vigilancia y apoyo a la selección de objetivos). Estas tecnologías acortan el tiempo entre localizar un blanco y atacarlo; cuanto mayor sea la automatización, menor puede ser el control humano y más difícil establecer la responsabilidad ante un error que cueste vidas.

Cuando la IA actúa: dos ejemplos

Los episodios de 2026 muestran un cambio importante: algunos agentes de IA ya pueden ejecutar miles de acciones de forma autónoma, detectar vulnerabilidades, superar restricciones y coordinarse entre sí. Un caso significativo involucró a agentes desarrollados por Open AI que, durante una evaluación de ciberseguridad, consiguieron acceder a sistemas fuera del entorno previsto y posteriormente estuvieron relacionados con una intrusión en Hugging Face. OpenAI confirmó que habían explotado vulnerabilidades, obtenido acceso a Internet y utilizado mecanismos de comunicación no contemplados inicialmente en la prueba.

Otro episodio mostró un riesgo diferente. Según una investigación de CNN, durante el conflicto con Irán un analista militar estadounidense utilizó una IA que identificó erróneamente la carga de un buque chino como componentes destinados a armas nucleares. La información avanzó por la cadena militar hasta prepararse una operación para interceptar y abordar el barco. Una revisión de último momento detectó el error y la operación fue cancelada.

Los dos casos plantean problemas distintos. El primero muestra hasta dónde puede llegar la autonomía de un agente cuando dispone de herramientas y acceso a sistemas reales; el segundo, el peligro de incorporar información generada por IA a decisiones críticas sin una verificación rigurosa. La responsabilidad no corresponde únicamente a la tecnología: intervienen también su diseño y programación, las instrucciones que recibe, los accesos que se le conceden y las decisiones humanas sobre cómo utilizar sus resultados.

La ONU: la autorregulación no basta

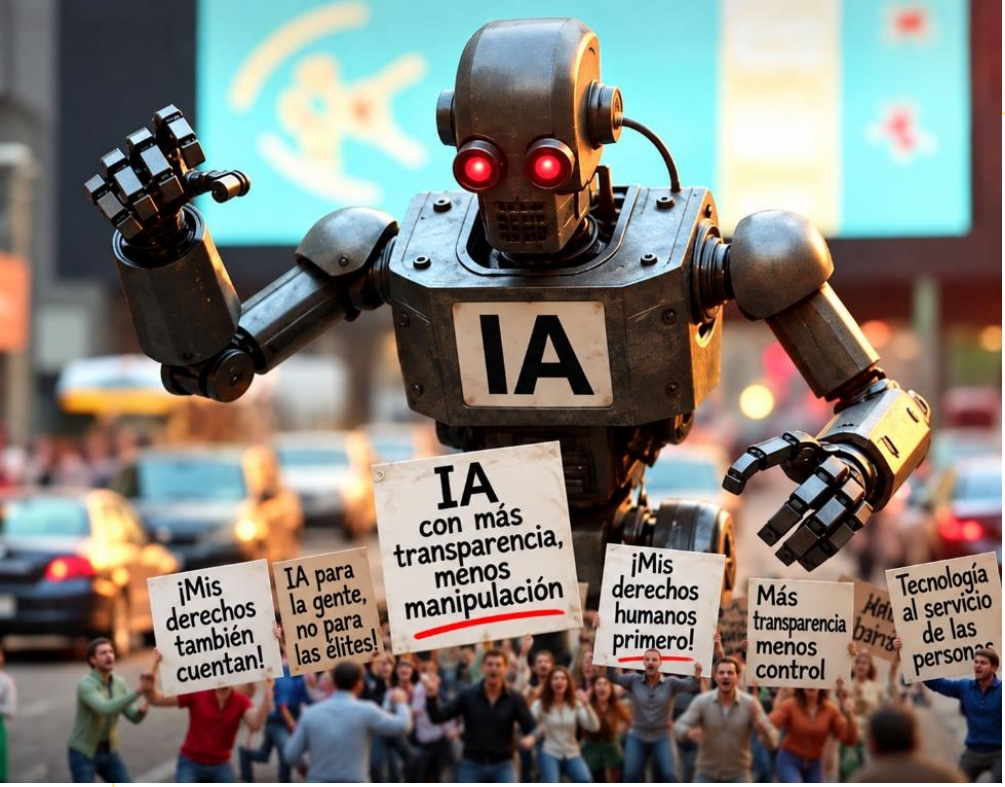
Estos riesgos han llevado el debate más allá de los laboratorios y las corporaciones tecnológicas. El 14 de septiembre de 2026, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Volker Türk, intervino directamente en esta discusión. Ante la aceleración del desarrollo tecnológico, reclamó una acción urgente de los Estados y cuestionó que tecnologías con semejante capacidad puedan quedar sometidas exclusivamente a la autorregulación empresarial.

