



Las TIC y la cibernsoberanía en China: la base del presidente Xi Jinping para perfeccionar el control social maoísta

Óscar Aribau Sorolla

Trabajo Final de Máster

Director: Dr. Jesús Solé-Farràs

Óscar Aribau Sorolla

Trabajo Final de Máster

Director: Dr. Jesús Solé-Farràs

Universitat Oberta de Catalunya (UOC), Zaragoza, julio 2018.

Máster Universitario “China y Japón: Mundo Contemporáneo”

| | |
|--|----|
| 1. Introducción | 4 |
| 2. Vigilancia y control social en la sociedad digital | 8 |
| Internet: de medio libertador a carcelero | 9 |
| La esfera pública y el control social en la ‘sociedad conectada’ | 12 |
| El autoritarismo en red | 14 |
| 3. La vigilancia y el control social en la República Popular China | 16 |
| La centralidad de la cibersoberanía | 17 |
| Censura, propaganda y vigilancia en la intranet china | 22 |
| El <i>big data</i> y el crédito social | 27 |
| 4. El control social de Xi Jinping frente al control social de Mao Zedong: análisis comparativo | 32 |
| 5. Conclusiones | 41 |
| Bibliografía | 46 |

1. Introducción

Desde 1948, la Declaración Universal de los Derechos Humanos de la ONU reconoce la privacidad y la intimidad de los individuos como uno de los derechos individuales a proteger en todo el mundo. En su artículo 12 asegura que “nadie será objeto de injerencias arbitrarias en su vida privada, ni su familia, ni cualquier entidad, ni de ataques a su honra o su reputación”. Pero, pese a este reconocimiento, la vida privada y la intimidad de los ciudadanos está constantemente sometida a la presión del interés general de los estados, y a menudo, los derechos y las libertades del individuo se ven socavados frente a los objetivos de las élites gobernantes que representan, al menos en principio, a la colectividad. Las estructuras de poder de cualquier sociedad, independientemente del sistema político elegido para su organización, han mirado con desconfianza el ámbito privado de los ciudadanos y lo han considerado como una parte oculta e inaccesible donde podría gestarse y germinar cualquier revuelta que terminara con el sistema político vigente. Incluso las garantistas democracias occidentales contemporáneas, escudadas en conceptos tan amplios como el de seguridad nacional, el mantenimiento de la estabilidad política o la prevención de delitos, se han esforzado en atravesar la frontera del círculo íntimo de los ciudadanos, incluso violando a escondidas sus derechos individuales, para obtener la mayor cantidad de información posible.

Para cualquier gobierno, el control de las comunicaciones y del ámbito privado de los ciudadanos se ha convertido en un elemento esencial para mantener la estabilidad y la legitimidad del sistema, aunque, quizás, uno de los casos más paradigmáticos es el de la República Popular China (RPCh). Desde su llegada al poder en 1949, el Partido Comunista Chino (PCCh) ha definido la intimidad y el círculo privado de los ciudadanos como los grandes enemigos del sistema. Durante casi 70 años, el PCCh y sus diferentes líderes han basado su hegemonía y su legitimidad en la eliminación del adversario y de la crítica, en el control absoluto de todos los ámbitos de la sociedad y la desaparición del ámbito privado de los ciudadanos, transformando en públicos todos los ámbitos sociales e individuales. Al transformar lo privado en público, el partido ha conseguido extender su control a todas las esferas de la sociedad, forjando su legitimidad en un control social basado en la conquista de los espacios íntimos de los ciudadanos.

Las reformas económicas y la transición de China hacia una economía de mercado hicieron suponer que la apertura al exterior traería aparejada una transición en el sistema

político: desde el autoritarismo hacia la democracia. La economía de mercado con características chinas, planificada y controlada por el gobierno, necesita un intercambio constante de información, y bajo esta premisa, muchos analistas supusieron que, una vez abierta la mano, al partido le sería imposible controlar tanto la gran cantidad de contenidos generados cómo quién los producía. Pero, la célebre frase de Deng Xiaoping, “un país, dos sistemas” era mucho más profética de lo inicialmente previsto. Si al principio era un llamamiento a Hong Kong, Taiwán y Macao para que volvieran a formar parte de la gran China porque el gobierno comunista era capaz de administrar un país con varios sistemas, el comunista en la zona continental y el capitalista en estas otras, con el paso del tiempo el mensaje de Deng podría aplicarse a cómo bajo el paraguas de un sistema socialista, se desarrolla un sistema económico de mercado planificado, con grandes características capitalistas, pero manteniendo un sistema de control social autoritario, a través del control férreo y exhaustivo de la información y las comunicaciones.

Tras la exitosa adaptación del autoritarismo chino a la economía de mercado, la digitalización supuso el otro gran desafío. Otra vez, parecía que el PCCh no sería capaz de soportar el golpe democratizador, en esta ocasión, de las tecnologías de la información y la comunicación (TIC). La economía globalizada, la desaparición de las fronteras y la ruptura del paradigma donde los estados tenían el monopolio de la información en favor de otro de múltiples emisores parecían factores determinantes para acabar con la hegemonía del PCCh. Pero, aunque el partido resistió la embestida de la digitalización, no fue hasta la llegada al poder del presidente Xi Jinping en 2012 cuando el autoritarismo chino empezó a utilizar toda la potencialidad de las TIC en su propio beneficio, es decir, como arma para mantener y recuperar la legitimidad perdida desde el inicio de las reformas económicas.

Cuando alcanzó el liderato, Xi se encontró con un sistema político y un partido erosionado por la creciente corrupción de cuadros y burócratas, y por el aumento de la desigualdad social fruto de exponencial crecimiento económico. Pero, en tan solo 6 años, Xi ha conseguido frenar la hemorragia de credibilidad y legitimidad tomando medidas encaminadas a fortalecer la jerarquía, la obediencia al líder y a eliminar a los adversarios reideologizando la sociedad y el partido para volver a situarlo en el centro de la vida de los ciudadanos. Para conseguir sus objetivos, el entorno digital se ha convertido en el aliado perfecto. Su concepto de cibersoberanía para diseñar la gobernanza de la red, que no es otra cosa que aplicar al mundo digital el concepto de soberanía nacional, es el que le ha permitido transformar las amenazas de las TIC en oportunidades. Por tanto, rechaza

una red global autoregulada, donde los gobiernos son meros espectadores de su evolución, y apuesta por un mundo cibernético al servicio de los intereses gubernamentales controlado y monitorizado para evitar que sea foco de conflictos que puedan minar la legitimidad del régimen.

A través de la cibersoberanía, el mundo virtual se convierte en una extensión más del real sometido al mismo poder, pero con infinitas posibilidades más de vigilancia y control por parte de los gobernantes. De hecho, el seguimiento digital que Xi Jinping ejerce sobre los ciudadanos ha conseguido perfeccionar el que Mao Zedong ejerció con mano de hierro durante décadas sobre la sociedad china. Manteniendo las directrices de la época maoísta, Xi ha seguido viendo los medios de comunicación como altavoces del gobierno y del partido para educar, organizar y movilizar a las masas, y como un elemento claro de control social en el que las TIC se han convertido, sin pretenderlo, en el aliado perfecto del autoritarismo. Con una tasa de penetración de internet, según el último informe disponible de la agencia gubernamental *China Internet Network Information Center* (CNNIC), del 53'2%, es decir, que más de la mitad de la población china es usuario de Internet, que el 95'1% de los *netizens* se conectan a través de su teléfono móvil o que el 67'5% de los *netizens* utilizaron algún sistema de pago electrónico a través un teléfono inteligente, la digitalización permite obtener gran cantidad de datos de los ciudadanos, sin que ellos sepan que están siendo espiados. En realidad, el *big data* se ha convertido en un recurso esencial para el control social y su efectividad está ligada a la fuerte implantación y uso de las tecnologías de la información y comunicación entre la ciudadanía.

La transformación digital del país, con un uso cada vez mayor de las TIC en la vida diaria de los ciudadanos, permite llegar hasta límites insospechados. De hecho, la agencia estatal de noticias *Xinhua*, anunciaba el 8 de abril de 2018 que 62 aeropuertos del país han puesto en marcha un sistema de reconocimiento facial para acelerar los controles de seguridad. Se trata de un sistema que compara la imagen captada por cámaras de seguridad situadas en los aeropuertos con la registrada en la base de datos del gobierno chino. El 27 de marzo de este año, el *South China Morning Post* aseguraba que la policía local de Shenzhen utilizará la inteligencia artificial (AI) y el reconocimiento facial para multar a los peatones que crucen la calle fuera del paso de peatones. Los infractores recibirán la notificación, de forma inmediata, a través de un SMS en sus teléfonos móviles.

Pero, lo que más ha sorprendido en Occidente ha sido el anuncio de la creación de un sistema de crédito social para el año 2020, una gran base de datos que unificará la información de confiabilidad financiera, registros industriales y comerciales, pagos de impuestos, seguridad social o infracciones de tráfico, y los traducirá en una cifra que marcará el grado de confiabilidad social de cada individuo. Sus conductas, las del mundo digital y analógico, estarán sintetizadas en un número que prohibirá ciertas actividades como, por ejemplo, viajar en tren de alta velocidad o avión. El sistema comenzó a construirse hace 3 años, incluyendo únicamente el historial de pago de impuestos, créditos y facturas, pero poco a poco, el gobierno ha ido añadiendo más información personal de los individuos. El crédito social del gobierno chino explota el *big data* que cada ciudadano genera por su presencia en la red. Incluye búsquedas, medios sociales, cámaras de vigilancia, geolocalización, transacciones comerciales e, incluso, en el internet de las cosas, y todo tratado a través de algoritmos y sistemas de inteligencia artificial.

Así pues, este trabajo quiere analizar cómo el gobierno de Xi Jinping está utilizando las TIC para aumentar el control que el gobierno chino ejerce sobre la sociedad, perfeccionando el sistema aplicado durante el maoísmo. Analizaré cómo la digitalización, la difuminación del ámbito privado de los ciudadanos y la ampliación de la esfera pública, junto con la creación de un mercado digital propio desconectado del resto del global, le está permitiendo al gobierno chino ampliar el control social superando los límites de la esfera privada de los individuos, que ni el propio Mao Zedong habría podido llegar a imaginar. Quiero demostrar la hipótesis que, gracias a las TIC, el PCCh de Xi ha conseguido ocupar la ansiada centralidad en la vida de los ciudadanos, y que su gobierno puede aplicar un control social permanente y en tiempo real sobre todos los individuos, teniendo en cuenta su idea de “una vez no confiable, siempre restringido”.

El documento se dividirá en tres apartados. El primero, titulado “Vigilancia y control social en la sociedad digital”, analizará cómo las TIC se han convertido en el arma que necesitaban los estados autoritarios para reforzarse y mantener su legitimidad. Para entender esta transformación de internet de medio libertador a carcelero, hay que analizar cómo la ubicuidad de la informática y las TIC han transformado los límites de ámbito privado de los ciudadanos, hasta hacer visibles a los ojos de los gobernantes todas nuestras acciones. Un cambio de la esfera pública que ha sustentado la transformación de los autoritarismos hacia el autoritarismo en red, o autoritarismo digital, que ha sabido aprovechar la capacidad de control que ofrecen las TIC. El segundo apartado, “La vigilancia y el control social en la República Popular China”, analizará sobre qué base se

sustenta, y cómo se ejerce la vigilancia y el control social en la China actual. Partiré de concepto clave de cibersoberanía, para explicar cómo se aplica la censura, cómo se implementa la vigilancia en la red, y cómo desaparece la privacidad de los ciudadanos con una legislación hecha según las necesidades arbitrarias del PCCh para mantener el poder. En el tercer y último apartado, con el título “El control social de Xi Jinping frente al control social de Mao Zedong”, compararé cómo se aplicaba el control social en la época maoísta, centrado en la conquista de parte de la esfera privada por parte del dominio público, a través de la comuna o de la fábrica, con la omnisciencia de Xi Jinping, que trasciende las actividades públicas para llegar a todas las actividades del ciudadano. En este punto, es interesante ver cómo evoluciona el crédito social entre las épocas de Mao Zedong o Xi Jinping, qué diferencias y qué similitudes registramos, y cómo Xi ha conseguido perfeccionar el sistema de control maoísta para hacerlo más férreo y exhaustivo.

Para analizar los dos períodos históricos diferentes del mismo país, China, pero bajo dos líderes diferentes, Mao Zedong y Xi Jinping, utilizaré el método comparativo. Entendiendo que la delimitación física, China, el sistema político, autoritario semipresidencialista, y los principales actores del sistema político, PCCh y las élites gobernantes, son prácticamente las mismas en ambos períodos, señalaré a las TIC y a la digitalización con la variable dependiente que permiten aumentar el control social ejercido por las élites gobernantes en la RPCh. En cuanto a la base documental, el trabajo se construirá sobre fuentes primarias (leyes, discursos u informaciones oficiales o estadísticas) y secundarias (tanto artículos académicos como periodísticos) para definir la época maoísta, la actual de Xi Jinping y establecer una comparación entre ambas.

2. Vigilancia y control social en la sociedad digital

Cuando nació internet, a mediados del siglo pasado, las grandes posibilidades de control social masivo que ofrecía quedaron en un segundo plano. Incluso cuando, a finales del siglo XX, el uso de la red y de las TIC traspasó las fronteras técnicas y académicas para convertirse un nuevo medio de comunicación a gran escala, muchos expertos coincidieron en señalar, únicamente, sus bondades como medio democratizador. Al realizar sus proyecciones de futuro, focalizaban sus análisis en la ruptura que la irrupción de las TIC suponía en el viejo paradigma de la comunicación social. Para ellos, lo más importante

era que nueva comunicación digital permitía la interacción individual e instantánea entre individuos sin que el poder o el estado, al menos en principio, pudieran controlarla.

Pero, esta expansión de las TIC como nuevo medio de comunicación de masas coincidió con la crisis de representatividad de las democracias occidentales. La globalización, la crisis del Estado del Bienestar o los diferentes períodos de crisis económicas han erosionado la confianza de los ciudadanos en los actores del sistema, sobre todo en los partidos políticos, como el canal para vehicular sus inquietudes, peticiones y exigencias (Eberhardt 2014). Quizás por esta crisis de representatividad, pero también, por las grandes posibilidades de comunicación, expresión y autoorganización que permitían las TIC, muchos analistas empezaron a ver en la comunicación digital como la cura de las heridas democracias, al permitir aumentar la participación de los ciudadanos en las decisiones políticas, e incluso, creando una ciberdemocracia o una nueva esfera pública global de debate y participación política (Lévy 2002, 166).

