

Vigilancia individual y fake news: cómo China usa los datos de las aplicaciones para controlar a los usuarios

En una entrevista con Infobae, la investigadora Aynne Kokas, autora de *Trafficking Data*, explica cómo la explotación de información digital, especialmente por parte de China, se usa para obtener ganancias comerciales y políticas



Por

[Martina Putruele](#)

13 de Noviembre de 2022

“¿Cómo se protegen los **datos de los usuarios**? ¿Dónde se almacena? Estas pueden parecer preguntas técnicas, indignas de la atención de la persona promedio. Sin



embargo, los flujos de datos globales entre los Estados Unidos y China hacen que los **problemas de protección de datos del consumidor** no sean solo un asunto nacional sino también internacional que moldea las relaciones entre estos dos países”.

Aynne Kokas es profesora de CK Yen en el Centro Miller y profesora asociada de estudios de medios en la Universidad de Virginia, Estados Unidos. La investigación de Kokas examina las relaciones entre los medios y la tecnología chino-estadounidenses. Su último libro, *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty*, explora las consecuencias internacionales de que las empresas estadounidenses y el gobierno de los Estados Unidos hayan ignorado la regulación de datos a favor del crecimiento explosivo y sin control de **Silicon Valley**, lo que en parte provocó que China emergiese como el principal moldeador de la gobernanza mundial de la información y la tecnología.

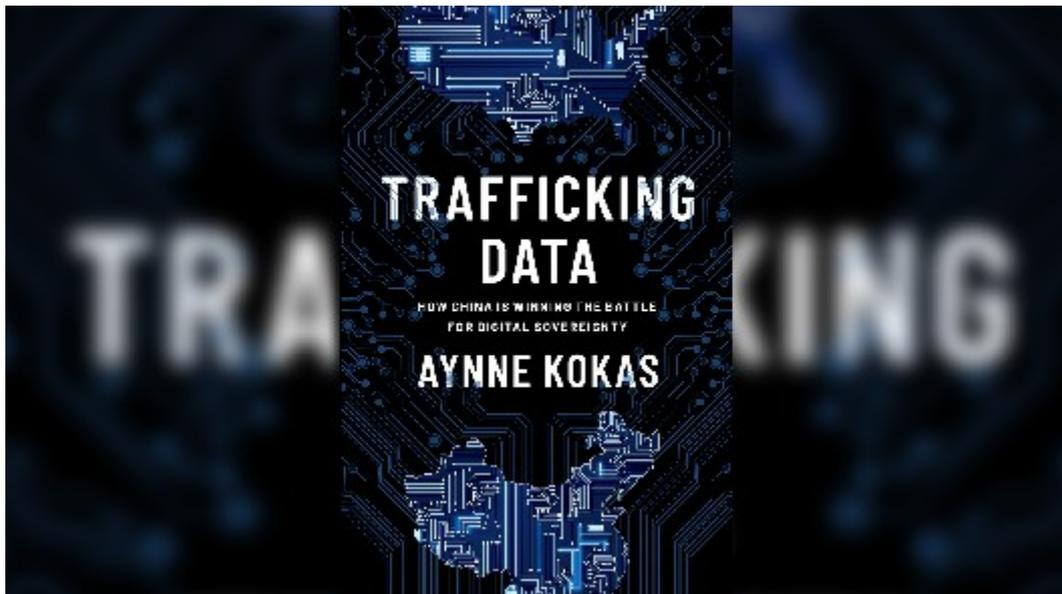
Basándose en años de trabajo de campo interno en los Estados Unidos y China, Kokas muestra cómo la explotación de datos se usa para obtener ganancias comerciales y políticas en el comercio entre los Estados Unidos y China y hace recomendaciones para mitigar los problemas económicos y de seguridad que resultan de este fenómeno.

Desde TikTok hasta las plataformas de juegos más populares, Aynne Kokas cuenta en una entrevista con **Infobae** por qué es importante entender cómo las empresas de tecnología recopilan nuestros datos y cómo el estado chino está capitalizando este flujo de datos para obtener ganancias políticas.

-¿Cómo define el tráfico de datos y de qué manera ocurre?

-El **tráfico de datos** es el movimiento no consentido de datos extraídos por corporaciones para uso de los gobiernos. Las formas clave en que esto ocurre son a través de **términos de servicio poco claros** y acuerdos de consentimiento en los que las corporaciones y los datos de los consumidores recopilan los datos de los usuarios, pero también a través de cosas como plataformas agrícolas u otros tipos de plataformas industriales. Luego, a través de marcos legales en lugares como **China**, que requieren el intercambio de datos de usuario. Hay un movimiento y una presión para compartir esos datos que se recopilan a través de acuerdos hechos por corporaciones con reguladores gubernamentales en el contexto chino, que es en el que me centro. Esto se vuelve realmente significativo porque el gobierno chino puede realizar auditorías de datos de seguridad nacional, lo que permite la adquisición a gran escala de datos de usuarios y una revisión a gran escala de datos de usuarios. También hay algo llamado **Fusión Civil Militar**, que permite al gobierno chino solicitar datos de corporaciones con el propósito de crecimiento militar.