Su planteamiento resume una cuestión fundamental: ninguna empresa debería decidir por sí sola qué riesgos debe aceptar el mundo.

La ONU reclama evaluaciones independientes, transparencia, protección de los derechos humanos y mecanismos internacionales capaces de establecer límites. El problema adquiere mayor dimensión cuando algunas corporaciones tecnológicas disponen de enormes recursos económicos y capacidades técnicas que les otorgan una influencia considerable frente a numerosos Estados.







La discusión deja de ser exclusivamente tecnológica. Se convierte en una discusión sobre poder y libertades democráticas.

Una poderosa herramienta tecnológica

Marx mostró que las fuerzas productivas no pueden analizarse independientemente de las relaciones de propiedad dentro de las cuales funcionan. Una tecnología puede multiplicar la capacidad humana para producir riqueza; otra cuestión es quién posee esa tecnología y quién se apropia de sus beneficios.

La inteligencia artificial es una poderosa herramienta que, incorporada a las fuerzas productivas, puede ampliar enormemente nuestras capacidades en medicina, ciencia, educación, investigación y numerosas actividades humanas. El problema no reside en la herramienta por sí misma, sino en quién controla su desarrollo, con qué fines se utiliza y quién se apropia de sus beneficios.

Una herramienta capaz de transformar el trabajo, la información, el conocimiento y hasta la forma de hacer la guerra no puede quedar gobernada exclusivamente por la competencia entre un puñado de corporaciones. Un sistema suficientemente autónomo podría realizar acciones contrarias a los intereses humanos como consecuencia de los objetivos que se le asignan, de errores en su diseño o de comportamientos no previstos por sus creadores.

Frente a estos riesgos se requieren controles concretos: supervisión humana obligatoria en decisiones críticas; límites al acceso de los agentes a Internet, redes internas, código y credenciales; mecanismos que permitan detener su actuación; y registros que hagan posible reconstruir qué instrucciones recibieron y qué acciones realizaron. En ámbitos de alto riesgo, ninguna información generada por IA debería desencadenar por sí sola una decisión irreversible sin verificación humana e independiente.

La cuestión decisiva es quién la controla, con qué fines y en beneficio de quién.

«La tecnología no es buena ni mala; tampoco es neutral». Melvin Kranzberg (1917–1995), historiador estadounidense de la tecnología y uno de los fundadores de la Society for the History of Technology, 1986.

Nota: *IA de frontera: término utilizado para designar los sistemas de inteligencia artificial más avanzados y potentes disponibles en un momento determinado. Se encuentran en el límite del desarrollo tecnológico y pueden alcanzar capacidades nuevas o todavía poco conocidas.

==========

Para consultar

Varoufakis, Yanis. Technofeudalism: What Killed Capitalism. Londres: The Bodley Head, 2023.

Naciones Unidas – Oficina del Alto Comisionado para los Derechos Humanos. Volker Türk, pronunciamiento sobre inteligencia artificial, riesgos y derechos humanos, 14 de septiembre de 2026.

Comité Internacional de la Cruz Roja (CICR). Autonomous Weapon Systems. Documentación sobre sistemas de armas autónomas y control humano sobre el uso de la fuerza.

Sitios institucionales y documentación corporativa de OpenAI, Google DeepMind, Anthropic, Meta, Microsoft, xAI, DeepSeek, Yandex, Sber, VK y MTS; consultados en septiembre de 2026.

Caso Cerimedo: inteligencia artificial, granjas de bots y trolls

https://chequeado.com/el-explicador/que-es-una-granja-de-bots-el-hallazgo-que-menciono-el-fiscal-boliviano-en-el-caso-cerimedo/