Internet: de medio libertador a carcelero

Pero, la visión democratizadora de las TIC va más allá dotar de nuevas herramientas de consulta, control y comunicación entre los ciudadanos y sus gobernantes de las viejas democracias occidentales, o en el advenimiento de una nueva ágora global de decisión y debate. Además de ser el canal necesario para ampliar el espacio de participación e intercambio de información entre ciudadanos o entre ciudadanos y el estado, la propia naturaleza descentralizada, inmediata, global e individual de la comunicación digital hizo que llegara a considerarse como el arma definitiva para derrocar a los viejos autoritarismos.

En realidad, esta corriente ciberooptimista ve en la digitalización una verdadera revolución de la comunicación de masas, que rompe el viejo paradigma comunicativo unidireccional mediatizado y controlado por el estado, que reconoce el nuevo sistema de comunicación digital como un instrumento libertador (Castells 2009, 269), y que permite y alienta el nacimiento y desarrollo de estructuras ciudadanas críticas con el sistema político (Lagos 2013, 398). Porque, de hecho, es esta posibilidad de comunicación entre ciudadanos teniendo en cuenta la afinidad o los intereses, y no el ámbito geográfico o estrato social, el que confiere a las TIC esta capacidad transformadora ya que permiten y facilitan la autoorganización de los ciudadanos para crear estructuras críticas con el poder.

Es verdad que las TIC ofrecen grandes posibilidades para aumentar la calidad democrática de los sistemas políticos. Por una parte, permiten la interconexión constante, permanente e instantánea de los ciudadanos de un barrio, ciudad, comunidad, estado o, incluso, la creación de una gran comunidad global para debatir, compartir y analizar determinadas situaciones para poder tomar decisiones conjuntas y coordinadas. Por otra, posibilita que los ciudadanos, a través de la rendición de cuentas y de la publicación periódica de los datos de la administración pública, puedan controlar la calidad de la acción de gobierno. Pero, esta visión idílica de las TIC como origen y fuente de una democracia universal, donde la comunicación no estaría mediatizada por el poder y sería omnidireccional quedó, muy pronto, eclipsada por los cyberpesimistas.

El avance imparable de la digitalización de la sociedad global y el aumento del peso de la vida virtual en el día a día de los ciudadanos empezó a mostrar la otra cara de las TIC. Si en el mundo analógico, el ámbito privado de nuestra vida no deja rastro y se mantiene invisible, la digitalización visibiliza los detalles de todos nuestros actos que, hasta el momento, permanecían ocultos. La gran cantidad de datos que, de cada ciudadano, es posible obtener a través del rastro que dejamos en la red a través de búsquedas, transacciones comerciales o bancarias, gustos musicales, comentarios en redes sociales o geolocalización, ofrecen grandes posibilidades de control social. De hecho, este volumen de información, *big data*, que cada ciudadano deja, en la mayoría de los casos de forma inconsciente, permite crear un sistema vigilancia constante y perpetuo construido a costa de la privacidad y de los derechos civiles de los ciudadanos (Van de Donk 1995). Por tanto, a las grandes posibilidades de democratización que ofrecen las TIC se contraponen a las, también, grandes posibilidades de control social al expulsar al ámbito público, y por tanto a la vista de todo el mundo, la vida privada de los ciudadanos.

Todas las sociedades tienen sistemas de control social para mantener el orden y asegurar su continuidad. Por control social entendemos la serie de mecanismos, impuestos o consensuados, formales o informales, que desalientan o previenen la desobediencia, castigando al miembro que norma con las normas establecidas. Para ser efectivo, el control social debe entrar en todos los ámbitos del individuo, desde el más obvio, el público, hasta el ámbito privado o íntimo (Noboa 2016, 185). Un fallo en el sistema de control social puede llevar a la desaparición del grupo (Rule 2007, 19-20; Chen 2004 523) y del propio sistema de organización social y política.

Para desplegar un sistema de control social efectivo, la vigilancia y la gestión de la información son elementos esenciales. Cuanta más información obtenga la estructura

de poder del funcionamiento de la sociedad que lidera, mejor podrá controlar el comportamiento de los individuos. Por eso, la vigilancia, entendida como la actividad rutinaria y sistemática utilizada para dirigir a los individuos y a la población (Ball, et al. 2006 :5) , es un factor imprescindible. Además, para que sea lo más exitosa posible y permita un control permanente de los ciudadanos, los sistemas de vigilancia deben ser constantes, omnipresentes y silenciosos (Soto 2016, 26). Su eficacia, como en el panopticismo de Jeremy Bentham (1748-1832), se articula en la capacidad de ver y vigilar sin ser visto. Bentham diseñó una prisión circular donde, una estructura levantada estratégicamente en el centro permitía la vigilancia de todas las celdas al mismo tiempo, pero sin que los reos supieran cuando estaban siendo observados. En realidad, es esta visibilidad permanente y la constante exposición del individuo el que garantiza el funcionamiento automático del poder (Foucault, 2009:233). Pero Michel Foucault (1926-1984), en esta sociedad vigilada y vigilante, de examen continuo y constante sobre los ciudadanos en busca del individuo potencialmente peligroso para la misma sociedad y para el orden social establecido (Soto 2016, 29) sitúa la información como un elemento esencial para clasificar, calificar y castigar a los ciudadanos (Foucault 2009, 215) y, por tanto, para poder mantener el orden social existente. El estado necesita conocer el mayor número de datos sobre los individuos para poder clasificarlos en función de la confiabilidad social, es decir, el grado de peligrosidad para el mantenimiento y supervivencia del sistema. Por eso, asegura Foucault, que hemos dejado atrás la sociedad disciplinaria y hemos entrado en la sociedad del control. Las viejas estructuras de control social formales y reconocibles de la sociedad disciplinaria en las que el individuo está inmerso e ingresado están en crisis. Lo está la familia, el hospital, la escuela, la fábrica y todos sistemas de control, dominio y sometimiento del individuo a la voluntad y las necesidades del poder y la colectividad.

Pero, aunque el pensador francés murió hace 34 años, su pensamiento permitía anticipar la sociedad digital en la que estamos inmersos. Con su visión de la transición a esa sociedad del control, anunciaba la disolución del poder como elemento claramente visible, monolítico e identificable para reconstruirlo con un nuevo sistema multimodal, capilar y más sutil, más efectivo que el modelo anterior, y que condiciona la vida de los individuos. Para Foucault, como ya lo era la sociedad de consumo en sí misma, la digitalización de la sociedad sería un claro ejemplo de la sociedad del control, con un poder diluido en la propia estructura de la sociedad e incorporada en la vida diaria de los

ciudadanos, donde el individuo es constantemente fiscalizado y monitorizado sin que sea consciente de ello.

Por tanto, la sociedad disciplinaria, basada en la vieja concepción del mundo físico, deja paso a la sociedad del control, donde las cifras y la información, lo intangible e invisible, se convierten en un valor esencial para el control social (Soto 2016, 30) con las inmensas posibilidades que ofrecen la informática y la telemática. La informática ubicua se ha convertido en el nuevo vigilante que todo lo ve sin estar, físicamente, en ningún lugar determinado, y las cifras y los datos, las nuevas herramientas en manos del poder para elaborar perfiles determinados de los ciudadanos. La digitalización y otros sistemas de computación y seguimiento facilitan la implantación de sistemas de vigilancia y control social a gran escala, la llegando a ser la misma vigilancia la principal característica de las sociedades actuales (Flaherty 1989, 1) y en la que la ingeniería del control social es imprescindible para el funcionamiento de la sociedad (Marx 2015, 117).

En realidad, la informática y los datos han convertido a las sociedades actuales en el panóptico perfecto, más allá de lo imaginable, donde el ciudadano no es consciente de ser observado, pero lo está más que nunca. La vigilancia estatal sobre los ciudadanos es permanente, constante y se nutre de la gran cantidad de información que generamos en nuestra vida digital y, todos, relacionados con el uso de sistemas de información y comunicación como teléfonos móviles, tarjetas de crédito, correo electrónico, navegadores, sistemas de geolocalización, historiales médicos digitalizados, tarjetas inteligentes para acceder aparcamientos, edificios o peajes y un largo etcétera. Pero, al mismo tiempo que el individuo se hace visible hasta un punto insospechado, las implantación y evolución de las TIC aumentan de forma desmesurada las tendencias de control social, tanto en sus posibilidades como en su eficacia. De hecho, permiten lo que siempre han ansiado los gobiernos, sistemas de recogida masiva de datos de políticos, ciudadanos, grupos sociales y organizaciones para ejercer un control sobre los individuos y su territorio con el fin de evitar movimientos críticos.

La esfera pública y el control social en la ‘sociedad conectada’

La digitalización ha cambiado la vida de los ciudadanos y su forma de socialización. Las TIC han abierto una ventana al mundo allá donde haya un punto de conexión. Del acceso

unimodal fijo del ordenador de sobremesa se ha pasado, en pocos años, a uno itinerante a través de múltiples dispositivos: ordenador portátil, tableta o teléfono móvil. La rápida extensión de la conexión individual permanente a internet ha universalizado su uso, convirtiéndose en el segundo escenario de nuestra vida. Cada vez son más los aspectos de nuestra cotidianidad analógica que tienen una versión digital: espacios para trámites administrativos, bancarios, educación reglada y/o universitaria, comercio y ocio. El nacimiento de las redes sociales ha digitalizado las relaciones sociales. Ya no podemos separar lo virtual y lo real. Vivimos en “una virtualidad real donde la comunicación virtual es una parte esencial de nuestra realidad cotidiana” (Castells 2014, 10).

La vida analógica y digital se complementan, son interdependientes y se influyen mutuamente. Cada vez, nuestro reflejo cibernético es más detallado. Al rastro que todos dejamos en nuestra vida en la red (historiales de búsqueda, perfiles de compra, lugar que hemos visitado, intereses musicales...) hay que sumar la digitalización de los espacios reales. El internet de las cosas, las casas domóticas, la conectividad de los vehículos o la geolocalización, junto con el uso del teléfono móvil y de las redes sociales permiten realizar un perfil del ciudadano altamente fiable. La computación ubicua, donde la informática está integrada en el entorno del individuo de forma permanente, hace visible lo que hasta ahora era de muy difícil acceso: la vida privada de los ciudadanos.

El control de la información de los usuarios es uno de los elementos claves del proceso de digitalización (Moore 1998, 365). Todos nuestros aspectos de la vida cotidiana están conectados en red. La intimidad del individuo, hasta ahora oculta a los ojos de los extraños, salta a la esfera pública. Cada vez es más difícil distinguir lo público y lo privado, situando la noción de privacidad del individuo bajo presión o en peligro de desaparecer. Las TIC en general, y las redes sociales en particular, han eliminado la separación que existía entre ámbito privado, público e íntimo, donde los ciudadanos han perdido el control sobre su propia información personal, exhibiendo sus datos en público para su uso compartido y de libre disposición (Bauman y Lyon, 2013). La totalidad del individuo está expuesto, nada queda oculto al vigilante panóptico de Bentham, que controla oculto desde la distancia, pero con efectos instantáneos. Se ha transformado el concepto de vigilancia y control. El observado está totalmente expuesto. Las TIC ofrecen toda la información necesaria para que la vigilancia y el control sean omnipresentes y ubicuos, pero al mismo tiempo, fluidos e invisibles al ojo del vigilado (Bauman y Lyon, 2013). Además, los constantes avances tecnológicos en electrónica, informática o inteligencia artificial prometen nuevas posibilidades de control.

En este escenario, serán los grandes avances en inteligencia artificial los que podrían derribar los últimos muros que separaban la vida privada de los ciudadanos con la esfera pública. Las nuevas formas de analizar nuestro rastro digital, *big data*, permite extraer información personal sobre cada individuo sin que él mismo la proporcione de forma explícita. Los nuevos sistemas de análisis de datos buscan patrones en los usos de redes sociales, consumo de entretenimiento o información, etiquetas en redes sociales o compras en el entorno digital. Con esta materia prima, la inteligencia artificial puede elaborar un patrón muy detallado del individuo con información sensible y muy interesante para gobiernos y empresas, incluyendo la afinidad política o la tendencia sexual. En realidad, los nuevos sistemas de tratamiento de datos, junto con la generalización de los programas de reconocimiento facial, permiten descubrir información de la vida privada de los ciudadanos sin que lo sepan y, por tanto, permiten establecer un sistema de vigilancia y control social altamente efectivo. Nunca hasta el momento, el sistema de poder había podido establecer una forma de vigilancia tan amplio, extenso e instantáneo como el que permite la digitalización de la sociedad, alertando sobre posibles individuos conflictivos incluso antes de que hayan incumplido las normas o hayan puesto en peligro el orden social establecido. La prevención del delito, a través del tratamiento de datos de comportamiento digital, traspasa una de las últimas barreras que protegía la intimidad y la privacidad de los individuos, y deja en manos del poder, independientemente de la forma bajo la que esté representado, libertad total de actuación para proteger el sistema social establecido.

El autoritarismo en red

Pese a la esperanza depositada en las TIC como herramienta aniquiladora de los autoritarismos (Castells 2009, 262; Lévy 2002, 33), en realidad, los ha fortalecido (Morozov 2010, 56). Las proféticas teorías se han enfrentado a unos sistemas autoritarios resilientes, que se han adaptado a los nuevos escenarios de comunicación global caracterizada por un gran volumen de información constante, instantánea, de múltiples emisores y que permite creación de grupos de interés intergeneracionales, interétnicos e interclasistas basados en el contacto entre usuarios anónimos (Castells 2013, 10-1). Los autoritarismos modernos están utilizando buena parte del nuevo paradigma comunicativo digital para reforzarse y legitimarse. Han aprendido a funcionar en entornos marcados por

la abundancia de información, lo que les ha permitido mejorar los tres pilares del control autoritario: la censura, la propaganda y la vigilancia (Morozov 2010, 82).

El fenómeno de las *fake news* y su influencia en el referéndum del Brexit o en elecciones que han llevado a Trump a la presidencia de Estados Unidos son un buen ejemplo de cómo la digitalización de la comunicación ha beneficiado a la propaganda. Sin tener en cuenta el objetivo de la campaña propagandística, es decir si tiene un fin económico o político, lo que parece evidente es que la entrada de más actores en el paradigma comunicativo tradicional dificulta enormemente la comprobación de la veracidad de los contenidos. Si a eso, le añadimos la sobreabundancia de información que recibe cada ciudadano, y la rapidez en su transmisión vemos que el entorno comunicativo digital es el perfecto para la propaganda, que será más efectiva que su versión analógica (Morozov 2010, 82).

