TECNOLOGÍA Y SOCIEDAD

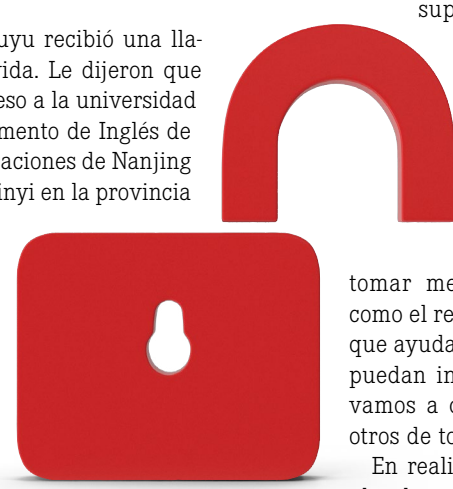
El **delirante** proyecto de **CHINA** para proteger la **privacidad** de los **datos**

MIT Technology Review
Publicado por Opinno

KAREN HAO
TRADUCIDO POR **ANA MILUTINOVIC**
26 DE OCTUBRE, 2021

Aunque parezca que el país no se preocupa por la información personal de sus ciudadanos, trabaja para controlar la recopilación y el uso por parte de las empresas. Lamentablemente, no aplica las mismas normas para el propio gobierno, que goza de bastante libertad para vigilar a sus ciudadanos.

A finales del verano de 2016, Xu Yuyu recibió una llamada que prometía cambiar su vida. Le dijeron que sus notas en los exámenes de ingreso a la universidad le habían valido la admisión al Departamento de Inglés de la Universidad de Correos y Telecomunicaciones de Nanjing (China). Xu vivía en la ciudad china de Linyi en la provincia costera Shandong, al sureste de Beijing (China). Su familia tenía pocos recursos. Todos dependían de los escasos ingresos de su padre, pero sus padres habían ahorrado arduamente para su matrícula; muy pocos de sus parientes habían ido a la universidad.



Unos días después, recibió otra llamada diciéndole que también le habían otorgado una beca. Para recibir los 2,600 yuanes (319 euros), primero tenía que depositar una «tarifa de activación» de 9,900 yuanes (1,325 euros) en su cuenta universitaria. Como había solicitado la ayuda económica solo unos días antes, Xu transfirió el dinero al número que le dio la persona que la llamó. Esa noche, la familia acudió corriendo a la policía para denunciar que habían sido estafados. El padre de Xu dijo más tarde que lo que más lamentaba fue preguntarle al policía si aún podían recuperar su dinero. La respuesta, «Probablemente no», solo empeoró la devastación de Xu. De camino a casa Xu sufrió un infarto. Murió en el hospital dos días después.

La investigación del caso determinó que, si bien la primera llamada había sido auténtica, la segunda provenía de estafadores que habían pagado a un *hacker* para conseguir el número de Xu, su estado de admisión y la solicitud de ayuda económica.

Para los consumidores chinos muy familiarizados con el robo de sus datos, Xu se convirtió en un símbolo. Su muerte provocó una protesta nacional para pedir mayores protecciones sobre la privacidad de datos. Solo unos meses antes, la Unión Europea había adoptado el Reglamento General de Protección de Datos (RGPD), en un intento de dar a los ciudadanos europeos el control sobre cómo se utiliza su información personal. Mientras tanto, Donald Trump estaba a punto de ganar las elecciones presidenciales estadounidenses, en parte gracias a una campaña que se basaba en gran medida en datos de los votantes, que incluían detalles sobre 87 millones de cuentas de Facebook, obtenidos ilegalmente por la consultora Cambridge Analytica. Los reguladores y juristas chinos seguían de cerca estos acontecimientos.

En Occidente existe una creencia generalizada de que ni el gobierno ni el pueblo chino se preocupan por la privacidad. Los gigantes tecnológicos estadounidenses utilizan esta supuesta indiferencia para argumentar que las complejas leyes de privacidad los pondrían en desventaja competitiva frente a las empresas chinas. En su testimonio en el Senado estadounidense en 2018 después del escándalo de Cambridge Analytica, el CEO de Facebook, Mark Zuckerberg, instó a los reguladores a no tomar medidas drásticas contra tecnologías como el reconocimiento facial: «Todavía tenemos que ayudar a que las empresas estadounidenses puedan innovar en esas áreas, de lo contrario vamos a quedar atrás de los rivales chinos y otros de todo el mundo».