Esto es un riesgo por tres razones. La primera es **la vigilancia de usuarios individuales**, que se siente como el tipo de preocupación más inmediata. La siguiente es la capacidad de desarrollar productos competitivos más robustos que podríamos usar en una era de competencia de IA tanto para la **competencia económica**. Pero también muchas de las herramientas o capacidades desarrolladas a través de los juegos, por ejemplo, también se pueden usar en un contexto militar y estamos viendo esto a través de cosas como **Tencent**, uno de los principales inversores de juegos. Y por último es **poder monitorear los patrones sociales y desarrollar campañas de desinformación** más específicas o incluso, en el caso de TikTok, alimentar ciertos tipos de información a través del algoritmo.



-¿Cómo es explotados los datos de un usuario por ejemplo en TikTok?

-La amplia gama de los datos de usuario se vuelve significativa. Incluye todo, desde su biometría, sus escaneos faciales, cómo interactúa con la aplicación, también descargar la aplicación puede recopilar información sobre todo lo que sucede en su teléfono. Y luego, por supuesto, sus preferencias, intereses. Ahora bien, esta información no es particularmente interesante o útil para vigilar o espiar a la mayoría de las personas allí. Vemos una especie de esfuerzos extraterritoriales para vigilar a los **ciudadanos chinos**, en particular a las personas de China que se han expatriado a otros países y vemos que esto ocurre no solo a través de la supervisión de las aplicaciones, sino también a través de cosas como las estaciones chinas que se han estado abriendo fuera de China.

-¿Quiénes son los principales actores del tráfico de datos en la actualidad?

-**Rusia**, por ejemplo, ha intentado, como saben, construir sus propias plataformas sociales incluso solo para uso local, pero no ha tenido tanto éxito. La razón por la que **China** es el ejemplo más significativo es por dos motivos. Uno, tienen una capacidad significativa para recopilar datos de usuarios porque hay plataformas muy populares. Y existen marcos geniales para transferir datos de usuario de manera muy clara. Ahora podemos ser críticos y creo que deberíamos ser muy críticos con las formas en las que las plataformas estadounidenses recopilaron y extrajeron datos a nivel mundial. Hemos visto que el gobierno de Estados Unidos ha trabajado con las corporaciones tecnológicas para recopilar datos sobre los usuarios. Pero también hemos visto en paralelo el tipo de fracaso del gobierno de los Estados Unidos para regular las plataformas tecnológicas del país, incluso en un nivel muy básico. Es por eso que cuando analizamos la extracción de datos de usuarios para uso generalizado por parte de los gobiernos, Estados Unidos no es necesariamente el ejemplo más significativo de esto, a pesar de que las empresas de **Silicon Valley** fueron pioneras en gran parte de este capitalismo de vigilancia extractivo.

-¿Y cómo pueden los países proteger nuestros datos y su soberanía digital?

-Creo que el primer paso es comprender que existe la **soberanía digital**. Las formas en que las personas usan las plataformas para servicios importantes, incluidos cosas como pagos o comunicación, se vuelven esenciales para pensar qué es realmente la soberanía en una nación y creo que eso es una desconexión que vemos en muchos casos. Ahora, la otra cuestión importante desde

el punto de vista de la política pública es desarrollar regulaciones nacionales de privacidad de datos. Por ejemplo, TikTok tiene diferentes términos de servicio en la Unión Europea que en los Estados Unidos porque están obedeciendo las leyes locales cuando esas leyes locales no existen. Entonces es muy difícil proteger realmente los datos de los usuarios.

-Qué países cuentan con protecciones para salvaguardar a las personas y, por supuesto, los datos del gobierno. ¿Y cuáles son estas protecciones?

-Países como **Japón, India, Australia, Corea del Sur y los de la Unión Europea** cuentan con protecciones de datos nacionales. Países como India tienen requisitos de localización de datos, lo que significa que los datos deben almacenarse internamente en ese país. India incluso tiene una plataforma de ciudadanía digital donde los usuarios tienen una especie de identidad digital nacional. Entonces, hay diferentes niveles de soberanía digital y uno de los desafíos es que esto requiere altos niveles de inversión, experiencia y capacidad técnica. Y esto se vuelve particularmente desafiante para los países que no tienen esas capacidades.

QUAD CORE

SECTOR CLAMP

Far far away, behind the world mountains, far from the countries, Valais and Consonance



-Entonces, ¿por qué es tan difícil para Estados Unidos regular si tiene estas capacidades?

-Esta es una gran pregunta y pasé mucho tiempo investigando. Y una cosa que quedó clara al hablar con funcionarios estadounidenses es que el poder desenfrenado del sector tecnológico estadounidense es un motor del poder nacional e internacional. Por lo tanto, es muy difícil de regular porque hay **intereses financieros realmente significativos** en juego para mantener el statu quo existente. En Europa, Japón o Australia, aunque se trata de democracias desarrolladas, no cuentan con un fuerte cabildeo de las empresas tecnológicas de Silicon Valley como una especie de fuerza existencial.

-¿Es posible tener plataformas sociales, pagar a través de aplicaciones, ser parte del mundo digital sin que nuestros datos personales estén expuestos?

-No quiero aterrorizar a los usuarios individuales. Creo que es importante que los usuarios individuales presten atención a los datos que comparten y las plataformas que utilizan. Pero no creo que deban preocuparse de que el gobierno chino los rastree, a menos que sean disidentes o ciudadanos chinos con preocupaciones financieras, ya sabes, o cosas por el estilo. Ahora, creo que es esencial y realmente importante que las personas trabajen con sus funcionarios electos, trabajen en sindicatos, trabajen en organizaciones comunitarias por los derechos digitales y para que los datos de los usuarios sean más justos y transparentes.