La transformación digital no solo ha permitido aumentar el efecto de las campañas de propaganda, también ha permitido la implementación de sistemas de control y censura altamente efectivos, que se sustentan en el desarrollo de una infraestructura de alta tecnología, pero también, fomentando un mercado digital propio, con una regulación muy restrictiva, que sirve a los intereses estatales previamente definidos (Kalatahil y Boas 2003, 3). Además, la propia redefinición de la esfera pública con el consecuente aumento de la información que existe sobre cada ciudadano incrementa exponencialmente las posibilidades de control sobre los ciudadanos por parte de los gobiernos, sean democráticos o autoritarios, haciéndolo más exhaustivo y férreo.

En el caso de los autoritarismos, la digitalización ha matizado sus formas de control, que ahora gracias a las TIC pueden ser más refinadas y quirúrgicas. Como definió la oenegé *Freedom House* en 2017, los nuevos autoritarismos ofrecen una falsa sensación de libertad y pluralismo, porque la represión política, aunque legalizada, se aplica de forma limitada, selectiva y oculta. Este nuevo autoritarismo cibernético es el que MacKinnon denomina como “autoritarismo en red”, que sigue sin respetar los derechos individuales y colectivos y usa la violencia y medidas coercitivas contra aquellos que considera una amenaza, pero al mismo tiempo, permite conversaciones críticas en redes sociales y en internet que pueden tener un cierto impacto en las políticas del gobierno: el ciudadano tiene la sensación de poder hablar con libertad, y además, ser escuchado (MacKinnon 2010b, 3-4). Así pues, el “autoritarismo en red” o autoritarismo matizado aproxima sus formas a las de una democracia permitiendo una cierta semilibertad con una gran circulación de información y ocultando al máximo la aplicación de la violencia. Pero,

es esa represión, además del control total sobre la economía, medios de comunicación y asuntos políticos, lo que sigue alejando a este autoritarismo moderno de un sistema democrático.

Por tanto, lejos de amenazar su continuidad, la digitalización ha fortalecido y transformado a los viejos autoritarismos. Por una parte, han sabido redireccionar la nueva comunicación digital con infinitos emisores y receptores para aumentar la propaganda y redireccionar o acallar las posibles voces críticas que pudieran surgir. Por otra, han sabido resituar el foco del control, ya no en el individuo, que se autocensura para evitar consecuencias negativas, sino en los actores del propio mercado. Son las empresas de un escenario cuidadosamente diseñado y controlado las que ejercen el control social de contenidos e información. Además, el desarrollo tecnológico del *big data* y la inteligencia artificial, ponen a su alcance infinitas posibilidades de control. Los avances en los sistemas de tratamiento y computación, que son cada vez más rápidos, asequibles, autónomos e inmediatos, permiten el despliegue de formas de vigilancia, control, detección, bloqueo y neutralización de amenazas. Por primera vez, y gracias a la digitalización, el poder puede establecer un sistema de control constante, invisible y permanente e interconectado, con respuestas inmediatas y contundentes, tomando decisiones autónomas sin intervención del ser humano, e incluso, con predicción de futuras amenazas. Así pues, la arbitrariedad y la inseguridad jurídica que sustenta a los autoritarismos ha encontrado su traducción en el mundo digital.

3. La vigilancia y el control social en la República Popular China

Para el gobierno chino, la masacre de la plaza de Tiananmen, en 1989, supuso un hito en la gestión de la comunicación en una situación de crisis. Con un país ya abierto al exterior, el PCCh aplicó un bloqueo total sobre la información que los medios nacionales o internacionales estaban produciendo sobre los hechos. Como informaba la agencia *Associated Press*, el 19 de mayo de 1989 en la noticia titulada “China Stops Live Coverage by American Television”, el gobierno, bajo los preceptos de soberanía y seguridad nacional, cortó la conexión vía satélite para que los medios extranjeros, sobre todo la CNN y la CBS, no pudieran informar de lo que estaba sucediendo en la capital china.

En China, el control de la información siempre ha sido uno de los elementos claves del control social ejercido sobre los ciudadanos. Si la matanza de Tiananmen obligó a los líderes chinos a buscar en el viejo maoísmo cómo gestionar la crisis, aumentando el control social y de la comunicación para mantener la legitimidad puesta en duda, la entrada de China en el mercado global, su transformación en la cadena de montaje del mundo, y la digitalización han vuelto a enfrentar al PCCh al mismo reto: cómo mantener el control social en una economía basada en la desaparición de las fronteras y caracterizada por un flujo incesante, instantáneo de información, casi imposible de controlar. Por eso, y aunque sus antecesores consiguieron mantener el control sobre la sociedad y la información a pesar de internet, es con la llegada al poder en 2012 del actual presidente de la República Popular, Xi Jinping, cuando la postura china sobre las TIC se clarifica. En la Segunda Conferencia Mundial de Internet celebrada el 16 de diciembre de 2015 dejó claro que no concebía la red como un sistema global sino como la suma de las redes locales. Para Xi Jinping la red es un asunto de seguridad nacional, lo que le permite al gobierno controlar el flujo de información dentro sus fronteras, entendiendo que de la seguridad en internet depende la seguridad nacional. El presidente chino trasladaba así el concepto de soberanía nacional al ciberespacio, y aparecía un concepto que ha condicionado y condicionará el desarrollo del uso de las tecnologías de la información y la comunicación (TIC) en China: la cibersoberanía.

La centralidad de la cibersoberanía

La globalización económica, la transformación digital y el crecimiento exponencial del ciberespacio como lugar de relación entre individuos, actores económicos y políticos ha forzado la aparición y la necesaria definición de algunos conceptos. Sin duda, el más urgente es el de cibersoberanía. Después de tres años de trabajo, 20 expertos en derecho internacional reunidos por el “Centro Cooperativo de Excelencia de la Ciberdefensa de la OTAN” definen cibersoberanía como el derecho del estado para controlar las actividades cibernéticas y las infraestructuras de información y comunicación digital situadas dentro de su territorio nacional, e incluyendo el mundo virtual como lugar donde se aplica la soberanía de un estado. Esto significa que las infraestructuras de las TIC situadas dentro el ámbito de aplicación de la soberanía están sujetas al control legal y regulatorio del estado y que la propia aplicación de la soberanía las protege de intromisiones extranjeras.

El estado tiene el derecho exclusivo a ejercer su poder sobre todos los elementos, también del mundo digital, que operan dentro del territorio nacional o del ámbito de aplicabilidad de la soberanía nacional, quedando tanto los propietarios como los usuarios de ese mercado digital bajo la jurisdicción judicial y administrativa del país (Schmitt 2013, 16). Por tanto, la cibersoberanía permite el control estatal total sobre las redes TIC, dando total autonomía al estado para definir un mercado digital, autónomo e independiente a través de una legislación nacional y un marco regulatorio propio.

El control estatal total sobre la infraestructura digital que permite el concepto de cibersoberanía también incluye a la información y los contenidos que circulan y se producen en la red. Se articula en dos objetivos claves: en la prohibición de cualquier influencia externa no deseada que pueda dañar al régimen y en la transformación de la gobernanza en la red donde son los estados los únicos interlocutores y los únicos actores autorizados para tomar decisiones y ejercer el poder en el ciberespacio (Schia y Gjesvik 2017, 1). Para China, el concepto de cibersoberanía, es decir, el control del ciberespacio, es imprescindible para mantener sus valores sociales fundamentales. En realidad, el gobierno chino ve en la red un punto de encuentro libre entre ciudadanos que necesita ser controlado y regulado para evitar el caos y el desorden al que se dirige de forma natural. Esa es la función esencial que debe tener el estado, a la que no puede renunciar, y que es esencial para la construcción de gobernanza de internet global basada en la cooperación entre estados, pero desde la propia independencia de cada uno (Hao 2017, 110-2).

En realidad, esta definición de cibersoberanía donde el estado, en este caso el chino, tiene un poder absoluto sobre infraestructuras y contenidos que se generan por las TIC, permite sentar las bases para definir un mercado digital basado en la independencia y la no ingerencia extranjera. Esta visión de cibersoberanía ha permitido definir un mercado particular y desconectado del resto del mundo. Como en el caso de Tiananmen, el gobierno chino ha creado un mercado digital sin influencia extranjera, limitado a las fronteras nacionales, construido para servir a sus propios intereses y donde todos los actores son fácilmente controlables.

Si el concepto de cibersoberanía construye el corpus conceptual del PCCh y las élites gobernantes chinas frente a la digitalización, lo que permite ponerlo en práctica es la construcción de un marco normativo muy amplio y vago, que forma una maraña legislativa que lo hacen prácticamente incomprensible y que facilita la arbitrariedad de las decisiones gubernamentales (Endeshaw 2004). Además, las leyes chinas son más una declaración de intenciones que normas para ser aplicadas, es decir, más redactadas de

cara a la galería para ser políticamente correctas o contentar a sectores determinados, estén dentro o fuera del país, y que para su aplicación real (Han 2016, 212).

Pero estas características del mercado digital chino, es decir, ni el control absoluto arrogado por el gobierno chino sobre las TIC, ni la arbitrariedad de un sistema normativo vago y difuso, cuya aplicación depende más de la interpretación de la ley que textualidad, no pueden sorprender. En realidad, ambas son características definitorias de los regímenes autoritarios, incluidos los modernos que, aunque clonan las formas de los sistemas democráticos para dar apariencia de seguridad jurídica y libertad, mantienen un control férreo sobre todos los ámbitos de la sociedad.

Hasta el inicio de las reformas económicas, China no empezó a construir su sistema legal de corte occidental, con normas supuestamente claras, definidas y publicitadas a priori. Una de las primeras leyes que vieron la luz fue el Código Penal (1979), que establece penas contra aquellos que ataquen a la revolución, divulgando secretos de estado y publicando materiales obscenos. Este corpus argumental, heredado de la época de Mao Zedong, se repetirá en buena parte de la legislación china hasta la actualidad por su gran eficacia para luchar contra sectores críticos y mantener el control sobre la población.

En la década de 1980 se establece un sistema definido de control sobre los medios de comunicación y la información. En 1982, el Ministerio de Radio, Cine y Televisión aprobó las normas para la gestión de productos audiovisuales, exigiendo una licencia para producir y distribuir grabaciones audiovisuales, y donde se obligaba a la revisión gubernamental de los contenidos importados, pero sin hacer públicos los criterios exactos de las revisiones obligatorias. Lo que sí se conoce es que se obligaba a confiscar todos aquellos productos anti-comunistas, anti-socialistas, obscenos, propagandísticos y de contenido malsano (Han 2016, 215). Se establece una legislación, autónoma e independiente de la influencia extranjera, basada en la soberanía nacional, construida para evitar la entrada de material que pudiera dañar la imagen del partido, las creencias y la ideología de la sociedad china, y que pusiera en peligro la legitimidad y la credibilidad del sistema. En realidad, esa primera legislación sienta las bases de la normativa posterior que se aplicará al sector y con un objetivo claro: controlar la información para controlar a la sociedad y mantener la legitimidad del régimen.

La primera norma china que incluye internet, de forma específica, como marco de aplicación se promulgó en 1995, un año después de la conexión de China a la red internacional con un objetivo claro, “controlar la red y las conexiones a la red

internacional” (Tsui 2001, 26). En 1997, el control gubernamental sobre la red se incluyó en el Código Penal, y 5 años después, la maraña legal china para controlar los contenidos del ciberespacio, según Amnistía Internacional, sumaba más de 60 leyes o normas. Solo en el año 2000, se promulgaron 6 normas que buscaban controlar el contenido digital. Uno de esos textos normativos, tramitado por el gobierno en el año 2000, es las “Medidas de administración de servicios de información por internet”, una lista de contenidos prohibidos, que amplía esas primeras consideraciones reflejadas en el Código Penal de 1979. Según esta norma, quedan prohibidos todos aquellos contenidos que se opongan a la constitución, que comprometan la seguridad nacional, que amenacen al gobierno, perturben la unidad nacional, perjudiquen el honor y los intereses nacionales, difundan rumores que perturben el orden social y alteren la estabilidad social y calumnien o insulten a personas, instiguen crímenes. Estas medidas construyen el marco legal necesario para que el estado chino contemporáneo pueda aplicar, con la ley en la mano, un control absoluto, discrecional y arbitrario sobre los contenidos de internet. Todos los supuestos para prohibir contenidos digitales y, en consecuencia, perseguir penalmente a quién los publique o los propague, tienen una clara orientación política que busca mantener la legitimidad, el poder y el control social que el PCCh ejerce en el país. Es, por tanto, una primera base legal que le permite al régimen establecer un control arbitrario en su propio beneficio, ya que cualquier acción que moleste a las élites o que pueda ser considerada como una amenaza puede ser incluida en los preceptos prohibidos. En 2010, el Consejo de Estado publicó el “Libro Blanco de internet” donde se deja clara la postura del gobierno con respecto a la red: tiene un papel activo de agente controlador y regulador sobre la infraestructura y los contenidos velando, dice en el punto 5 sobre seguridad en internet, que ninguna organización o individuo podrá participar en actividades que pongan en peligro la seguridad del Estado, el interés público o los derechos legítimos de otras personas.

La expansión de internet en China ha ido acompañada de un fortalecimiento del control estatal sobre la infraestructura y los contenidos. Como ha venido haciendo desde su llegada al poder en 1949, para extender y afianzar su control de las TIC, el PCCh ha invocado a la seguridad nacional y la lucha contra posibles ataques extranjeros y/o de enemigos del partido o del país, para actuar de forma arbitraria contra los contrarios a sus intereses. Bajo el paraguas del concepto de cibersoberanía y parapetado tras la amplia idea de seguridad nacional, el presidente Xi ha ido diseñando una arquitectura legal que le permite un control absoluto sobre la red y los ciudadanos, llegando a ser una versión

perfeccionada del que ejerció durante décadas Mao Zedong. Para conseguirlo, desde su llegada al poder en 2012 se han aprobado las leyes de Anti-espionaje (2014), Seguridad Nacional (2015), Anti-terrorista (2016) y la que regula la presencia de ONG (2016), además de modificarse el Código Penal (2015).

A principios de junio de 2017, y con el único objetivo reconocido por el PCCh de garantizar la seguridad nacional y reducir la vulnerabilidad del sistema informático chino a amenazas externas, entró en vigor la ley de ciberseguridad. Este texto obliga a todos los “operadores de infraestructuras de información clave” a almacenar en territorio chino los datos que generen y a pedir permiso al gobierno si quieren trasladar esa información fuera del país. Además, todas las empresas autorizadas a operar en sectores clave están obligadas a someterse a revisiones de seguridad por parte del gobierno, forzándolas a revelar los códigos fuente de sus programas y otros datos confidenciales, lo que las expone al espionaje industrial o al robo de la propiedad intelectual. Pero, lo que más llama la atención es, de nuevo, la vaguedad en la definición de los sectores clave, que son, según la ley “cualquier infraestructura de información clave que pueda causar graves daños a la seguridad nacional, la economía o el interés público si se destruyeran, quedaran inutilizadas o se filtraran. Con esta redacción, prácticamente todos los sectores pueden ser considerados como un sector clave y objetivo a controlar por el gobierno. En realidad, este texto demuestra cómo Xi quiere reforzar el concepto de un mercado tecnológico propio y desconectado del mundo, dificultando la entrada de competencia extranjera.