En realidad, esta idea de las posturas chinas sobre la privacidad no representa la situación actual. En los últimos años, el gobierno chino, en busca de fortalecer la confianza y la participación de los consumidores en la economía digital, ha empezado a implementar protecciones de privacidad que, en muchos aspectos, se parecen a las actuales de América y Europa.

A pesar de que el gobierno chino ha reforzado la privacidad del consumidor, también ha intensificado la vigilancia estatal. Utiliza muestras de ADN y otros datos biométricos, como reconocimiento facial y de huellas dactilares, para controlar a los ciudadanos en todo el país. Ha aumentado la censura de internet y ha desarrollado un sistema de «créditos sociales», que castiga los comportamientos que, según las autoridades, debilitan la estabilidad social. Durante la

pandemia, implementó un sistema de *apps* de «código de salud» para indicar quién podía viajar, en función de su riesgo de tener coronavirus (COVID-19). También ha utilizado numerosas tecnologías invasivas de vigilancia en su dura represión de los musulmanes uigures en la región noroeste de Xinjiang (China).

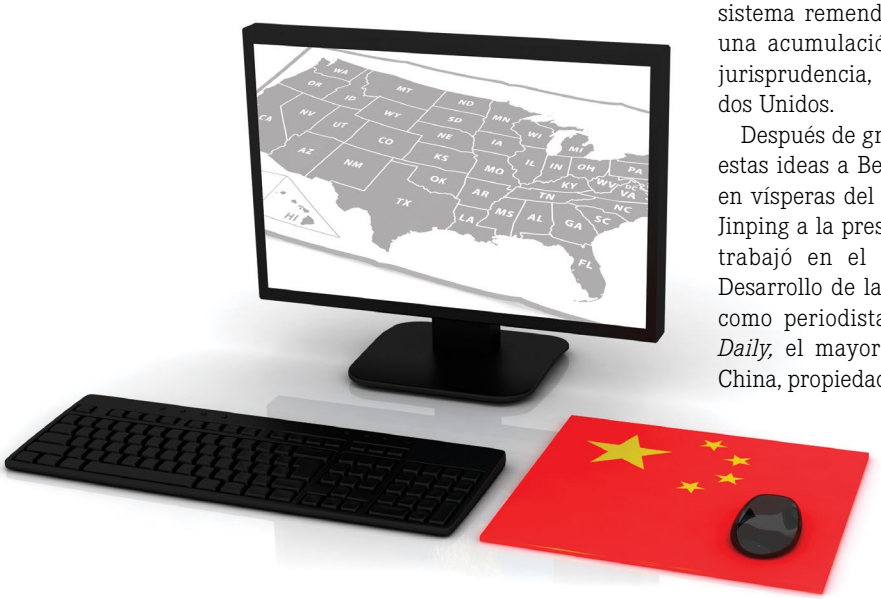
Según Samm Sacks, el destacado especialista en China de la Universidad de Yale (EE. UU.) y del grupo de expertos de Washington (EE. UU.) New America, esta paradoja se ha convertido en una característica definitoria del emergente régimen de privacidad de datos de China. De ahí surge la pregunta: ¿Puede un sistema perdurar con fuertes protecciones de la privacidad del consumidor, pero casi ninguna contra la intromisión gubernamental? La respuesta no afecta solo a China. Sus empresas de tecnología tienen una presencia cada vez más global y los reguladores de todo el mundo están atentos a sus decisiones políticas.

Se podría decir que noviembre de 2000 marcó el nacimiento del moderno Estado de vigilancia chino. Ese mes, el Ministerio de Seguridad Pública, la agencia gubernamental que supervisa la aplicación de la ley a diario, anunció un nuevo proyecto en una feria comercial en Beijing. La agencia ideó un sistema nacional centralizado que integraría la vigilancia física y digital utilizando la última tecnología. Su nombre: Escudo Dorado (Golden Shield).

