ANGELA H. ZHANG

“No me preocupa que la IA nos mate; **me preocupa que nos matemos unos a otros por culpa de la IA”**

Angela Huyue Zhang es una voz experta en la regulación de la inteligencia artificial y la rivalidad tecnológica entre Estados Unidos y China, dos temas que mezclan innovación, geopolítica y economía, y están transformando las reglas del juego a nivel mundial.

TEXTO: **ELENA SANZ** FOTOGRAFÍA: **IRENE MEDINA**



Zhang analiza la carrera tecnológica entre China y EE.UU. desde la perspectiva de una persona nacida en el país asiático y afincada en California.

Angela Huyue Zhang nació hace 45 años en Zhanjiang, China, una ciudad de clima subtropical húmedo donde se habla el dialecto min nan. Fue la primera de su familia en estudiar en la universidad, y escogió Derecho porque "era una carrera competitiva y respetada", confiesa. Tardó unos años en darse cuenta de que también ponía en sus manos una herramienta muy útil para comprender las instituciones, los sistemas y el poder. Y a ello se ha dedicado concienzudamente en la última década.



Su trayectoria formativa empezó en la Universidad de Chicago, donde se licenció. Luego se mudó a Europa, donde trabajó varios años en Londres. Su trabajo le llevó de vuelta a su país, concretamente a Hong Kong, el tercer centro financiero más potente del mundo, después de Nueva York y Londres. Ha vuelto a EE. UU. y actualmente imparte clases en la Universidad de California del Sur, donde trata de transmitir al alumnado sus conocimientos sobre la intersección entre el derecho, la tecnología y la geopolítica.

Zhang investiga las dinámicas institucionales de la regulación y la gobernanza, poniendo especial énfasis en entender la rivalidad tecnológica entre Estados Unidos y China y la regulación mundial de la inteligencia artificial (IA). Es autora de dos libros que, de momento, no se han publicado en castellano: *High Wire: How China Regulates Big Tech and Governs Its Economy* y *Chinese Antitrust Exceptionalism: How The Rise of China Challenges Global Regulation*.

Hace más de dos siglos que el filósofo y jurista inglés Jeremy Bentham ideó una infraestructura penitenciaria en la que los presos vivían bajo la presión de sentirse permanentemente observados. Eso les hacía autorregularse sin necesidad de grilletes, comportarse correctamente sin necesidad de barrotes. Ahora esa "vigilancia de la mirada" se ha trasladado al mundo digital. En efecto, dependemos de las plataformas de redes sociales y, a menos que individualmente alguien decida mantenerse desconectado de internet, todos dejamos un montón de huellas digitales en el mundo *online* que nos hacen vivir bajo vigilancia permanente. Pero no por parte de los gobiernos, ojo, sino de las grandes empresas tecnológicas, que ocupan una posición muy importante en la economía moderna. Y no lo esconden, más bien al contrario: empresas como Meta se enorgullecen de que su principal activo competitivo sea el control de los datos de los usuarios.

Con los agentes de la IA generativa eso se amplifica: usarlos implica ceder una gran cantidad de información, incluyendo nuestro correo electrónico y nuestros datos financieros. Es verdad que cuanto más "poder" concedemos a los asistentes de IA, más nos pueden ayudar. Pero eso también nos coloca en una encrucijada, porque ponemos en manos de las grandes tecnológicas una enorme capacidad de control sobre los datos de los consumidores, de la que no existen precedentes. Lo saben casi todo sobre nosotros, incluso más que nosotros mismos. Y eso da bastante miedo.

Ser conscientes de ello es el primer paso para su regulación, aunque existe todo un abanico de opciones. No hay más que mirar las diferentes posturas que han adoptado Europa, China y Estados Unidos ante la misma realidad. ¿Nos las puede resumir? La Unión Europea ha aplicado tradicionalmente una normativa bastante estricta. Por eso, cuando Meta se planteó introducir en Europa Llama 3 —que es su modelo insignia de código abierto—, lo descartó rápidamente, porque era consciente de que utilizaba sin autorización una gran cantidad de datos de sus usuarios para entrenar su modelo de IA, y que el Reglamento General de Protección de Datos (RGPD) europeo no lo iba a dejar pasar.