Como vemos, la ley de ciberseguridad mantiene y aumenta la discrecionalidad del gobierno sobre las infraestructuras y los contenidos de las TIC. La norma prohíbe la publicación de contenidos que perjudiquen el honor nacional, que se sospeche que puedan intentar deponer el sistema socialista o la alteración del orden social y económico en vigor. La norma, como siempre, vuelve a ser tan amplia y poco definida que puede ser aplicada a cualquier actor de la red por cualquier motivo que moleste al régimen. Y bajo estas premisas, son los propios operadores, en concesión administrativa o propiedad de las élites gobernantes, las que deben censurar la información que se considere inapropiada, identificar a los usuarios con su nombre real y proporcionar toda la información a las investigaciones estatales. Así pues, la ley de ciberseguridad, utilizando el concepto de cibersoberanía y para defender la seguridad nacional, da un poder total y arbitrario al gobierno para controlar el mercado digital, excluyendo a la competencia extranjera, teniendo total acceso a la información de las empresas y de los ciudadanos, y dejando en manos de las empresas la censura de los contenidos inapropiados.

Otras leyes que, por su amplia interpretación y vaguedad son el arma perfecta del gobierno para controlar y censurar son la ley antiterrorista y la de inteligencia nacional. La antiterrorista, aprobada a finales de 2015, obliga a las empresas tecnológicas a entregar información que se considere sensible al gobierno chino, también de los usuarios, además de estar obligados instalar puertas traseras en sus productos para evitar los sistemas de seguridad y permitir el libre acceso gubernamental. Por sí solos, estos dos puntos, ya permiten un acceso total y discrecional al gobierno a toda la información almacenada de sus productos y de los ciudadanos por parte de las empresas del mercado digital. Pero, además, hay que añadir que la ley impide publicar información sobre terrorismo, políticas gubernamentales o ataques terroristas en medios de comunicación sin una autorización expresa, y permite al gobierno restringir toda la información sobre la materia que se pueda publicar en redes sociales. Es, en realidad, una posibilidad más de control y censura del gobierno de Xi Jinping porque la ley define de una forma muy amplia el concepto de terrorismo. Para el gobierno chino terrorismo “cualquier proposición o actividad que, por medio de violencia, sabotaje o amenaza, genera pánico social, socava la seguridad pública y amenaza a los organismos gubernamentales con intereses políticos e ideológicos”. En cuanto a la ley de inteligencia nacional, que todavía es un borrador, Amnistía Internacional alerta, en su análisis del texto provisional, que esta futura ley legaliza la censura, la vigilancia y la detención arbitraria en nombre la seguridad nacional más allá de la proporcionalidad y de lo permitido por las leyes internacionales (Amnistía Internacional 2017, 3).

Censura, propaganda y vigilancia en la intranet china

En total, más de 60 leyes y una docena de organismos se encargan de monitorizar la red para controlar el cumplimiento de las diferentes normativas. El principal organismo de control es el Departamento Central de Propaganda del PCCh, aunque el sistema gubernamental para regular y controlar los medios está en constante evolución. Desde 2014, el máximo órgano de control sobre la red es la Comisión Central de Asuntos del Ciberespacio (CCAC), presidida por Xi Jinping. Depende del Comité Central del PCCh, su función es coordinar las políticas de los diferentes ministerios sobre las TIC y sus contenidos, y tiene autoridad plena para decidir sobre la regulación de contenidos y

ciberseguridad. Entre otros asuntos, ha sido el órgano encargado de elaborar la polémica Ley de Ciberseguridad. Ante esta comisión rinde cuentas, y ejecuta sus mandatos, el gran órgano de control efectivo de la red en China, la Administración del Ciberespacio de China (ACC). Sus funciones son monitorizar, controlar, supervisar, censurar los contenidos digitales. Por ejemplo, es la encargada de controlar los nombres de usuarios de la red china, si los comentarios realizados cumplen con lo estipulado en la legislación y, también los contenidos digitales. En realidad, la ACC es la encargada de aplicar las directrices políticas que sobre contenidos y la red marca el comité del PCCh. Además de la creación de éstos y otros organismos específicos para controlar la red, se mantiene la vigilancia habitual sobre los medios del todopoderoso Departamento de Propaganda del PCCh, que coordina las actuaciones de la Administración Estatal de Prensa, Publicaciones, Radio, Cine y Televisión, creada en 2013 para garantizar que se promueva la doctrina del partido. También en 2014, el ministerio de Seguridad Pública publicó los reglamentos en el que sitúa a la red como un ámbito más de aplicación del procedimiento penal chino.

En 2013, el Tercer Plenario del XVIII Congreso del Partido Comunista Chino marcó la hoja de ruta. Un año después del encumbramiento de Xi Jinping como líder del PCCh, el denominado “Documento 9” señalaba el mantenimiento de la disciplina jerárquica dentro del partido y el mantenimiento y fortalecimiento del control estatal sobre los medios para “orientar correctamente a la opinión pública” como sus objetivos más inmediatos ante el ataque ideológico de Occidente. También llamaba a mantener y promover el fortalecimiento del ideario socialista en la sociedad china, reforzando todos los tipos de sistemas y propaganda, señalando específicamente las oportunidades que ofrece el ámbito digital, y situaba a la red como el campo de batalla para orientar a la opinión pública, purificando, limpiando y manteniendo el ambiente sano en el ciberespacio. Tras ese llamamiento, el PCCh ha reforzado y ampliado su estructura de propaganda en la red, control y vigilancia sobre los contenidos, empresas y usuarios en la red. Pero, ¿cómo aplica el gobierno chino el control sobre la red? En realidad, no hay una única forma. Se trata de un sistema de control ejecutado en diversos niveles, de forma directa e indirecta, con diferentes sistemas, gran variedad de legislación aplicada por numerosos organismos y con un alto grado de incertidumbre sobre su alcance.

El sistema más conocido del control de contenidos o censura sobre la red del gobierno chino es el denominado como “Gran Cortafuegos”, un hardware o software controlado y ejecutado por el administrador de la red, que filtra o bloquea el acceso de

los usuarios a determinadas direcciones, puntuales o grandes bloques como todas las de un país determinado, dominios concretos o cualquier página que contenga una palabra o un grupo de palabras concreto (MacKinnon 2010).

Pero, no todo el control de los contenidos sobre la red lo ejecuta directamente gobierno. Desde la década de 2000 en adelante, ha aumentado la delegación de la aplicación de las políticas de control y censura hacia actores no gubernamentales (Cheung 2006, 11). De hecho, las empresas tecnológicas, en aplicación de la legislación, se han convertido en verdaderos agentes de control y censura, el brazo ejecutor de la legislación y de las motivaciones políticas del PCCh. Puesto que, según la ley, todas las empresas tecnológicas chinas son responsables de todo lo que aparece y se publica en sus dominios, suya es también la responsabilidad de aplicar la ley bajo amenaza de perder la concesión administrativa o licencia legal para poder seguir con su actividad. Por tanto, la propia empresa es la que se encarga de eliminar el contenido no deseado, según la ley o el PCCh, o eliminar resultados en el caso de los buscadores para, así, no mostrar la ruta a páginas prohibidas o que se considere que amenazan el mantenimiento del orden social o la legitimidad del partido (MacKinnon 2010).

Como medida de control de usuarios y contenidos, no debemos olvidar el monitoreo clásico de la red, que fiscaliza el uso del ciberespacio que hacen los ciudadanos, comentarios que publican o direcciones que visitan. Desde el año 2000, el Ministerio de Seguridad Pública ha contratado a 30.000 personas para rastrear la red, una ciberpolicía desplegada en 700 ciudades y provincias, dedicada a la monitorización constante de redes sociales, páginas de información, y cualquier dirección del ciberespacio para mantener el cumplimiento de la red en el mundo digital, para eliminar el contenido indeseado y detener a los usuarios que incumplen la ley (Lum 2006, 7). Además, como añade Lum, el gobierno chino impulsa la creación de plataformas ciudadanas digitales para que sean los propios ciudadanos los que ejerzan como controladores y rastreadores, convirtiéndose en delatores, y aumentando la sensación de control social en el mundo digital.

El gobierno chino tiene otras formas de controlar los contenidos: con ataques cibernéticos a organizaciones o páginas determinadas para dejarlas inaccesibles a los ciudadanos; bloqueando y apagando totalmente el acceso a la red en momentos muy determinados; controlando y limitando las posibilidades de registro de dominios a ciudadanos anónimos; u obligando a la instalación de programas en los dispositivos bloquear el acceso a contenidos prohibidos y para monitorizar al usuario.

Pero, suponiendo que algún comentario se escape al control ejercido gracias a la informática o al equipo de ciberpolicías, la propaganda se ha convertido en otra de las grandes herramientas de control del régimen. Es interesante observar cómo el PCCh ha conseguido lo impensable, utilizar el potencial democratizador de las TIC en su favor, para acallar a los críticos y dirigir a la opinión pública. El gobierno chino utiliza los comentarios, supuestamente de ciudadanos anónimos, para cambiar la tendencia de la conversación de la crítica hacia un terreno más favorable para el régimen. Realizan una función similar a la de un relaciones públicas, cambiando la imagen negativa por otra más positiva para los gobernantes. Para conseguirlo, el gobierno ha contratado a un ejército de comentaristas, denominado como “el partido de los 50 céntimos”, dedicado exclusivamente a introducir comentarios en el flujo de información de chats, redes sociales o blogs. Se calcula que este ejército de comentaristas profesionales formados por el gobierno, que pueden ser entre 30.000 y 2 millones, generan 448 millones de comentarios falsos en redes sociales (King, Pan y Roberts 2017, 1). Con esta fórmula, el régimen busca mejorar su imagen, reducir los elementos negativos, pero también, generar una sobreinformación sobre un asunto para redirigir el debate hacia otros asuntos más favorables al sistema.

Dentro de esta gran variedad de fórmulas que ha desplegado el PCCh para controlar internet, no podemos olvidar la autocensura, tanto de empresas como de usuarios. La persecución de ciudadanos que publican contenidos inapropiados, la detención arbitraria y puntual de algunos de ellos, muchas veces con gran publicidad por parte de las autoridades a modo de castigo ejemplar, hace que los ciudadanos eviten mantener actitudes críticas o contrarias al régimen y, por tanto, a la ley. Precisamente para fomentar la autocensura y para aumentar el control social, el gobierno chino ha dirigido sus esfuerzos en eliminar el anonimato de la red. Desde 2010, los ciudadanos chinos tienen que usar su nombre real, a través de su tarjeta de identificación, para poder acceder a internet en los cibercafés o para comprar una tarjeta SIM. Desde 2005, la obligatoriedad de registro con nombre real ya se había extendido a portales web chinos masivamente utilizados y redes sociales, que exigen este registro que liga la vida digital y la real, antes de publicar cualquier comentario en línea.

Obligando a uso del nombre real, el gobierno puede rastrear las actividades en la red de cada usuario, creando una ficha personal tan amplia y detallada, que hasta la transformación digital hubiera sido imposible de elaborar, ya que la vida privada quedaba oculta tras las paredes del domicilio, y ahora con las paredes de cristal que ofrecen las

TIC, está expuesta a la mirada del controlador omnisciente. El gobierno completa esa gran base de datos global con la información que, sobre cada usuario, tienen las empresas privadas que prestan los servicios digitales. Por ejemplo, los proveedores de correo electrónico deben mantener información personal y dirección electrónica de los ciudadanos, y la pueden divulgar sin autorización del usuario. Lo mismo sucede con los proveedores de acceso a internet, que deben registrar las direcciones o nombres de dominio a los que han accedido los usuarios, y con los proveedores de información digital, que deben informar sobre qué han publicado, quién, cuándo, cómo y la dirección donde está alojada. Todos estos servicios están obligados a guardar la información durante 60 días y proporcionar todos estos registros al estado si lo requiere (Opennet 2012).

El acceso a los datos privados de los usuarios de las TIC va mucho más allá del correo electrónico. Ya en 2008, la principal operadora china de telefonía móvil, *China Mobile Communications Corporation*, reconoció en el Foro de Davos, que la compañía tenía acceso a un sinnúmero de datos personales de los usuarios, incluida la ubicación, y que los entregaba a las autoridades chinas cuando los solicitaban. Pero desde entonces, la información personal que puede aportar un dispositivo móvil ha aumentado de forma exponencial. La generalización de la conexión a internet a través de los teléfonos inteligentes supone que los dispositivos móviles, además de la ubicación, registran la actividad de los usuarios en redes sociales, comentarios que publica, definir su círculo de amistades en el mundo virtual, páginas que visita, intereses, historial de compra o el historial de ubicación, entre muchos otros datos. Todos estos datos personales en manos de la operadora están, en realidad, en manos del gobierno chino que puede ampliar hasta el infinito la ficha personal de cada ciudadano.

Como vemos, la colaboración de las empresas privadas es esencial para el seguimiento de los ciudadanos. Quizás por eso, además de por el control de la información y contenidos en la red, el gobierno chino se ha esforzado en expulsar, con un marco regulatorio muy exigente y contrario a la mayoría de las leyes occidentales, a las empresas occidentales de ámbito internacional de su territorio. Separando el mercado tecnológico chino del resto del mundo ha alentado el crecimiento y fortalecimiento de empresas propias, en manos de los círculos cercanos a las élites gobernantes, que son fácilmente controlables, que comparten las políticas del gobierno y las cumplen sin poner ninguna objeción para poder mantener la licencia gubernamental para poder seguir con su actividad. La colaboración, forzada o por implicación voluntaria, es amplia y se ha demostrado en varios casos. Además, de las clarificadoras declaraciones de la principal

operadora de telefonía móvil de China, al gigante de las redes sociales china, *Tencent*, reconoció que su aplicación de mensajería instantánea, *QQ*, a más usada en China, tenía un sistema de bloqueo de palabras clave y que, además, monitorizaba y registraba toda la actividad digital del usuario y quedaba a disposición de las autoridades chinas (Opennet 2012).