Algunas empresas occidentales, con ganas de sacar tajada, como el conglomerado estadounidense Cisco, el gigante finlandés de telecomunicaciones Nokia y la canadiense Nortel Networks, trabajaron con esta agencia china en diferentes partes del proyecto. Ayudaron a construir una base de datos a nivel nacional para almacenar la información sobre todos los adultos chinos y desarrollaron un sistema sofisticado para controlar el flujo de información en internet, lo que más tarde se convertiría en el Gran Cortafuegos (Great Firewall). En realidad, gran parte del equipo usado ya había sido estandarizado para facilitar la vigilancia en EE. UU., como consecuencia de la Ley para la Asistencia de las Comunicaciones en el Orden Público de 1994.

A pesar del equipo estandarizado, el proyecto Escudo Dorado se vio obstaculizado por los silos de datos y las guerras territoriales dentro del gobierno chino. Con el tiempo, la idea del Ministerio de un sistema unificado se convirtió en dos operaciones separadas: un sistema de vigilancia y base de datos, dedicado a recoger y almacenar información, y el sistema de crédito social, en el que participan unos 40 departamentos gubernamentales. Cuando la gente repetidamente hace algo que no está permitido, desde cruzar la calle imprudentemente hasta involucrarse en la corrupción empresarial, su puntuación del crédito social cae y se les puede impedir comprar billetes de tren y avión o pedir una hipoteca.

el gobierno chino ha empezado a implementar las protecciones de la privacidad que se parecen a las actuales de Estados Unidos y Europa.

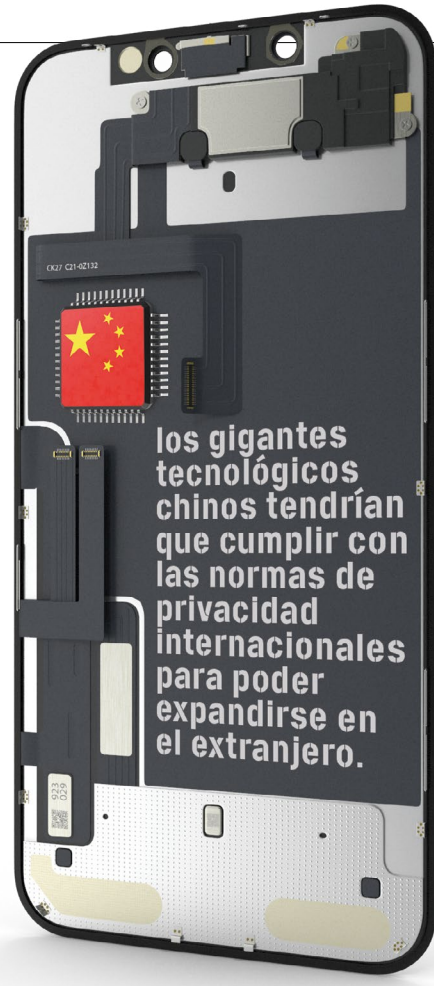


En el mismo año que el Ministerio de Seguridad Pública anunció el Escudo Dorado, Hong Yanqing entró a la Universidad de Policía del Ministerio en Beijing. Pero después de siete años de formación, al obtener su licenciatura y maestría, empezó a tener dudas sobre convertirse en policía. En cambio, pidió estudiar en el extranjero. En el otoño de 2007, se trasladó a los Países Bajos para realizar un doctorado en derecho internacional de los derechos humanos, aprobado y subvencionado por el gobierno chino.

Durante los siguientes cuatro años, se familiarizó con la práctica occidental del derecho a través de su investigación de doctorado y varías pasantías en organizaciones internacionales. Trabajó en la Organización Internacional del Trabajo sobre la ley global de discriminación en el trabajo y la Organización Mundial de la Salud sobre la seguridad vial en China. El experto resalta: «Es la cultura tan legalista de Occidente lo que realmente me sorprende. Parece que la gente acude mucho a los tribunales. Por ejemplo, para los derechos humanos, la mayoría de los libros de texto trata sobre importantes casos que resuelven problemas de derechos humanos».