Pero esa regulación estricta, que *a priori* nos parece positiva, también está recibiendo duras críticas porque se la considera un freno para la innovación. Al fin y al cabo, los datos son como la sangre que fluye por las venas de la economía digital. Y, al detener el flujo de datos, estamos bloqueando gran parte de las transacciones digitales y la innovación.

Sin modelos de código abierto, las empresas de la UE se volverán menos competitivas que otras grandes potencias. Aun así, Europa apuesta por defender los derechos humanos y respetar la libertad individual y la privacidad. Se aferra a sus valores tradicionales. Nada que ver con Estados Unidos, donde priman los intereses industriales y la influencia política que ejercen los grupos de presión. A nivel federal, de momento no contamos con una normativa única, al estilo del RGPD. La regulación en materia de datos le corresponde a los estados. Pero incluso en el estado de California, donde resido y que cuenta con la normativa sobre datos más progresista del continente, es mucho menos estricta que la que se ve en Europa.

> **"Empresas como Meta se enorgullecen** de que su principal activo competitivo sea el control de los datos de sus usuarios"

Por supuesto que a los tribunales llegan demandas de usuarios, que se suelen resolver basándose en el consentimiento del consumidor. Pero no representan un gran obstáculo para estas grandes empresas tecnológicas ya que, incluso cuando "pierden", lo perciben como un coste inherente a su actividad empresarial.

China sí tiene una Ley de Protección de la Información Personal muy similar al RGPD europeo, aunque no se aplica de la misma manera. Así es. Ambos textos legales se parecen mucho, pero en China su aplicación es extremadamente laxa. Tenerla no implica hacer que se cumpla. Ha habido un par de casos en que se ha aplicado, pero ambos estaban más relacionados con cuestiones de seguridad nacional que con una verdadera apropiación indebida de datos personales. El Gobierno chino entiende que si adopta una postura muy estricta con la regulación de datos estrangulará la innovación, y eso es algo que el gigante asiático no se puede permitir porque su economía está experimentando una desaceleración importante. Ahora mismo, el crecimiento económico y la innovación son la prioridad. Y si hay que escoger, la soberanía de los datos prevalece sobre la necesidad de proteger la libertad individual. ▶

Lo curioso es que cuando hablamos con los ciudadanos chinos, con la gente de a pie, no se les nota preocupados por la privacidad de sus datos. Piensan que lo que hace el Estado es lo mejor para la sociedad, que los mecanismos de seguridad que el Gobierno chino ha puesto en marcha hacen que las calles sean más seguras y que se reduzcan los robos, la delincuencia, los delitos con violencia... En ese sentido, defienden que se vive mucho mejor en China que, por ejemplo, en Londres. Y aceptan el precio que hay que pagar —la privacidad, la libertad individual— por el bien común.

En cambio, en un país democrático, donde hay más controles y contrapesos y más respeto por la libertad individual, el equilibrio se establece de forma muy diferente. En ese sentido, China es el polo opuesto a la Unión Europea.

Hace unas semanas, investigadores de Anthropic afirmaron que hoy en día hay más de un 10 % de posibilidades de que la IA pueda matar a un humano en la próxima década. ¿Qué le parece? Creo que debemos tomárnoslo con cautela, ya que también se especula que esas supuestas "revelaciones" sobre problemas de seguridad podrían ser, en realidad, una estrategia de *marketing* de la compañía. Todas esas advertencias de que la IA podría estar (o llegar a estar) fuera de control generan mucho miedo entre el público pero, a la vez, envían un mensaje muy claro a otros países: que la capacidad de los modelos de IA generativa de Estados Unidos es superior al resto. Por eso me mantengo en el escepticismo, prefiero cuestionar que esta cifra del 10 % tenga alguna base científica.

"Me inquieta que agentes de IA provoquen incidentes **capaces de generar tensiones geopolíticas**"

En cualquier caso, creo que existe una preocupación legítima sobre la forma en que los laboratorios líderes en el desarrollo de la IA están organizando sus campos de pruebas. Pero cabe preguntarse: ¿reducen deliberadamente las medidas de seguridad y por eso aparecen agentes incontrolables?