Pero, aunque el caso chino es el más paradigmático, las democracias occidentales tampoco se libran del uso de las TIC para aumentar el control social de sus ciudadanos. A la cesión ilegal de datos personales privados de los usuarios de la gran red social *Facebook* a una empresa privada de mercadotecnia electoral, que decantó la balanza hacia el sí en el referéndum del Brexit o que llevó a Trump a la presidencia de EE.UU., hay que sumar el sistema de espionaje global que llevó a cabo la Agencia Nacional de Seguridad de EE.UU. (NSA por sus siglas en inglés) entre 2007 a 2015, y que denunció el exagente de la CIA, Edward Snowden. Entre esos años, la NSA tuvo en funcionamiento desde 2007 el programa *Mystic*, que permitía grabar, analizar, tratar y recuperar todas las llamadas telefónicas de un país. Pero, la violación de la intimidad de los individuos de todo el mundo no terminaba ahí, porque con el consentimiento expreso de las grandes empresas tecnológicas norteamericanas de implantación global, la NSA podía acceder a los servidores centrales de *Google*, *Microsoft*, *Yahoo*, *Skype* o *Apple* para recopilar el historial de búsquedas de los usuarios, sus correos electrónicos, chats, registro de conexiones, fotografías y todos sus registros de la vida digital. Así pues, vemos cómo bajo el paraguas de la seguridad nacional estados altamente garantistas y defensores de los derechos individuales llevan a cabo sistemas de vigilancia e información masiva, con la complicidad de sus empresas nacionales para conseguir los datos de los usuarios e implementar sistemas de vigilancia.

El *big data* y el crédito social

Si partimos de las grandes posibilidades que tiene el gobierno chino para obtener y controlar la información privada que los usuarios generan en internet, y que permiten hacer un perfil exhaustivo de su vida diaria, podemos establecer una relación de proporcionalidad entre el uso de la red, la información que obtiene el gobierno del individuo y las posibilidades de control social que ofrece. Por tanto, a mayor uso de las

TIC, más información de los usuarios está disponible en la red y mayor posibilidad de control social.

En China, según los últimos datos disponibles de finales de 2016 del CNNIC, 731 millones de ciudadanos eran usuarios de internet, el 53'2% de la población, mientras que el 95'1% de los *netizens* se conectan a través de su teléfono móvil. Además, el 91% de los *netizens* usaban algún programa de mensajería instantánea, el 82'4% de los usuarios de Internet han utilizado algún buscador y el 84% se informaba a través de la red. Según el “2017 Interim Report” de *Tencent*, la propietaria de la mayoría de plataformas sociales chinas en Internet, la más importante es *WeChat* con 963 millones de usuarios tras sumar los datos de *WeChat* y *Weixin*, seguida por la red de mensajería instantánea *QQ* alcanzó los 86 millones de usuarios mensuales activos, frente a los 586 millones de la tercera plataforma, *QZone*, con 586. La cuarta red social china es *Weibo* que, según los datos de la propia empresa, alcanzó en 2017, los 392 millones de usuarios activos mensuales, con un crecimiento anual del 32%. Aunque no es una red social, en la definición del mercado cibernético chino, no hay que olvidar el gran grupo de comercio electrónico *Alibaba*, el más importante del mundo por delante de *Amazon*, con 515 millones de usuarios anuales en 2017, según el “December Quarter 2017 Results” que ha publicado el grupo.

Ante las grandes posibilidades que ofrece *el big data* para el control social, el 14 de junio de 2014, el Consejo de Estado de la República Popular China publicaba el “Esquema de planificación para la construcción de un sistema de crédito social (2014-2020)” para crear un sistema de crédito social que evalúe a individuos y agencias gubernamentales en cuatro grandes áreas: asuntos administrativos, actividades comerciales, comportamientos sociales y sistema judicial. Según el documento del Consejo de Estado que publicó Rogier Creemers el 14 de junio de 2014 en su blog “China Copyright and Media”, el sistema se basa en un mecanismo de recompensas y castigo, recomendando la sinceridad y castigando la insinceridad, beneficiando a quien sea de confianza y restringir movimientos y operaciones de quienes no lo sean (Shazeda 2017). De hecho, el sistema busca incentivar las buenas conductas con facilidades para las personas confiables y restringiendo las actividades de las personas no confiables o conflictivas para crear una sociedad libre de problemas basada en la sinceridad (Wang 2017).

Pero pese a que la meta está en 2020, el sistema de crédito social lleva años dando pequeños pasos. Bajo un primer objetivo de crear un gran sistema que mida la confiabilidad crediticia de los ciudadanos para evitar el aumento de fraudes e impagos en

los préstamos bancarios, la Comisión Nacional para la Reforma y el Desarrollo, ha puesto en marcha el carné por puntos de buen ciudadano. Desde el 1 de mayo de 2018, los ciudadanos que hayan cometido faltas administrativas, económicas, tengan cuentas pendientes con la justicia o tengan deudas no podrán viajar en avión o tren de alta velocidad durante un año (Xinhua 2018a). La prohibición ya comenzó a aplicarse en 2017 y afectó a más de 6 millones de ciudadanos que tenían deudas financieras pendientes. De momento, es solo un primer paso para dividir la sociedad en buenos y malos ciudadanos, facilitando la vida a los buenos, según el estándar de crédito social, y penalizando a los malos o peligrosos. Pero para la total implantación del sistema de crédito social dentro de 2 años, el gobierno chino debe conseguir crear una gran base de datos que incluya la información que la administración tiene del ciudadano, pero también, la que está al alcance de las empresas tecnológicas. Por eso, el Banco Nacional de China ha dado permiso a ocho empresas privadas para realizar pruebas piloto de sus propios sistemas de solvencia y desarrollar algoritmos que les permitan puntuar a sus clientes para ofrecer facilidades, productos o servicios solo a los que obtengan buenas cifras. De hecho, las compañías que están desarrollando estos sistemas de puntuación pertenecen a los dos gigantes tecnológicos chinos: *Tencent* y *Alibaba*. El proyecto de *Alibaba*, *Sesame Credit*, tiene en cuenta cinco grandes apartados: el historial de crédito de los usuarios, hábitos de comportamiento, capacidad para pagar deudas, información personal y redes sociales (Shazeda 2017). Pero, *Sesame Credit* ya está puntuando a sus usuarios teniendo en cuenta estos apartados y con beneficios y servicios para aquellos que alcanzan una determinada puntuación de confiabilidad y predictibilidad. El sistema de *Sesame Credit* sitúa en 350 la puntuación más baja y en 950 la más alta. Aquellos que obtienen 600 puntos tienen préstamos para comprar en *Alibaba*, con 650 se puede alquilar un coche sin dejar depósito, con 700 se puede viajar a Singapur sin tener que aportar determinados documentos, y si se alcanzan los 750 se puede obtener un visado para viajar a Europa con mayor rapidez. Pero hay más, aquellos que superen los 650 puntos pueden aplazar el pago de tratamientos médicos, pueden usar sombrillas de forma gratuita, u obtener beneficios para alquilar una casa. La cifra de crédito social de la plataforma *Sesame Credit* se utiliza como referencia, como mínimo, en 10 ciudades chinas (Molins 2018).

Pero, sin duda, el gran reto será ampliar estos cinco supuestos con los que se mide la confiabilidad social del individuo a todos los ámbitos de su vida, tanto la analógica como la digital. Aunque el carné por puntos marca el camino, el objetivo final es conseguir la integración de datos oficiales con datos de uso y consumo del ciudadano para

obtener, a partir del mayor número de información posible, un perfil que defina al individuo y lo puntúe según el grado de confiabilidad y conflictividad social, e incluso, se pueda hacer una predicción de su posible comportamiento. Uniendo algoritmos con *big data*, el gobierno busca implantar un alto estándar de moralidad, a través del crédito social, y fortalecer su control sobre la población.

Para conseguir este objetivo, la visibilidad total de la vida de los ciudadanos que aportan las TIC a través del *big data* y la inteligencia artificial son esenciales, y proyectos como el de la ciudad china de Guiyang demuestran hasta qué punto el gobierno considera el sector tecnológico, en muchos sentidos, como estratégico para el futuro del país. Según publica Yuan Shenggao, en el diario oficialista *China Daily*, Guiyang es una de las 16 zonas piloto del país para desarrollar la industria del *big data*, y por eso, allí se están desarrollando proyectos para compartir los datos gubernamentales y unificar el modo de almacenamiento y gestión de los más de 5'3 millones de datos de 54 departamentos e institutos oficiales. Desde 2017, Guiyang utiliza ya el *big data* para grabar, compartir, analizar los datos de los ciudadanos para prestarles mejores servicios. De hecho, desde 2017 está en marcha el portal *Zhuminsheng*, una plataforma de búsqueda y consulta para asuntos civiles, que usa los datos recopilados por los departamentos gubernamentales para ofrecer hasta 180 servicios en línea relacionados con la seguridad social, atención médica, educación y empleo. Pero según Shenggao, una ciudad de esta región, Qingzhen, ha dado un paso más creando una plataforma de evaluación social o crédito social uniendo evaluación crediticia y comunicaciones sociales.

En todo este sistema de control, otro de los elementos claves está en la unión entre la inteligencia artificial y las cámaras de vigilancia de circuito cerrado (CCTV). Se calcula que hay, diseminadas por todo el país, 180 millones de cámaras de seguridad, 20 millones con inteligencia artificial. Con el objetivo público de mejorar la seguridad y agilizar trámites, según una noticia publicada por la agencia estatal de noticias *Xinhua* el 8 de abril de 2018 titulada “Facial recognition assists airport security checks in China”, el *Instituto de Tecnología Inteligente y Verde de Chongqing* y la *Academia China de las Ciencias* han desarrollado un sistema de reconocimiento de los viajeros en menos de un segundo, asociando su imagen de las cámaras de seguridad con los datos que sobre él tiene el gobierno. Este proyecto permite agilizar los controles de seguridad en los aeropuertos, reduciendo el tiempo de facturación y embarque. El sistema ya se ha puesto en marcha en 62 aeropuertos de todo el país, en los que han instalado 557 canales de seguridad. El mejor ejemplo del cómo del gobierno está usando los avances tecnológicos

para mantener, reforzar y fortalecer el control social lo encontramos en la contestataria región autónoma uigur de Xinjiang, la única junto con el Tíbet donde la etnia han no es mayoría. La oenegé *Human Rights Watch* (HRW) ha denunciado que el gobierno chino ha puesto en marcha, en esa región, un programa de vigilancia predictiva basado en el análisis del *big data*. Se trata de la “Plataforma Integrada de Operaciones Conjuntas”, impulsada por la Oficina de Seguridad Pública de Xinjiang, que recibe, almacena y procesa los datos de los ciudadanos obtenidos de diferentes fuentes para predecir el terrorismo.

Una de las fuentes de información son los sistemas de CCTV, donde la inteligencia artificial y el reconocimiento facial, permiten extraer gran cantidad de datos. También hay que añadir el sistema de rastreo wifi, que recoge y almacena dirección IP de los ordenadores, teléfonos inteligentes y cualquier dispositivo en red. La plataforma también utiliza la información que ya tiene la propia administración por diversos motivos, como la propiedad de un vehículo, datos sanitarios, planificación familiar, banca, registros legales, informes oficiales. A esto hay que añadir los datos que los funcionarios y fuerzas de seguridad están obligados a enviar a la plataforma si observan algún comportamiento o actividad extraña como tener muchos libros en casa sin ser profesor. Además, el gobierno provincial, bajo la excusa de una campaña sanitaria, ha elaborado una exhaustiva recogida de datos biométricos de toda la ciudadanía, que incluye huellas digitales, ADN, escáneres de iris y muestras de sangre de todos los residentes en la región de entre 12 y 65 años. Toda esta gran cantidad de información, más la facilitada por las propias empresas tecnológicas, es tratada y sometida a la computación en la nube para que los algoritmos señalen indicios sospechosos: el control predictivo. A partir de ahí, la plataforma señala una lista de individuos peligrosos y que deben ser detenidos para evitar cualquier problema social. En muchos casos, los señalados terminan en campos de reeducación, recordando a la época más dura del maoísmo.

Pero, aunque se puede llegar a pensar que el caso de la región de Xinjiang es un caso aislado de cómo el gobierno chino está utilizando las TIC, la computación en la nube o el *big data* en el control social, hay otros proyectos nacionales que van en esa misma dirección. La muestra está en la denominada “Policía en la nube” (*Police Cloud* en inglés), un sistema que usa los datos disponibles de un ciudadano en la red, desde el historial médico, uso de redes sociales o del teléfono móvil, para elaborar un historial que señala dónde y con quién ha estado cada ciudadano y qué ha estado haciendo. El objetivo de este sistema, denuncia HRW, es descubrir relaciones entre personas, eventos y lugares

para mostrar actividades o relaciones inusuales o peligrosas para el sistema. Esta plataforma, como en el caso de Xinjiang, no es otra cosa que una gran base de datos que integra una gran cantidad de información del ciudadano que la digitalización ofrece: desde los datos básicos como dirección o edad, que ya están en manos de la policía, relaciones familiares, los incluidos en el *hukou*, pero también los que están en la nube como registros de hoteles, vuelos y trenes, datos biométricos, imágenes de CCTV o la información recopilada por las empresas tecnológicas derivada del uso de las TIC. Un ingente volumen de información, que la computación en la nube, la inteligencia artificial, el *big data* y los algoritmos permiten transformar en un pormenorizado análisis del pasado y el presente de los ciudadanos que ofrecen la posibilidad de predecir o alertar posibles actividades o actitudes conflictivas del individuo y, por tanto, dañinas para la paz y la tranquilidad social. analiza el presente y el pasado de los ciudadanos (Human Rights Watch 2017).

4. El control social de Xi Jinping frente al control social de Mao Zedong: análisis comparativo

Para comprender cómo China ha entendido y aplicado el control social desde sus orígenes es necesario analizar la influencia que ha ejercido la moral confuciana. Según las enseñanzas confucianas, la buena conducta de los ciudadanos basada en la moral y las normas establecidas es la que permite mantener el orden social. Entre las buenas acciones está, por ejemplo, la aceptación de la jerarquía establecida en la que el individuo está sometido a la familia y al estado, así como primar las obligaciones frente a los derechos y privilegios de los individuos (Rojek 1989, 142). Confucio situaba a la sociedad y la búsqueda del bien común por delante de cualquier interés individual y, por tanto, es de toda la sociedad la responsabilidad de mantener el orden social y de aplicar las normas, formales o informales, de control social (Chen 2002, 2), y todos sus miembros se convierten en controladores de actitudes contrarias al orden social establecido (Chen 2004, 526). De hecho, hay dos figuras que ejemplifican esta concepción arraigada en la sociedad china. Una es la *baojia*, un sistema de agrupación comunal formada por entre 10 y 25 vecinos, creada durante la dinastía Song (960-1279) y resucitada durante la República (1912-1949), sobre la que el estado delegó la seguridad de la comunidad, y que supuso la institucionalización de la vigilancia mutua entre los ciudadanos. Con la *baojia*,

todo el mundo era vigilante y, al mismo tiempo, vigilado y todos los integrantes eran responsables del cumplimiento de las normas. La otra figura, en vigor durante toda la época imperial, era “La ley de Acusación Secuencial”, es decir, una norma que responsabilizaba al colectivo (familia, comunidad o agrupación) del incumplimiento de las normas por parte de uno de los individuos. En este caso, igual que con la *baojia*, se trata de colectivizar la responsabilidad para colectivizar, también, la vigilancia y el control social.