Hong encontró que esto era extrañamente ineficiente. Para él, acudir a los tribunales era el recurso final para reparar las deficiencias de la ley, no una herramienta principal para establecerla en primer lugar. Creía que una legislación elaborada de manera más integral y con mayor previsión lograría mejores resultados que un sistema remendado mediante una acumulación fortuita de jurisprudencia, como en Estados Unidos.

Después de graduarse, llevó estas ideas a Beijing en 2012, en vísperas del ascenso de Xi Jinping a la presidencia. Hong trabajó en el Programa de Desarrollo de la ONU y luego como periodista del *People's Daily,* el mayor periódico de China, propiedad del gobierno.



Xi comenzó a expandir rápidamente el alcance de la censura gubernamental. Los comentaristas influyentes, o «Big V», llamados así por sus cuentas verificadas en las redes sociales, se habían sentido cómodos criticando y ridiculizando al Partido Comunista Chino. En el otoño de 2013, el partido arrestó a cientos de microblogueros por lo que describió como «propaganda maliciosa de rumores» y exhibió a uno especialmente influyente en la televisión nacional para convertirlo en un ejemplo.

Ese momento marcó el inicio de una nueva era de censura. Al año siguiente, se fundó la Administración del Ciberespacio de China. Esta nueva agencia central era responsable de todo lo relacionado con la regulación de internet, incluida la seguridad nacional, la censura de los medios de comunicación y del discurso, y la protección de datos. Hong dejó *People's Daily* y se unió al departamento de Asuntos Internacionales de la agencia. Lo representó en la ONU y en otros organismos internacionales y trabajó en la cooperación en ciberseguridad con otros gobiernos.

En julio de 2015, la Administración del Ciberespacio publicó el borrador de su primera ley: La Ley de Ciberseguridad, que entró en vigor en junio de 2017 y requería que las empresas obtuvieran el consentimiento de las personas para recoger su información personal. Al mismo tiempo, reforzó la censura de internet al prohibir los usuarios anónimos, una disposición impuesta por las regulares inspecciones gubernamentales de los datos de los proveedores de servicios de internet.

En la primavera de 2016, Hong quiso regresar al mundo académico, pero la agencia le pidió que se quedara. La Ley de Ciberseguridad había dejado la regulación de la protección de datos personales en un estado deliberadamente vago, mientras que las violaciones de datos de los consumidores y el robo habían alcanzado niveles insoportables. Un estudio de 2016 de la Sociedad de Internet de China encontró que el 84 % de los encuestados había sufrido alguna filtración de sus datos, incluidos sus números de teléfono, direcciones y detalles de las cuentas bancarias. Esto creaba una creciente desconfianza hacia los proveedores de servicios digitales que requerían acceso a información personal, como los servicios de transporte compartido, de entrega de alimentos y las *apps* financieras. La muerte de Xu Yuyu echó todavía más leña al fuego.

la creciente sensibilidad de la sociedad a las infracciones sobre la privacidad del consumidor no ha llevado a muchos límites a la vigilancia estatal.

Al gobierno le preocupaba que esas opiniones debilitaran la participación en la economía digital, que se había convertido en una parte central de su estrategia para reforzar el lento crecimiento económico del país. La aparición del RGPD también provocó que el gobierno chino se diera cuenta de que los gigantes tecnológicos chinos tendrían que cumplir con las normas de privacidad internacionales para poder expandirse en el extranjero.

Hong fue puesto a cargo de un nuevo grupo de trabajo que iba a redactar la Especificación de la Protección de la Información Personal (PIPS) para ayudar a resolver estos desafíos. Este documento, aunque no vinculante, iba a indicar a las empresas cómo los reguladores pretendían implementar la Ley de Ciberseguridad. En el proceso, según esperaba el gobierno, eso les empujaría a adoptar nuevas normas para la protección de datos por su cuenta.

El grupo de trabajo de Hong se dedicó a traducir al chino todos los documentos relevantes que pudo encontrar. Tradujeron las instrucciones sobre la privacidad publicadas por la Organización para la Cooperación y el Desarrollo Económicos y por su contraparte, la Cooperación Económica Asia-Pacífico; tradujeron el RGPD y la Ley de Privacidad del Consumidor de California (EE UU). Incluso tradujeron la Declaración de los Derechos de Privacidad del Consumidor de la Casa Blanca de 2012, adoptada por la administración de Obama, pero que nunca se convirtió en ley. Además, Hong se reunía regularmente con expertos y reguladores de protección de datos europeos y estadounidenses.

