

•

Cómo la IA y el capitalismo de vigilancia están socavando la democracia

Por [Suresh Venkatasubramanian](#) | 21 de agosto de 2025

La IA está suavizando la individualidad de las personas y, en su lugar, las agrupa en grupos que se consideran con un comportamiento determinado. Imagen: [Jamillah Knowles & We and AI / People and Ivory Tower AI 2](#) / [Licencia CC-BY 4.0](#)

El 6 de marzo de 2025, Axios informó que el Departamento de Estado había lanzado un nuevo programa de vigilancia de redes sociales llamado "Catch and Revoke". El objetivo de este programa era utilizar inteligencia artificial para ayudar a revisar las huellas en redes sociales de decenas de miles de titulares de visas de estudiante y encontrar [evidencia de presuntas simpatías terroristas expresadas tras el ataque de Hamás a Israel](#).

Ya sea que esto le parezca un desarrollo aterrador, una aplicación emocionante de la IA, una flagrante violación de los derechos de la Primera Enmienda o incluso simplemente algo desconcertante, este incidente captura la dinámica de cómo se combinan la inteligencia artificial, la vigilancia y las amenazas a la democracia. En resumen: la promesa de la IA de predecir y controlar el comportamiento alimenta un círculo vicioso de vigilancia que inevitablemente desencadena abusos de poder.

A lo largo de la historia, los humanos siempre han buscado maneras de predecir (y controlar) el comportamiento, ya sea consultando un oráculo, lanzando huesos, leyendo hojas de té o incluso examinando la forma del rostro y el cuerpo de una persona para determinar rasgos de personalidad (lo cual parece terriblemente contemporáneo si comienzas a sumergirte en la literatura sobre "IA emocional"). A medida que las personas se volvieron más hábiles en la recopilación de datos de diversos tipos, surgió el campo de la estadística para ayudarlos a [usar datos para la predicción](#). (Uno de los hechos curiosos sobre la investigación de IA es que prácticamente todos los debates que uno encuentra sobre el uso apropiado de la inteligencia artificial en algún entorno social tienen paralelos en la historia, a

menudo mucho anteriores, que dejan claro que los esfuerzos para predecir y controlar el comportamiento nunca tuvieron que ver con la IA en absoluto).

El problema de usar datos para hacer predicciones es que el proceso puede utilizarse como arma contra la sociedad, amenazando los valores democráticos. A medida que se difuminan los límites entre los datos privados y públicos en la sociedad moderna, muchos no se darán cuenta de que su vida privada se está convirtiendo en datos para tomar decisiones sobre ellos. La IA ha potenciado estas capacidades, suavizando la individualidad de las personas y, en su lugar, agrupando a cada una en un grupo que se considera que se comporta de cierta manera. Y si bien los datos y la IA pueden usarse para el bien, la única manera de lograr estos resultados beneficiosos es con controles restrictivos y bien diseñados para evitar daños a la democracia, de forma similar a como lo hicieron los humanos con la energía nuclear.

El avance de la IA. La transición hacia la estadística, el big data, el aprendizaje automático y la ciencia de datos consistió en combinar las técnicas fundamentales para la predicción del comportamiento con la magia computacional y la obtención de grandes cantidades de nuevos tipos de datos. Todo esto se tradujo en representaciones vectoriales de alta dimensión que los algoritmos de aprendizaje automático procesaron y escupieron. Estos algoritmos son expertos en encontrar patrones en los datos y utilizarlos para realizar predicciones sobre el futuro. A medida que las técnicas para aprender patrones a partir de los datos se volvieron más complejas, generando una amplia gama de métodos (supervisados, no supervisados, semisupervisados, en línea, reforzados), la naturaleza de los datos y el tipo de predicción requerida se volvieron menos importantes que la caja mágica intermedia utilizada para realizar la extrapolación. Los humanos habían descontextualizado el problema de la predicción.

Encontrar patrones que pretendan predecir el comportamiento de las personas es solo el primer paso. El impulso de la "IA para el bien" surge rápidamente aquí: si los responsables pueden predecir cómo se comportan las personas en diferentes circunstancias, quizá puedan ayudarlas a alcanzar su mejor versión. Si los expertos pueden predecir quiénes son propensos a tener malos hábitos financieros, quizá puedan orientarles más educación o impulsarles hacia mejores prácticas. Si los educadores pueden predecir qué estudiantes tendrán dificultades en la escuela, quizá puedan destinar más recursos para ayudarlos. Un [artículo](#) reciente sobre IA y bienestar en Marie Claire ejemplifica esta idea: ¿Qué pasaría si, con

la ayuda de la IA, su reloj no solo pudiera detectar enfermedades y problemas de salud antes de que surjan, sino también comunicarse directamente con nuestros médicos para indicarnos el tratamiento adecuado? ¿Qué pasaría si pudiera comunicarse con el resto de sus dispositivos en tiempo real y optimizar su entorno para que su dormitorio estuviera preparado para un sueño reparador, mantuviera su refrigerador lleno con los alimentos que su cuerpo realmente necesita y su equipo de fitness en casa calibrado para brindarle el entrenamiento más efectivo según su nivel de energía? ¿Qué pasaría si, con la ayuda de la IA, todo su entorno vital pudiera estar tan optimizado que estuviera inmerso en el tipo exacto de bienestar que su cuerpo y mente necesitan en cada momento, sin mover un dedo?