Pero, aunque cuando llegó al poder en 1949, Mao Zedong, rechazó frontalmente el confucianismo por verlo como el producto de un régimen feudal corrupto, el PCCh consiguió reformular y actualizar las tradicionales formas de control y las ha utilizado para, adaptándose a las grandes transformaciones sociales, mantenerse durante casi 70 años en el poder. Durante casi 30 años, el maoísmo se caracterizó por generar un estado de tensión y alerta constante entre los ciudadanos, en busca de cualquier elemento dentro de la sociedad que atentara o pudiera hacerlo, en contra del orden social establecido, o incluso, tuviera pensamientos que no coincidieran con la ideología oficial.

Durante casi tres décadas, la sociedad china vivió bajo una permanente agitación con fuertes campañas de propaganda y reafirmación ideológica en la que los medios de comunicación, convertidos en meros altavoces del partido y del gobierno, tenían cuatro funciones definidas: propagar las políticas del partido, educar, organizar y movilizar a las masas (Wetherbee 2010, 113). Todos los contenidos de los medios de comunicación estaban controlados y mediatizados por el partido, hasta tal punto que no había diferencia entre información y las campañas masivas de propaganda lanzadas para legitimar las políticas desplegadas, construir una fuerte imagen de Mao como líder indiscutible y conseguir una total identificación entre sociedad y el propio partido. El culto a la personalidad de Mao, junto con la paranoia social azuzada desde las élites de búsqueda de los individuos que amenazaran la continuidad del sistema y minaran su legitimidad, alcanzó su punto álgido durante la Revolución Cultural, en la década de 1960. La creación y despliegue de la denominada Guardia Roja, grupos de jóvenes auto-organizados y desplegados por todo el país, en busca de individuos contra-revolucionarios, burgueses o afines al capitalista. Esto supuso la faccionalización de la sociedad china, donde todos eran investigadores e investigados al mismo tiempo, y donde cualquier acusación, por arbitraria que ésta fuera, era tomada en cuenta y suponía la detención, muerte o el ingreso en un campo de reeducación del individuo. En realidad, el estado de paranoia se debía a volatilidad de las acusaciones, que podían ser absolutamente inconcretas y sin base real,

pero que activaban el mecanismo ideológico de aniquilación física o mental del ciudadano. Solo durante la traumática Revolución Cultural, millones de personas fueron perseguidas, acosadas, encarceladas de forma arbitraria, torturadas, humilladas y asesinadas.

Las acusaciones y las disputas no llegaban nunca a un juzgado. Con un sistema judicial inexistente, el partido ejercía las funciones de sistema judicial y la doctrina política marcaba la dirección para mantener el orden social, y las masas, es decir, las organizaciones grupales como los comités de defensa y seguridad, los comités vecinales o las unidades de producción se erigieron como las grandes estructuras de control social. Los ciudadanos se convirtieron, al mismo tiempo, en perseguidos y perseguidores, controlados y controladores, para mantener el orden social y asegurar el cumplimiento de la ideología del partido. De esta forma, el maoísmo consiguió que el partido entrara en todos los aspectos de la vida de los ciudadanos, convirtiéndose en el elemento central de la sociedad china: dirigía ya todos los aspectos de la vida de los individuos, desde la definición de las políticas nacionales hasta su ámbito privado.

Las medidas económicas adoptadas durante el maoísmo permitieron mantener y aumentar paulatinamente el control social sobre los individuos hasta niveles impensables hasta el momento. Con la colectivización de la tierra y la instauración de las comunas como sistemas de producción agraria, y la creación de las unidades de producción o *danwei* en el desarrollo de la industria estatal, la esfera pública arrebató los pocos momentos de privacidad e intimidad que podía tener un ciudadano durante el maoísmo. La individualidad se diluyó frente al colectivo.

Antes de la privatización de las empresas estatales, cada ciudadano estaba asignado a una unidad de producción o *danwei*. Esta unidad, además de cubrir la mayoría de las necesidades del individuo, comida, vivienda o asistencia médica, era una de las principales estructuras de control social de la época maoísta. Tenía que dar permiso para casarse o divorciarse a sus miembros, repartía las cartillas de racionamiento o permisos de viaje. Por tanto, era la herramienta que garantizaba que sus integrantes cumplieran con las directrices del partido y permitía ejecutar un férreo control social, dando facilidades y beneficios a aquellos que cumplieran con las prerrogativas estatales (Tanigawa 2008, 115). Durante años, el *danwei* se erigió como el principal punto de movilización, ideologización de la sociedad y control social. Pero, además de estas unidades de producción, el maoísmo estableció otros sistemas de control social como los denominados comités de calle o comunidad, que como las *baojia*, eran grupos reducidos de un número determinado de

individuos que se controlaban mutuamente, que actuaba como grupo facilitador de trabajo o asistencia médica, pero también, como agencia de vigilancia y de punto de información policial.

La muerte de Mao Zedong, en 1976, y la llegada al poder de Deng Xiaoping, marcaron el inicio de la espectacular transformación de China. Las reformas económicas que comenzó a aplicar Deng para convertir la economía comunista en una planificada de mercado tuvieron consecuencias más allá de las puramente económicas. La paulatina privatización de las empresas nacionales y el fin de las históricas unidades de trabajo o *danwei* supuso el inicio de un lento declive en el sistema de control social que comenzó a dirigirse hacia un destino incierto. El férreo control social maoísta comenzaba a desmoronarse. La apertura de China al exterior, la entrada de capital extranjero, la necesidad de intercambio de información como elemento básico para implantar y asentar un sistema económico de mercado con “características chinas”, la paulatina pérdida de la centralidad del partido en la sociedad, el proceso de globalización y la confirmación de China como un eslabón esencial de la nueva cadena de montaje globalizada, y la irrupción de las TIC pueden ser algunas de las múltiples causas que afectaron al sistema de control social que había construido Mao Zedong.

Tras años de incertidumbre, la llegada al poder de Xi Jinping en 2012 ha conseguido revertir la tendencia. Desde ese momento, ha centrado sus esfuerzos en reideologizar al partido y a la sociedad. El objetivo principal era volver a situar al PCCh en el centro de la vida de los ciudadanos, tanto en la esfera pública y en la privada, para poder volver a poner en marcha el efectivo sistema de control social de la época maoísta basado en el control de los medios y de la opinión pública y todos los individuos. Pero a Xi, le hubiera resultado casi imposible conseguir sus objetivos y revertir la evolución del control social hasta niveles tan altos como los de la época maoísta sin las TIC. De hecho, la digitalización se ha convertido en el gran aliado del presidente chino para recuperar, actualizar y perfeccionar el viejo control social maoísta.

A finales de 2017, el XIX Congreso del Partido Comunista Chino situó a Xi Jinping al mismo nivel que los históricos Mao Zedong y Deng Xiaoping. Los 2.300 delegados aprobaron incluir en los estatutos del partido el denominado “Pensamiento de Xi Jinping sobre el socialismo con características chinas para una nueva era”, es decir, el gran sueño chino de rejuvenecimiento de la nación para recuperar su papel de líder mundial. En ese mismo congreso, también consiguió que los estatutos situaran a la lucha

contra la corrupción, una de sus principales obsesiones y arma de control político desde que llegó al gobierno, como uno de los principales objetivos del partido.

Pocos meses después del congreso, en marzo de 2018, Xi ejecutaba su definitivo asalto al poder con una extensa reforma constitucional que ha eliminado la limitación de dos mandatos al frente de la presidencia del país. Esta modificación borra de la constitución aprobada en 1982, el sistema de poder colegiado diseñado por Deng Xiaoping para evitar los excesos provocados por la gran acumulación de poder de los 27 años de maoísmo. Desde la muerte de Mao, ningún líder chino había conseguido acumular tanto poder en sus manos ni podía mantenerlo de por vida. Ahora, Xi ha vuelto a situar la figura del líder y del partido en el centro política y la sociedad china. Un ejemplo está en la reciente reforma constitucional que le ha permitido, junto a la eliminación de limitación de mandatos, poner en marcha de la todopoderosa Comisión Nacional de Supervisión (CNS), un órgano anticorrupción estatal situado por encima de los tribunales, que rendirá cuentas y recibirá encargos del propio Xi y su entorno, y que se dedicará a vigilar el correcto comportamiento de los funcionarios. Pero, quizás, la característica que más llama la atención de esta decisión es que absorbe a la Comisión de Central para la Inspección de la Disciplina (CCID), órgano del PCCh que le ha servido para ejecutar su campaña anticorrupción con un claro objetivo de purga de los adversarios, con agencias estatales, volviendo a fusionar estructuras del estado con las del propio partido. Con esta decisión, los límites entre estado y partido, que habían comenzado a trazarse con las reformas económicas de Deng Xiaoping y la transición hacia una economía de mercado planificada, vuelven a difuminarse.

La no diferenciación entre partido y estado tiene graves consecuencias, por ejemplo, en la seguridad jurídica, lo que afecta al control social. Ahora más que nunca, las alambicadas y vagas normas estatales tendrán un componente ideológico en su aplicación, lo que permitirá una clara discrecionalidad por parte de las autoridades que se regirán por directrices políticas definidas por el líder. En realidad, Xi está deshaciendo el camino que comenzó Deng, y vuelve a la senda del maoísmo, donde no existía una normativa legal escrita, ni un sistema judicial o un estado separado del partido. Esta reforma ofrece, como en la época maoísta, plenos poderes al líder y al partido, para llevar a cabo sus políticas o, como en el caso de Xi, aplicar la campaña anticorrupción que ya ha venido utilizando como sistema de purga política de sus adversarios y de los críticos, para ampliar el control y la coacción más allá del partido, incluyendo también, a todos aquellos ciudadanos que ocupen un puesto público. Por tanto, la arbitrariedad con la que

puede funcionar la Comisión Nacional de Supervisión está directamente relacionada con el control social que puede ejercer el partido sobre los ciudadanos.

Por tanto, empezamos a observar puntos de encuentro entre el maoísmo y el gobierno de Xi Jinping, entre otros asuntos, en materia de control social. Ambos períodos y líderes coinciden en su visión de los medios de comunicación como altavoces del ideario del partido, y para conseguirlo, deben ser minuciosamente controlados; en el culto a la personalidad del líder; en la centralidad del partido y a su designación como origen de cualquier decisión que adopte, sea en el ámbito que sea, además de la fuerte ideologización de la sociedad. En este ámbito, Xi ha conseguido perfeccionar el sistema maoísta porque, mientras bajo el gobierno de Mao la arbitrariedad de las decisiones de los gobernantes para mantener el orden social partía de la inexistencia de un sistema normativo, en el caso de Xi Jinping, ha conseguido supeditar el sistema legislativo al partido con una redacción de las leyes lo suficientemente amplia y ambigua como para dejar un amplio margen a la arbitrariedad en su aplicación para cumplir con las necesidades autoritarias del gobierno. Por tanto, vemos cómo dos sistemas autoritarios similares pero alejados en el tiempo buscan conseguir los mismos objetivos, ejercer un férreo control social sobre los ciudadanos para mantener el sistema, su legitimidad y credibilidad, pero con escenarios muy diferentes. Mientras, al maoísmo consiguió aplicar un férreo control social en un estado aislado del mundo, con las fronteras cerradas, y con un sistema económico planificado donde el estado tenía todo el poder y el control, en el caso de Xi, ha conseguido poner en marcha un sistema de control social tan exhaustivo como el maoísta en un país con un sistema planificado de mercado, abierto al mundo y pieza clave del sistema económico globalizado.

En los dos períodos, la clave para ejercer un duro control social en todos los ámbitos para asegurar el mantenimiento del orden establecido y, por tanto, del sistema vigente, ha sido asegurar el control de todos los aspectos de los ciudadanos, sobre todo, la vida privada. Como hemos visto, bajo el maoísmo las estructuras de producción, como las *danwei*, junto con otras estructuras informales de organización, se constituyeron como elementos claros de control social. Además, la generación de un estado de tensión colectivo consiguió convertir en vigilantes a todos los ciudadanos. Bajo el gobierno de Xi Jinping, las TIC y su particular visión sobre su uso y gobernanza, han sido los elementos claves que le han permitido implementar un sistema de control social similar al maoísta en un escenario, a priori, más adverso.

Ante el desmantelamiento paulatino del sistema económico socialista centralizado, el gobierno chino se quedó sin su gran arma para controlar a los individuos y a la sociedad. La transformación a una economía planificada de mercado, donde el ciudadano, aunque solo sea como consumidor, tiene una identidad propia y diferenciada del grupo, no permitía espacios de control social similares a los maoístas. Pero, la entrada de las TIC cambió la situación. En realidad, la digitalización ha ofrecido al gobierno chino de Xi Jinping una posibilidad de control que había desaparecido con las reformas económicas impulsadas por Deng Xiaoping. De nuevo, la vida privada de los ciudadanos ha vuelto a entrar en la escena pública, pero en esta ocasión, con unas posibilidades más amplias y perfectas de control. Todo queda reflejado, cualquier acción puede y es analizable, todo son variables de un algoritmo que permite predecir comportamientos, y generar un sistema universal de reputación social, el crédito social, basado no tanto en las acusaciones más o menos reales en las que el maoísmo basó el sistema de control, sino en hechos medibles como establecer el lugar de residencia, rutas habituales y las que se salen de la rutina, personas con las que se entra en contacto tanto en la vida analógica como en la digital, en qué o en quién se gasta el ciudadano el dinero, aficiones, información a la que solicita acceso, con quién se ha reunido un su casa, conversaciones mantenidas o interacciones establecidas en el mundo digital. Éstas son solo algunas de las posibilidades que el gobierno chino de Xi tiene, ahora mismo, a su alcance para elaborar un sistema de crédito o reputación social, para dividir a los ciudadanos en confiables o elementos enemigos del sistema y a los que el sistema debe controlar o, directamente, detener sin que, por el momento, hayan cometido algún delito. De hecho, el actual sistema de crédito social muestra gradaciones en el índice de confiabilidad social, dejando atrás la criminalización por igual de todos los ciudadanos, independientemente de si el atentado contra el sistema hubiera sido leve, grave, muy grave, de acción o pensamiento. Al establecer este sistema de puntuación numérica que acompañará de por vida al ciudadano, el gobierno chino puede diseñar acciones punitivas concretas para cada grupo de individuos sin tener que recurrir a una generalización del mismo grado de castigo y, por tanto, le permite mantener la imagen de un sistema de control más relajado y no generar un sistema colectivo de rechazo y alarma social.