Poco a poco, con todos esos documentos y consultas, surgió una elección general. «La gente decía, en términos muy simplistas: ‹Tenemos el modelo europeo y el estadounidense›», recuerda Hong. Los dos enfoques divergían sustancialmente en su filosofía e implementación. La decisión de cuál seguir se convirtió en el primer debate del grupo de trabajo.

En el centro del modelo europeo se encuentra la idea de que las personas tienen el derecho fundamental a que sus datos estén protegidos. El RGPD responsabiliza a los recopiladores de datos, como las empresas, a demostrar por qué necesitan esos datos. Por el contrario, el modelo estadounidense privilegia la industria sobre los consumidores. Las empresas definen por sí mismas qué constituye una recogida de datos razonable; los consumidores solo pueden elegir si quieren utilizar ese servicio. Las leyes sobre la protección de datos también son

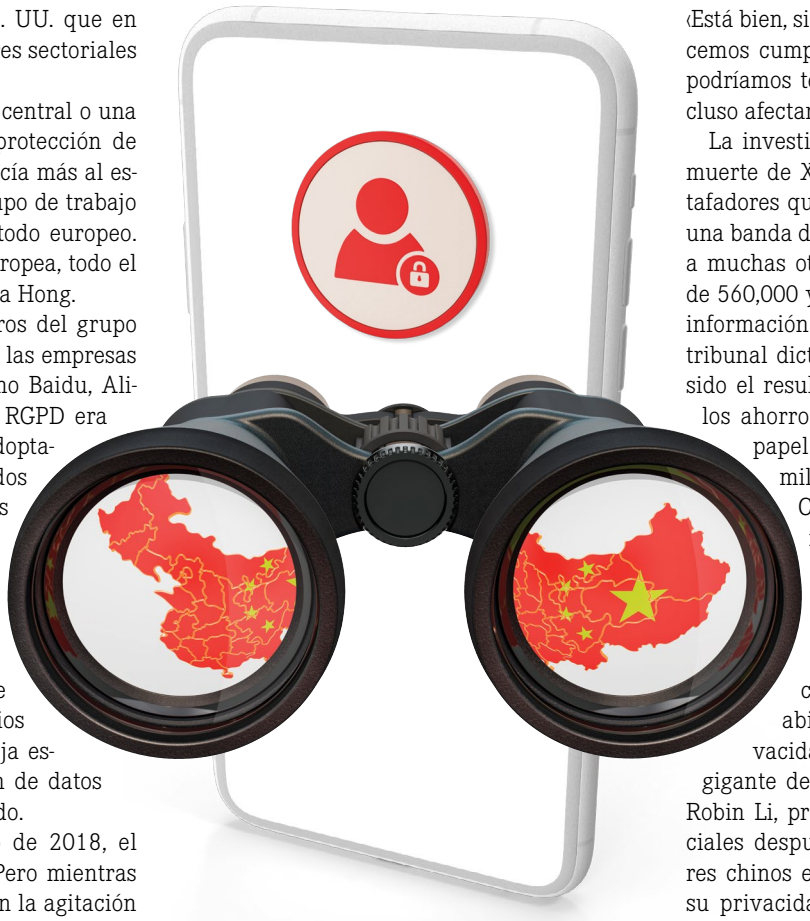
mucho más fragmentadas en EE. UU. que en Europa, divididas entre reguladores sectoriales y estados específicos.

En aquel momento, sin una ley central o una agencia única encargada de la protección de datos, el modelo de China se parecía más al estadounidense. Sin embargo, el grupo de trabajo encontró más convincente el método europeo. «La estructura de la normativa europea, todo el sistema, resulta más claro», explica Hong.

Pero la mayoría de los miembros del grupo de trabajo eran representantes de las empresas tecnológicas gigantes chinas, como Baidu, Alibaba y Huawei, y creían que el RGPD era demasiado restrictivo. Así que adoptaron sus rasgos generales, incluidos sus límites en la captación de datos y sus requisitos sobre el almacenamiento y la eliminación de datos, y luego aflojaron parte de su expresión. El principio de la minimización de datos del RGPD, por ejemplo, sostiene que solo se deben recopilar los datos necesarios a cambio de un servicio. PIPS deja espacio para otro tipo de captación de datos relevantes para el servicio prestado.