En China no necesitan recurrir al miedo para demostrar que son mejores. Además, están contentos con quedar segundos en esta carrera. Al fin y al cabo, ser el número uno es bastante arriesgado: exige invertir enormes recursos sin tener claro qué dirección tomar. Mientras que hay una presión tremenda sobre el número uno, el número dos conoce más o menos la trayectoria del primero. Esto le permite tomar atajos y llegar a la meta de forma más eficiente, ahorrando unos costes enormes. Esto tiene mucho sentido para los desarrolladores chinos, que no tienen suficientes chips ni manejan tanto capital.

Todo esto se entiende mejor si pensamos en China como un gran exportador. De momento, le va bastante bien exportando vehículos eléctricos y baterías solares. Y el siguiente paso es la inteligencia artificial. De hecho, ya está empezando a vender *tokens* al resto del mundo (las unidades de datos más pequeñas que necesitan los diferentes modelos de IA para procesar, interpretar y generar textos), así que no necesitan tener los mejores modelos. Pueden limitarse a ofrecer modelos de código abierto ligeramente inferiores, pero lo suficientemente buenos y a un precio superasequible. Esa es, diría yo, su nueva apuesta de exportación a gran escala.

Delegar muchas decisiones y resoluciones de problemas a la IA implica que, a veces, perdamos información en el proceso. Es realmente difícil rastrear cómo se tomó una decisión concreta. ¿Debería preocuparnos esa falta de transparencia? Si hay tanta controversia sobre la regulación de la IA es, precisamente, porque todavía no conocemos con exactitud cómo funciona el cerebro humano. Y si las redes neuronales en que se basa la IA se han construido a imagen y semejanza de nuestro cerebro, es imposible prever en qué momento pueden quedar fuera de control. Esa incertidumbre también explica muchas de las controversias actuales. Por ejemplo, por qué destacados expertos como Geoffrey Hinton y Yoshua Bengio[1], padres del *deep learning* o aprendizaje profundo, creen que esto va a acabar con nosotros en algún momento. O que, por el contrario, otras figuras destacadas, como Jensen Huang, CEO de Nvidia, aseguren que la IA es "más tonta que un gato".

Al final, todo nos conduce a una pregunta clave: ¿cómo regulamos en condiciones de incertidumbre? Para mí, la respuesta pasa por comenzar recopilando toda la información, toda la evidencia científica posible.

1 **Bengio, Y.** "*AI and Catastrophic Risk*" en *Journal of Democracy* (2023, vol. 34, 4, pp. 111-121). Disponible en: https://muse.jhu.edu/article/907692



"En China, si hay que escoger, la soberanía de los datos prevalece sobre la necesidad de proteger las libertades individuales"

Panóptico digital

¿Se definiría como una persona optimista respecto al futuro? Tengo sentimientos encontrados. Por un lado, no considero que la IA suponga una amenaza existencial para la humanidad ni me preocupa que se esté descontrolando. Creo que muchos de los incidentes que venimos observando hasta ahora se deben, en mayor o menor medida, a fallos humanos. Porque son incidentes que se habrían evitado si hubiéramos adoptado medidas de seguridad más adecuadas. En este sentido, considero que soy optimista.

A pesar de analizar fenómenos que ocurren en su país, paradójicamente los libros de Zhang no han sido traducidos al chino.

Lo que sí me preocupa, y mucho, es que el aumento de los incidentes de ciberseguridad pueda contribuir a más conflictos y desencadenar nuevos enfrentamientos entre países. Recientemente hemos visto cómo, a través de un chatbot de OpenAI, los agentes de IA obtuvieron acceso no autorizado a los servicios del Gobierno australiano. En principio, Australia mantiene buenas relaciones con Estados Unidos. Pero si un país sintiera que la tecnología de otro país está amenazando su infraestructura de información crítica, creo que no lo gestionaría como un simple incidente de ciberseguridad: se convertiría en una crisis geopolítica, e incluso podría desembocar en un conflicto militar. Ese tipo de consecuencias no deseadas sí me inquietan: incidentes con agentes de IA capaces de generar tensiones geopolíticas, de provocar un peligroso aumento de las fricciones.

En definitiva, no me preocupa que la IA nos mate, me preocupa que nos matemos unos a otros por culpa de la IA.