La tecnología ofrece la posibilidad de almacenar y tratar grandes bases de datos, interconectadas, de consulta inmediata y resultados instantáneos. Permite, por ejemplo, que todos los sistemas policiales y burocráticos que vigilan y recaban información sobre los ciudadanos puedan volcarse en una única base de datos. Todos los datos recopilados,

a través del medio, organismo, agencia o estructura estatal, pueden centralizarse para generar una gran ficha del ciudadano. Toda la información generada por todas las estructuras gubernamentales y del partido, por pequeña que sea, está ya a disposición de las élites gobernantes. Nada se pierde ni se queda en un ámbito determinado, todo se comparte, lo que permite conformar un sistema globalizado, universal y basado en todos los ámbitos de la sociedad de reputación social. El gobierno de Xi utiliza las TIC para elaborar listas negras, al estilo maoísta, pero con tantos datos como la digitalización permite. De hecho, las TIC como nuevo sistema de control permiten mantener un permanente estado de vigilancia, que condiciona los comportamientos de los ciudadanos, pero con una gran ventaja: eliminando la variabilidad del factor humano.

Por tanto, vemos como las TIC permiten aumentar el control social establecido por el partido hasta niveles superiores a los establecidos durante la época maoísta. En realidad, el sistema actual es más fiable, al basarse no en acusaciones más o menos arbitrarias, sino en datos y cifras de la vida real del ciudadano, que pasados por el tamiz ideológico del partido permiten clasificar al ciudadano. Por tanto, vemos que pese al uso de datos objetivos como materia prima, el sistema de crédito social es, al introducir la variable ideológica, igualmente arbitrario como lo era el maoísta, y por tanto, utilizable por el gobierno para sus propios intereses o para mantener el orden social, su legitimidad y credibilidad ante la sociedad y los individuos. Pero, incluso la arbitrariedad derivada del nuevo sistema de reputación social tiene, bajo el gobierno de Xi, una aplicación distinta. Como buen sistema autoritario moderno matizado, busca ofrecer un aspecto de seguridad jurídica, libertad y estado semidemocrático, con lo que cualquier acción o detención es puntual, quirúrgica y lo más escondida posible, fuera de la gran campaña de agitación y persecución generalizada de la Revolución Cultural.

Pero hay otro motivo por el que las TIC y la digitalización acercan al control social ejercido por el maoísmo y con el aplicado ahora por Xi Jinping. Mientras, el mantenimiento del orden social era más sencillo en un sistema comunicativo donde el estado tenía el monopolio de la información y donde las fronteras estaban cerradas, Xi ha conseguido mantener el monopolio de la información en un sistema económico y de comunicación globalizado. Aplicando el concepto de cibersoberanía ha conseguido levantar fronteras donde, supuestamente no las había, en las TIC. Con los sistemas de censura, vigilancia, monitoreo y el bloqueo de acceso, y con la definición normativa de un mercado propio desconectado del resto con obligaciones estrictas para las empresas

tecnológicas internacionales que estén interesadas en el mercado chino, el gobierno de Xi ha conseguido definir un mercado más manejable.

Esta construcción de una intranet china desconectada del mundo se ha llevado a cabo bajo el paraguas de la cibersoberanía. Con la intención de poder ejercer un claro control de la información y contenidos que circulan por la red, y para evitar el contacto de los ciudadanos con elementos que podría alterar el orden y la paz social del sistema, el gobierno bloquea el acceso a determinadas páginas web extranjeras. Hasta hace unos años, la única posibilidad de acceder, sin cortapisas, a la red global era a través de las Redes Virtuales Privadas (VPN por sus siglas en inglés). En estos momentos, el control del gubernamental está dificultando la conexión a través de esta vía, con lo que el muro entre la red china y la red global es cada vez más alto.

Pero la desconexión del mercado chino, por motivos claramente ligados al control social y estratégico del sector de las TIC, ha provocado la creación de un gran mercado chino, con un alto volumen de contenidos, que ofrece a los ciudadanos todo el entretenimiento demandado y que cubre las necesidades de interacción de una sociedad digital. El mercado chino, tanto por usuarios como por generación de contenidos y uso, se ha convertido en uno de los más importantes del mundo. A nadie se le escapa, que el gobierno chino ha incentivado la creación de este gran mercado digital chino, poniendo en marcha el bloqueo de acceso a la red global, pero también, poniendo todas las trabas posibles a las empresas extranjeras para desembarcar en el mercado chino. La ley obliga a permitir un acceso total a los servidores de las empresas y a permitir un control exhaustivo de todos los contenidos. Estas trabas, junto con el cierto clima de inseguridad jurídica al tratarse de sectores estratégicos para el estado, hacen que las empresas extranjeras desechen la posibilidad de instalarse en China.

Por si había alguna duda, la Cámara de Comercio de la Unión Europea en China ha alertado de las intenciones de Xi Jinping de llevar el concepto de cibersoberanía al aspecto de creación tecnológica. Buscando la autosuficiencia tecnológica, en 2015, lanzó un plan para potenciar el desarrollo de sectores claves para el futuro del país como la robótica o la biomedicina. De hecho, en un informe publicado en 2017, la Cámara de Comercio de la Unión Europea en Pekín denuncia el claro favoritismo del gobierno chino para crear un fuerte sector local, inyectando grandes cantidades de dinero público para crear grandes compañías en cerca una decena de sectores tecnológicos clave. En realidad, se trata de grandes empresas financiadas y apoyadas, de forma directa o indirecta, por el gobierno y situadas -como en el caso de *Weibo* o *Tencent*- dentro de la órbita de las élites

gobernantes. Por eso, la creación del nuevo mercado tecnológico chino, a modo de intranet, es uno de los elementos claves para que el PCCh y su líder, Xi Jinping, puedan ejercer un control férreo sobre la sociedad. Controla, no solo la información, sino el propio mercado y las empresas que lo conforman.

Por tanto, la digitalización de la sociedad y de la vida de los ciudadanos le ha dado al presidente Xi la posibilidad de perfeccionar el sistema de control social maoísta. Lo primero que demuestra que Xi ha conseguido actualizar el viejo sistema maoísta es que mantiene un total control sobre los contenidos en un escenario, en principio adverso, como es la red. Ahora el control es, gracias a las TIC, realmente permanente y se ejerce en todos los ámbitos y momentos de la vida cotidiana, no únicamente en los de la esfera pública como durante el maoísmo, pese a la estricta vigilancia del *danwei*. El control es exhaustivo, constante, no deja ángulos muertos, y la respuesta es más rápida y efectiva. Pero, la inteligencia artificial es, quizás, lo que ofrece al gobierno de Xi la gran ventaja competitiva, ya que consigue lo que Mao tanto ansió: crear un sistema de crédito social o confiabilidad social basado en las acciones realizadas como en las que podrían producirse, teniendo en cuenta patrones de comportamiento extraídos del comportamiento digital. En realidad, ahí podemos situar la gran perfección del sistema de control maoísta de Xi, neutralizar cualquier amenaza para el sistema político o económico antes de que, esa amenaza, se haya manifestado. En realidad, esto dota al gobierno de la tan ansiada arbitrariedad necesaria para poder cumplir con los objetivos del líder y del sistema sin contestación legal ninguna.

5. Conclusiones

Aunque la irrupción de las TIC en las sociedades de finales del siglo XX y principios del XXI permitió asociarlas con una posibilidad de mejora de la calidad democrática de los sistemas políticos, e incluso, identificarlas como el arma que permitiría derrocar los autoritarismos, la imagen que muestra las consecuencias de la galopante digitalización es otra muy diferente. La ampliación de la esfera pública a todos los ámbitos del individuo con la desaparición de la privacidad, el rastro electrónico permanente que permite una vigilancia constante y ubiqa de los ciudadanos, y los avances que permiten la predicción de conductas peligrosas para el sistema dejan un escenario abonado para el

fortalecimiento de los autoritarismos y pueden tentar a las democracias a emprender una deriva totalitaria.

La llegada al poder de Xi Jinping supuso un verdadero cambio en el uso de las TIC como arma de control social. Con la mirada puesta en el viejo maoísmo, que consiguió ejecutar un férreo control de la sociedad para impedir el nacimiento y desarrollo de sectores críticos con el partido o con el propio líder, Xi ha sabido usar las herramientas que le ha ofrecido la digitalización de la sociedad para actualizar, adaptar, modernizar y, por tanto, perfeccionar el control social maoísta, incrementado su eficacia para conseguir la inmutabilidad del sistema y mantenerse como líder absoluto del país.

Como buen autoritarismo moderno, Xi presenta al sistema chino de aspecto democrático, pero ‘mejorado’ para evitar el caos y la crisis que generan las democracias occidentales de corte liberal. Por eso, diseña un sistema legal a base de normas y regulaciones, que son lo suficiente vagas para poder aplicarlas con cierta arbitrariedad al introducir la variable de las directrices políticas. Sobrepasando el débil sistema legal chino construido tras la muerte de Mao Zedong, Xi ha vuelto a fortalecer al partido, a situarlo en el centro de la vida de los ciudadanos, y manteniendo el control absoluto sobre todos los aspectos de la sociedad china. Pero, más que el partido, Xi ha recuperado el culto a la personalidad de la época maoísta, siendo él el líder supremo que todo lo controla y todo lo ve. El partido, controlado por Xi, ha vuelto a dominar todos los aspectos de la vida en el país. Los últimos retoques de la constitución han terminado con las ideas de Deng Xiaoping de limitación de mandatos y de un poder colegiado para evitar la acumulación de poder de la época Mao. Ahora, Xi Jinping no tiene limitación de mandatos, todo pasa por él y está volviendo a fusionar el partido con el estado, como en el caso de la Comisión Nacional de Supervisión. El partido y el líder vuelven a controlar la vida del país y los ciudadanos.

En esta vuelta a los orígenes del control social maoísta, las TIC y la visión que sobre ellas y su gobernanza tiene Xi, han sido una herramienta esencial. Primero, porque su concepto de cibersoberanía, le ha permitido ejercer un control total sobre contenidos e infraestructuras digitales. El estado y, por tanto, el partido ha establecido una maraña de normativas y leyes que le permiten acceder, en cualquier momento, a los contenidos y las infraestructuras del sector tecnológico. Además, leyes como la anti-terrorista o la ciberseguridad dan amplia potestad al gobierno y al partido para controlar, eliminar contenidos contrarios al orden establecido, o que, pueden dañar a la moralidad o al partido. Por tanto, la maraña legal diseñada por Xi permite con férreo control,

mediatizado y permitido por el desarrollo de las TIC, pero manteniendo la arbitrariedad de la época maoísta. Segundo, porque el desarrollo de las TIC y la digitalización de la sociedad y de la mayoría de los aspectos de la vida de los individuos permiten establecer un control más exhaustivo sobre la ciudadanía, pero manteniendo el falso aspecto de democracia o de sistema cercano a la democracia con sensación de un cierto grado de libertad.

La transformación digital de la sociedad y de todos los aspectos de la vida de los ciudadanos ha permitido conseguir una de las viejas aspiraciones de control social de la época maoísta, la entrada en la esfera pública de la mayoría de los aspectos de la vida privada. Esta ampliación de la escena pública deja a la vista de cualquier información de los usuarios que, hasta entonces, era muy difícil o, casi, imposible de recopilar. Hasta la digitalización de la sociedad y de la vida de los ciudadanos, ni las tradicionales figuras de control social chinas, la *baojia* o las más modernas maoístas, como la *danwei*, permitían establecer un control permanente, ubicuo y generar decisiones instantáneas. El partido puede ocupar, gracias a la transformación digital la centralidad ansiada, no solo de la vida política, sino entrando hasta el territorio más íntimo de los ciudadanos. Ahora, las TIC permiten conocer prácticamente todos los detalles de la vida del individuo, desde el perfil crediticio y de compras, hasta qué tipos de búsqueda realiza en la red, qué tipo de amigos tiene en redes sociales, qué contenidos comparte o quién son sus amigos. Todo esto, junto con la información tradicional que el estado ya tiene sobre cada ciudadano y con el desarrollo de nuevos sistemas de monitorización y reconocimiento fácil, permiten implementar una gran base de datos centralizada, con información detallada de cada ciudadano.

En los últimos años, el gobierno chino ha otorgado permiso a ocho empresas privadas, todas del sector tecnológico, para diseñar un sistema de crédito social. Cada proyecto busca crear un algoritmo que, con la ingente cantidad de datos que el gobierno tiene sobre cada individuo, pueda situarlo en una escala numérica de confiabilidad social y separar a los confiables de los peligrosos para la continuidad del sistema. De hecho, el propio gobierno ha ido un paso más allá de los propios proyectos del sector privado. En la región autónoma uigur de Xinjiang, el gobierno ha implementado un proyecto de control social que incluye la predicción de futuros actos contrarios. En realidad, esta es la gran meta de cualquier gobierno autoritario y, por supuesto, del gobierno chino: sobre la información obtenida de cada ciudadano predecir si el individuo será o no peligroso para el sistema y, por tanto, para el orden social y político establecido.

Para conseguir sus objetivos, Xi Jinping ha necesitado definir un mercado tecnológico propio y separado del resto. Bajo el paraguas de la cibersoberanía, y con los sistemas de censura aplicados por el gobierno chino para evitar el acceso a contenidos e información potencialmente peligrosos para el estado y el partido, Xi ha conseguido mantener un férreo control sobre los contenidos. Pero la cibersoberanía, con la discrecionalidad de acceso a contenidos e infraestructuras y las duras condiciones normativas exigidas por el gobierno a las empresas extranjeras que quieran operar en territorio nacional, hacen que China no sea un mercado atractivo para la inversión extranjera. Esto, junto con el gran interés del gobierno de Xi de situar a China como una de las grandes potencias tecnológicas, han permitido crear un mercado tecnológico chino de empresas nacionales, financiadas en mayor o menor medida por el gobierno, en manos de círculos cercanos a las élites gobernantes y, por tanto, fácilmente manejables para cumplir con los objetivos de partido y del gobierno, o incluso, que forman parte de las estructuras de poder creadas por el propio Xi para mantener el orden social y el control político de la sociedad.