PIPS entró en vigor en mayo de 2018, el mismo mes en el que el RGPD. Pero mientras las autoridades chinas observaban la agitación de Estados Unidos por el escándalo de Facebook y Cambridge Analytica, se dieron cuenta de que un acuerdo no vinculante no sería suficiente. La Ley de Ciberseguridad no tenía un mecanismo sólido para hacer cumplir la protección de datos. Los reguladores solo podían multar a los infractores con hasta 1'000,000 yuanes (120,600 euros), una cantidad intrascendente para las grandes empresas. Poco después, el Congreso Nacional del Pueblo, el máximo órgano legislativo de China, votó para comenzar a redactar una Ley de protección de la información personal dentro de su actual período legislativo de cinco años, que finaliza en 2023. La idea consiste en fortalecer las disposiciones de la protección de datos, establecer sanciones más severas y probablemente crear una nueva agencia de ejecución.

Después del caso Cambridge Analytica, Hong recuerda: «La agencia gubernamental entendió: ‹Está bien, si realmente no implementamos o hacemos cumplir esas normas sobre privacidad, podríamos tener un enorme escándalo, que incluso afectaría los asuntos políticos›».



¿Puede un sistema perdurar con fuertes protecciones de la privacidad del consumidor, pero casi ninguna contra la intromisión gubernamental?

La investigación de la policía local sobre la muerte de Xu Yuyu al final identificó a los estafadores que la habían llamado. Se trataba de una banda de siete personas que había estafado a muchas otras víctimas por un valor de más de 560,000 yuanes (74,960 euros) utilizando su información personal obtenida ilegalmente. El tribunal dictaminó que la muerte de Xu había sido el resultado directo del estrés por perder los ahorros de su familia. Por eso, y por su papel en la organización de decenas de miles de otras llamadas, el cabecilla, Chen Wenhui, de 22 años, fue condenado a cadena perpetua. Los demás recibieron penas de prisión de entre tres y 15 años.

Con ese incentivo, los medios de comunicación y los consumidores chinos empezaron a criticar más abiertamente las violaciones de privacidad. En marzo de 2018, el CEO del gigante de las búsquedas en internet Baidu, Robin Li, provocó indignación en las redes sociales después de sugerir que los consumidores chinos estaban dispuestos a «intercambiar su privacidad por la seguridad, comodidad o eficiencia». «Tonterías. Es más exacto decir que [es] imposible defender [nuestra privacidad] de manera efectiva», escribió un usuario de las redes sociales, citado más tarde por *People's Daily*.

A finales de octubre de 2019, los usuarios de redes sociales expresaron una vez más su enfado después de que comenzaran a circular fotos de alumnos de una escuela con cintas de control de ondas cerebrales en sus cabezas, supuestamente para mejorar su atención y aprendizaje. La autoridad local de educación intervino y le dijo a la escuela que dejara de usar las cintas para la cabeza porque violaban la privacidad de los alumnos. Una semana después, un profesor chino de derecho demandó al Zoo de Vida Silvestre de Hangzhou por sustituir su sistema de entrada basado en huellas dactilares por reconocimiento facial, alegando que el zoológico no había obtenido su consentimiento para almacenar su imagen.

Pero la creciente sensibilidad de la sociedad a las infracciones sobre la privacidad del consumidor no ha llevado a muchos límites a la vigilancia estatal, ni siquiera a un escrutinio de la misma. Como señala la investigadora de Human Rights Watch Maya Wang, esto se debe en parte a que la mayoría de los ciudadanos chinos no conocen la escala o el alcance de las operaciones del gobierno. En China, igual que en EE. UU. y Europa, existen amplias exenciones de seguridad pública y nacional a las leyes de privacidad de datos. La Ley de Ciberseguridad, por ejemplo, permite al gobierno exigir datos a los actores privados para ayudar en las investigaciones y procesos penales. El Ministerio de Seguridad Pública también acumula enormes cantidades de datos sobre las personas. Como resultado, se puede reforzar la privacidad de datos en la industria sin limitar significativamente el acceso del Estado a la información.