RELACIONADO:

Por qué Estados Unidos debe proteger la independencia de su regulador nuclear

Lo que hace que la predicción de IA sea tan poderosa y lucrativa es su capacidad para controlar lo que sucederá a continuación. Si un banco puede afirmar que predice qué harán las personas con un préstamo, puede usar esa información para decidir si deben obtenerlo. Si un funcionario de admisiones puede afirmar que predice el rendimiento de los estudiantes en la universidad, puede usar esa información para decidir a qué estudiantes admitir.

El comercio de datos. Una vez que las personas usan la IA para "saber" algo sobre sí mismas, alguien venderá esa información a alguien que no solo quiere "saber" algo sobre una persona o un grupo de personas, sino también obtener un comportamiento específico de esa persona o personas que pueda surgir de ese conocimiento.

Los expertos han comentado copiosamente sobre esta dinámica (de recopilación de datos con el único propósito de impulsar toda una empresa económica de comercio de datos), más prominentemente bajo el término general de "capitalismo de vigilancia". Lo que hace la IA es convertir esto en un trinquete de vigilancia, un dispositivo que solo va en una dirección, que es algo como esto: Para hacer las inferencias que quiero hacer para aprender más sobre ti, debo recopilar más datos sobre ti. Para que mis herramientas de IA funcionen, necesito datos sobre muchos de ustedes. Y una vez que haya recopilado estos datos, puedo monetizarlos vendiéndolos a otros que quieran usar la IA para hacer otras inferencias sobre ti. La

IA crea una demanda de datos, pero también se convierte en el resultado de la recopilación de datos.

El problema de estar inundado de datos e inferencias es que nunca se limita a un propósito inocente o bienintencionado. Casi de inmediato se convierte en un arma tentadora para quienes quieren ejercer el poder sobre una sociedad, con o sin el consentimiento de sus miembros. Y de ahí provienen las mayores amenazas a la democracia y la gobernanza democrática.

Líneas difusas. Considero la democracia de forma expansiva. Si la sociedad cree en un gobierno por, para y del pueblo, sus miembros deben sentirse cómodos expresándose en público, siendo ellos mismos en privado y con límites claros entre ambas esferas de actividad. Como nos han advertido innumerables académicos, la difuminación de estas líneas tiene graves consecuencias para la sociedad.

Pero esto es exactamente lo que hace la vigilancia impulsada por IA. Hay muchas esferas de la vida que las personas asumían que eran privadas o se les prometió que lo serían, pero debido a la vigilancia impulsada por IA se han empujado a la esfera pública, con graves consecuencias. En un régimen posterior a Dobbs, los rastreadores de datos menstruales ahora se utilizan para la búsqueda legal de solicitantes de aborto. De hecho, a principios de este mes, un jurado encontró que "Meta violó la Ley de Invasión de la Privacidad de California cuando registró intencionalmente la información de salud sensible de millones de mujeres a través de la aplicación de seguimiento del período Flo". En su búsqueda de objetivos de deportación, ICE ahora está utilizando la información médica y financiera más privada de las personas compartida con el gobierno con la promesa de protección de la privacidad. Los dispositivos Echo de Amazon han sido objeto de órdenes judiciales por las grabaciones de audio realizadas por el dispositivo dentro de nuestros hogares, grabaciones que se realizaron incluso cuando las personas presentes no estaban hablando directamente con el dispositivo. (En mi casa tenemos discusiones políticas ruidosas y entusiastas y hemos desconectado nuestro Echo por completo por temor a que nuestras declaraciones sean malinterpretadas más tarde).

Lo que antes se creía privado ya no es privado. Además, existen cosas que sabíamos que eran públicas —más o menos—, pero que nunca imaginamos que serían sacadas de contexto y convertidas en armas. Los timbres Ring de Amazon miran hacia afuera, hacia nuestras calles, nuestros vecinos y a todo aquel que llama a nuestra puerta. Puede que la gente no espere privacidad en público, pero ¿esperarían que la policía controlara la señal de video del timbre de

un vecino para evaluar el grado de amenaza si agitaran las manos violentamente en una animada discusión sobre su jardín o un incidente en nuestro vecindario? Eso es lo que el nuevo —y antiguo— CEO de Ring quiere hacer con los ahora omnipresentes timbres .