En realidad, el interés del gobierno de Xi en transformar a China en una potencia tecnológica en 2025 busca, en parte, incentivar el desarrollo de tecnologías propias que permitan conseguir sus objetivos como líder y como partido entre otros, en el ámbito de la vigilancia y el control social. Quizás por eso, China se está convirtiendo en un referente en el desarrollo de las TIC para controlar a la sociedad incluyendo, cada vez más, la inteligencia artificial para ampliar los sistemas de control. De hecho, China ha conseguido implementar el primer gran sistema de censura y control de los contenidos, a través del bloqueo de web, usuarios y palabras prohibidas, a gran escala, y sobre una base de más de 700 millones de *netizens*. Ahora, además de desarrollar nuevos sistemas de control y vigilancia utilizando la inteligencia artificial, el objetivo es conseguir un grado de desarrollo tecnológico que permita la creación de una gran base de datos para los más de mil millones de ciudadanos chinos, que posibilite la interconexión y el tratamiento de un gran volumen de información para permitir la creación del gran sistema de crédito social.

Pero además de implementar novedosos y férreos sistemas de vigilancia sobre individuos y contenidos en la red, Xi ha llevado la propaganda hasta el mundo cibernético. El gobierno utiliza las características propias de la comunicación digital en su propio beneficio. Además de mantener el bloqueo de usuarios, con detenciones puntuales si la transgresión del orden social se considera como peligrosa, Xi utiliza las grandes posibilidades de manipulación informativa y de propaganda que ofrece la red en su propio

beneficio. En ocasiones acalla a la crítica con acciones punitivas, en otras generando un gran volumen de información y contenidos sobre otro asunto para desviar la atención de la ciudadanía sobre un problema concreto. De hecho, el gobierno chino ha cambiado su forma de controlar la red, empezando a utilizar la propaganda a gran escala como otro elemento más de control social, induciendo la creación de un estado emocional y de pensamiento determinado entre la opinión pública. Y para esto, como hemos visto en el caso de las *fake news*, la red es terreno abonado que los gobiernos autoritarios, como el de Xi, explotan para conseguir sus objetivos.

Por tanto, considero probada la hipótesis inicial del trabajo: las TIC le han permitido al PCCh de Xi situarse realmente en el centro de la vida de los ciudadanos y ejercer un control social permanente y en tiempo real sobre ellos. De hecho, Xi Jinping ha perfeccionado el sistema de control social maoísta usando las TIC. La desaparición de la vida privada y la exposición constante y abierta de los datos de los usuarios le ha permitido entrar, como nunca antes, en el ámbito privado de los ciudadanos. Con la eliminación de las sombras que generaba la privacidad, los avances tecnológicos para almacenar y tratar todos los datos para obtener patrones de comportamiento han permitido superar el control maoísta. Si Mao quería descubrir a todo aquel ciudadano contrario a la revolución, para asegurar la pervivencia del sistema aplicando grandes dosis de arbitrariedad interesada, el *big data* y los algoritmos ofrecen la posibilidad de predecir al ciudadano problemático y neutralizarlo antes de que pueda actuar contra el régimen. La vigilancia ubíqua, perpetua e invisible, junto con unos sistemas de conexión y tratamiento de datos cada vez más rápidos, permiten ejercer un control exhaustivo y omnipresente sobre los contenidos de la red y los medios digitales, pero al mismo tiempo, establecer pautas de comportamiento que defina a los buenos y los malos ciudadanos, los confiables por el sistema y los no confiables. La perfección de Xi sobre el maoísmo es obvia: todos los ciudadanos, a todas horas, en todos los lugares tienen su número que señala la confiabilidad social. Nada se escapa. La tecnología ha perfeccionado al ojo humano. Nada se escapa de la inteligencia artificial, ni de los algoritmos, Xi lo sabe y lo utiliza para perfeccionar el viejo sistema maoísta. Ahora el control es más exhaustivo, nada se escapa al control del estado, pero todo, en un ambiente social relajado y bajo una falsa apariencia de democracia.

Bibliografía

Amnistía Internacional. “China. Submission to the NPC Standing Committee’s Legislative Affairs Commission on the ‘National Intelligence Law’”. London: Amnesty International Publications 2017. URL:

<https://www.amnesty.org/download/Documents/ASA1764122017ENGLISH.pdf>

Ball, Kirstie, et. al. “A report on the Surveillance Society”, *Information Commissioner’s Office*, 2006.

Bauman, Zygmunt y David Lyon. *Vigilancia líquida*. Buenos Aires: Paidós, 2013.

Castells, Manuel. *Comunicación y poder*. Traducido por María Hernández Díaz. Madrid: Alianza Editorial, 2009.

——— “El poder de las redes”, *Vanguardia Dossier*, n. 50 (2014): 6-13 URL:

https://www.researchgate.net/profile/Gustavo_Cardoso5/publication/301867379_Movilizacion_social_y_redes_sociales/links/572a5b0708ae2efbdbc1f6c/Movilizacion-social-y-redes-sociales.pdf

Chen, Xiaming. “Community and Policing Strategies: A Chinese Approach to Crime Control”, *Policing and Society*, vol. 12, n. 2 (2002): 1-13 DOI: 10.1080/10439460290006646

——— “Social and Legal Control in China: A Comparative Perspective”, *International Journal of Offender Therapy and Comparative Criminology*, vol. 48, n.5 (2004): 523-36 DOI: 10.1177/0306624X04265225

Cheung, Anne. “The Business of Governance: China’s Legislation on Content Regulation in Cyberspace”, *International Law and Politics*, Vol. 38, n. 1 (2006): 1-38

ChinaFile. “Document 9: A ChinaFile Translation”, *Third Plenum of the Eighteenth Party Congress of the Chinese Communist Party*, 8 noviembre 2013. URL:

<http://www.chinafile.com/document-9-chinafile-translation>

CNNIC (China Internet Network Information Center). “The 39th Statistical Report on Internet Development in China”. Ministerio de Información e Industria. República Popular China. 2017. URL:

<https://cnnic.com.cn/IDR/ReportDownloads/201706/P020170608523740585924.pdf>

Creemers, Rogier. “Planning Outline for the Construction of a Social Credit 2014-2020”, *China Copyright and Media*, 14 de junio de 2014. URL: <https://chinacopyrightandmedia.wordpress.com/2014/06/14/planning-outline-for-the-construction-of-a-social-credit-system-2014-2020/>

Eberhardt, María Laura. “Democracias representativas en crisis. Democracia participativa y mecanismos de participación ciudadana como opción”, *Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades*, n. 33 (2015): 83-106. DOI: 10.12795/araucaria.2015.i33.04

Endeshaw, Assafa. “Internet regulation in China: The never-ending cat and mouse game”, *Information and Communication Technology Law*, vol. 13, n. 1 (2004): 41-78 DOI: [10.1080/1360083042000190634](https://doi.org/10.1080/1360083042000190634)

Flaherty, David. *Protecting Privacy in Surveillance Societies*, Chapel Hill: University of North Carolina Press, 1989.

Foucault, Michel. *Vigilar y castigar, nacimiento de la prisión*. México: Siglo XX Editores, 2009.

Freedom House, “New Report: ‘Breaking Down Democracy’”, 5 de junio de 2017. URL: <https://freedomhouse.org/article/new-report-breaking-down-democracy>

Han, Dong. “From vagueness to clarity? Articulating legal criteria of digital content regulation in China”, *Global Media and Communication*, n. 3 (2016): 211-27 DOI: 10.1177/1742766516675495

Hao, Yeli. “A Three-Perspectiva Theory of Cyber Sovereignty”, *Prism: A Journal of the Center for Complex Operations*, n. 2 (2017): 109-15 URL: http://cco.ndu.edu/Portals/96/Documents/prism/prism_7-2/10-3-Perspective%20Theory.pdf

Human Right Watch (HRW). “China: Police ‘Big Data’ Systems Violate Privacy, Target Dissent”, 19 de noviembre de 2017. URL: <https://www.hrw.org/news/2017/11/19/china-police-big-data-systems-violate-privacy-target-dissent>

Kalathil, Shanti y Taylor Boas. *Open networks, closed regimes. The impact of the Internet on Authoritarian Rule*. Washington: Carnegie Endowment for International Peace, 2003.

King, Gary, Jennifer Pan y Margaret Roberts. “How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument”, *Harvard Dataverse*, vol. 1 (2017). DOI: [10.7910/DVN/QSZMPD](https://doi.org/10.7910/DVN/QSZMPD)

Lagos, Taso, Ted Coopman y Jonathan Tomhav. “‘Paralel poleis’: Towards a theoretical framework of the modern public sphere, civic engagement and the structural advantages of the internet to Foster and maintain parallel socio-political institutions”, *New Media & Society*, n. 3 (2014): 398-414. DOI: [10.1177/1461444813487953](https://doi.org/10.1177/1461444813487953)

Lévy, Pierre. *Cyberdémocratie: essai de philosophie politique*. Paris: Odile Jacob, 2002.

“Libro Blanco de internet”. *Consejo de Estado de la República Popular China*, 8 de junio de 2010. URL: http://www.gov.cn/english/2010-06/08/content_1622956.htm

Lum, Thomas. “Internet Development and Information Control in the People’s Republic of China”, *CRS Report for Congress*, 2006. URL: <https://fas.org/sgp/crs/row/RL33167.pdf>

MacKinnon, Rebecca. “China’s Internet Censorship and Controls: The Context of Google’s Approach in China”, *Human Rights in China*, 12 de enero de 2010. URL: <https://www.hrichina.org/en/content/3248>

—— “Networked Authoritarianism in China and Beyond: Implications for global Internet freedom”, *Hoover Institution & the Center on Democracy, Development and the Rule of Law (CDDRL)*, Stanford University, (2010b). URL: http://fsi.stanford.edu/sites/default/files/evnts/media/MacKinnon_Libtech.pdf

Marx, Gary. “Technology and Social Control”, *International Encyclopedia of the Social & Behavioral Sciences*, 2nd edition. (2015): 117-24 URL: http://web.mit.edu/gtmarx/www/tech_soc_control.pdf

Molins, Albert. “China estrena su ‘Gran Hermano’”, *La Vanguardia*, 3 de mayo de 2018. URL: <http://www.lavanguardia.com/internacional/20180503/443196686690/china-puntuacion-ciudadanos-delitos-sociales.html>

Moore, Adam. “Intangible Property: Privacy, Power, and Information Control”, *American Philosophical Quarterly*, n. 4 (1998): 365-78 URL: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3134093_code202561.pdf?abstractid=1973736&mirid=1

Morozov, Evgeny. *The Net Delusion. The dark side of internet freedom*. New York: Public Affairs, 2011.

Noboa, María Fernanda. “Vigilancia Líquida, de Zygmunt Bauman y David Lyon”, *Revista de Relaciones Internacionales de la UNAM*, n.124 (2016): 185-92 URL: <http://www.revistas.unam.mx/index.php/rri/article/download/57550/51043>

OpenNet Initiative. “Research: China including Hong Kong”, 9 de agosto de 2012. URL: https://opennet.net/research/profiles/china-including-hong-kong#footnote106_6w7jokf

Rojek, Dean. “Social control in the People’s Republic of China”, *Criminal Justice Review*, vol. 14, n. 2 (1989): 141-53 DOI: [10.1177/073401688901400204](https://doi.org/10.1177/073401688901400204)

Rule, James. “Social control and modern social structure”. En *The Surveillance Studies Reader*, editado por Sean Hier y Josh Greenberg. Berkshire: Open University Press, 2007.

Schia, Niels y Lars Gjesvik. “Policy Brief: China’s cyber sovereignty”, *Norwegian Institute of International Affairs*, n. 2 (2017): 1-4 URL: https://brage.bibsys.no/xmlui/bitstream/handle/11250/2434904/NUPI_Policy_Brief_2_17_Schia_Gjesvik.pdf?sequence=4&isAllowed=y

Schmitt, Michael. *Tallin Manual Process on the International Law applicable to Cyber Warfare*, Cambridge:Cambridge University Press, 2013

Shazeda Ahme “Cashless Society, Cached Data. Security Considerations for a Chinese Social Credit System”, *The Citizen Lab* (blog), *Munk of Global Affairs Universidad de Toronto*, 24 de enero de 2017. URL: <https://citizenlab.ca/2017/01/cashless-society-cached-data-security-considerations-chinese-social-credit-system/>

Shenggao, Yuan. “Big data benefits boom in Guiyang”, *China Daily*, 6 de marzo de 2018. URL: http://www.chinadaily.com.cn/cndy/2018-03/06/content_35793303.htm

Soto, Alejandra. “Control y vigilancia social: panorama histórico y aproximación a la sociedad en red”. Trabajo de Grado, Universidad Javeriana, 2016. URL: <https://repository.javeriana.edu.co/bitstream/handle/10554/20898/SotoCastelblancoAlejandra2016.pdf?sequence=1&isAllowed=y>

Tanigawa, Shinichi. “The Chinese Danwei as a Mobilizing Structure: A Research Design for the Cultural Revolution in the Cities”, *Bulletin of the Faculty of Letters*, Aichi Gakuin University, n. 37 (2008): 115-24 URL: http://kiyou.lib.agu.ac.jp/pdf/kiyou_01F/01_37F/01_37_115.pdf

Tsui, Lokman. “Internet in China: Big Mama is Watching You”. Trabajo Final de Máster. University of Leiden. 2001. URL: <https://www.lokman.nu/thesis/010717-thesis.pdf>

Van De Donk, Wim, Thomas Snellen y P.M. Tops. *Orwell in Athens. A perspective on Information and Democracy*. Amsterdam: IOS Press, 1995.

Wang, Maya. “China’s Chilling ‘Social Credit’ Blacklist”, *The Wall Street Journal*, 11 de diciembre de 2017. URL: <https://www.wsj.com/articles/chinas-chilling-social-credit-blacklist-1513036054>

Wetherbee, Rebecca. “Censorship and Evolving Media Policy in China”, *The Elon Journal of Undergraduate Research in Communications*, vol. 1, n. 1 (2010) URL: <http://www.elon.edu/docs/e-web/academics/communications/research/11weatherbeejspring10.pdf>

Xinhua. “China intensifies punishment for credit defaulters”, *China Daily*, 16 de marzo de 2018. URL: <http://www.chinadaily.com.cn/a/201803/16/WS5aabcc2da3106e7dcc142279.html>

—— “Facial recognition assists airport security checks in China”, 8 de abril de 2018. URL: http://english.gov.cn/news/top_news/2018/04/08/content_281476105314850.htm

Zheng, Haiping. “Regulating the Internet: China’s Law and Practice”, *Beijing Law Review*, vol. 4, n. 1 (2013): 37-41 DOI: 10.4236/blr.2013.41005