Además, el inicio de la pandemia alteró este ya de por sí incómodo equilibrio.

El 11 de febrero, Ant Financial, el gigante de la tecnología financiera con sede en Hangzhou (China), lanzó la plataforma de creación de *apps* AliPay Health Code. El mismo día, el gobierno local hizo pública una *app* que había creado utilizando esta plataforma. La *app* de Hangzhou pedía a las personas que registraran por su cuenta su información de viajes y salud, y luego les daba un código de color rojo, amarillo o verde. De repente, los 10 millones de habitantes de Hangzhou debían mostrar el código verde para tomar el metro, comprar alimentos o entrar a un centro comercial. En una semana, los gobiernos locales de más de 100 ciudades habían utilizado AliPay Health Code para desarrollar sus propias *apps*. El gigante tecnológico rival Tencent lo siguió rápidamente con su propia plataforma para crearlas.

Las *apps* visibilizaron el preocupante nivel de vigilancia estatal y provocaron una nueva ola de debate público. En marzo de este año, el profesor de periodismo en la Universidad de Beijing y bloguero Hu Yong, argumentó que la recopilación de datos sobre la pandemia por parte del gobierno había cruzado una línea. No solo había dado lugar a casos de robo de información, escribió, sino que también había abierto la puerta a que esos datos se utilizaran más allá de su propósito original. «¿Ha demostrado la historia que una vez que el gobierno tenga herramientas de vigilancia, mantendría la modestia y la precaución al usarlas?», preguntó.

De hecho, a finales de mayo, unos documentos filtrados revelaron los planes del gobierno de Hangzhou de crear una *app* de código de salud permanente que calificara a los ciudadanos sobre distintos comportamientos como hacer deporte, fumar y dormir. Después de una protesta pública, las autoridades municipales cancelaron el proyecto. Los medios estatales también han publicado críticas sobre la *app*.

El debate llegó rápidamente al gobierno central. Ese mismo mes, el Congreso Nacional del Pueblo anunció que tenía intención de acelerar la Ley de Protección de la Información Personal. La escala de los datos recogidos durante la pandemia hizo que la aplicación de la ley fuera más urgente, según los delegados, que destacaron la necesidad de aclarar el alcance de los procedimientos de la recogida y eliminación de los datos por parte del gobierno durante las emergencias especiales. En julio, el órgano legislativo propuso un nuevo proceso de «aprobación estricta» para las autoridades gubernamentales antes de recopilar datos del sector privado. El lenguaje sigue siendo vago, para poder desarrollarlo más tarde, tal vez a través de otro documento no vinculante, pero esta medida «podría marcar un paso hacia una limitación del amplio alcance» de las exenciones gubernamentales existentes para la seguridad nacional, escribieron Sacks y otros expertos en China de New America.

Hong coincide en que la discrepancia entre las normas que rigen la recogida de datos de la industria y el gobierno no durará mucho, y que el gobierno pronto empezará a limitar su propio alcance. Y afirma: «No podemos dirigirnos a un actor y dejar fuera al otro. No sería un enfoque muy científico».

Otros analistas no están de acuerdo. El gobierno podría fácilmente hacer esfuerzos superficiales para abordar la reacción de la sociedad contra la recogida visible de datos sin tocar realmente el núcleo de las operaciones nacionales del Ministerio de Seguridad Pública, opina Wang, de Human Rights Watch, y añade que cualquier ley probablemente se aplicaría de manera desigual: «En Xinjiang, los musulmanes turcos no pueden decir nada sobre cómo son tratados».

Aun así, Hong sigue siendo optimista. El año pasado empezó a trabajar como profesor de derecho en la Universidad de Beijing y tiene un blog sobre ciberseguridad y problemas de datos. Cada mes, se reúne con la comunidad incipiente de responsables de la protección de datos en China, quienes observan cuidadosamente cómo evoluciona la gobernanza de datos en todo el mundo. **</>**

El artículo original «El delirante proyecto de China para proteger la privacidad de los datos.» pertenece a la edición digital de *MIT Technology Review*.