Las publicaciones en redes sociales ciertamente no son privadas. Pero cada persona tiene su propio estilo y personalidad al publicar, y el estallido más común en redes sociales es cuando alguien reenvía la publicación de otra persona fuera de contexto y provoca una avalancha de críticas en internet. Ahora bien, ¿qué sucede si esa publicación fuera de contexto es procesada por IA para determinar si quien la reenvía es simpatizante de terroristas, como propone el Departamento de Estado ? ¿Y si esas publicaciones se combinan con imágenes de vigilancia de una cámara Ring mientras una persona marcha por la calle como parte de una protesta, lo que ahora se interpreta como simpatizante de una organización terrorista? Lo público ahora está vigilado, y lo privado ahora es público.

RELACIONADO:

Cómo afectará la prohibición regulatoria del Partido Republicano a la carrera global de la inteligencia artificial

Homogeneización del comportamiento. Existe un argumento para defender el uso de la IA en la vigilancia. Dice así: «Estos sistemas de vigilancia son malos porque son imprecisos, y la IA lo solucionará».

Este ha sido un razonamiento común en los debates sobre reconocimiento facial, donde las primeras críticas a estos sistemas se centraron en su incapacidad para reconocer tonos de piel más oscuros o características faciales que no sean masculinas y blancas. El problema es que la IA no solucionará esto. Las predicciones que hacen los sistemas de IA sobre nuestro probable comportamiento futuro se construyen, por diseño, a partir de patrones de comportamiento observados en muchas personas. Por lo tanto, cualquier afirmación de precisión no significa «sabemos cómo es probable que te comportes, Suresh, en este escenario». Significa «hemos decidido que tú, Suresh, eres miembro de esta clase de individuos que, en promedio, se comportan de esta manera».

Esta atenuación de nuestra individualidad, nuestras peculiaridades y nuestras tendencias únicas a reaccionar a los estímulos que nos rodean es la antítesis de la idea de la democracia como celebración de la originalidad. Es una inversión causal escalofriante. No se trata de tomar nuestras expresiones individuales de libertad y encontrar

puntos en común; se trata de eliminar todo lo que nos hace únicos y diferentes con fines de predicción y control. Y esto es intencional, no accidental.

El deseo de vigilar es bipartidista. Se trata de poder, no de política partidista. Esto parece difícil de aceptar ocho meses después del inicio de la actual administración, que ha ignorado todas las protecciones contra la vigilancia desenfrenada, la recopilación de datos y el (mal)uso de la IA que ha podido encontrar. Pero la tentación de recopilar datos y luego usarlos para la vigilancia es extremadamente fuerte, aún más dentro del gobierno, donde se recopilan tantos datos como si nada, y la gente confía (o se ve obligada a confiar) en las agencias gubernamentales para el manejo de algunos de sus datos financieros y personales más privados.

Diseñando controles. Esta situación plantea un dilema muy difícil para quienes (yo incluido) mantenemos la esperanza de que la sociedad pueda usar la IA y los datos para el bien común, y creemos que las personas solo necesitan las medidas de seguridad adecuadas para hacerlo. La facilidad con la que se puede violar el Estado de derecho, destruir las protecciones y abusar de los datos al servicio del poder plantea una gran pregunta sobre el riesgo de *cualquier* recopilación y uso de datos, incluso si existiera un propósito benigno desde el principio.

Aún no tengo una buena respuesta a la pregunta que he planteado.

Pero los dejaré, lectores del *Boletín*, con una imagen que nos recuerda la fundación de esta publicación. El desarrollo de la IA se presenta en países de todo el mundo como una "carrera armamentística". Los buenos casos de uso de la IA se convierten fácilmente, y con frecuencia, en malos. La producción de sistemas de IA requiere una enorme cantidad de recopilación de datos y consumo de energía. Las inferencias y los conocimientos generados por estos sistemas de IA pueden ser sumamente peligrosos en las manos equivocadas. Todo esto hace que la IA se parezca en gran medida a la energía nuclear: radiactiva, peligrosa y, sí, a veces útil. La única forma en que los humanos han podido aprovechar la energía nuclear es con controles restrictivos y bien diseñados, y si bien estos pueden haber limitado algunas oportunidades comerciales potenciales, en general han ayudado a mantener el mundo más seguro y libre que sin ellos. No veo forma de que sigamos utilizando la IA sin controles igualmente restrictivos y bien diseñados para evitar daños a nuestra democracia y sociedad, y preservar su libertad.

Nota del editor: este artículo fue producido con el apoyo del Future of Life Institute.

