
**Título:** Ciberseguridad en China: desafíos del siglo XXI

**Autora:** Ana Z. Sánchez Álvarez

**Biografía:** Periodista e investigadora española afincada en China. Doctoranda en Periodismo en la Universidad Complutense de Madrid (UCM) y estudiante del Máster en Comercio Internacional de la Universidad Camilo José Cela. Colaboradora honorífica del Departamento de Empresa Informativa de la Facultad de Ciencias de la Información (UCM 2005-2013) y dela Sección Departamental de Filosofía del Derecho Moral y Política de la misma institución (2004). Entre 2008 y 2013 trabajó en el departamento de Noticias del Canal en Español de la Televisión Central de China (Pekín). Ha trabajado y realizado colaboraciones para diferentes medios (Puntoradio, COPE Madrid2, Radio Intercontinental, Ya.com, PINradio.net), así comoen la producción y realización de un proyecto documental independiente sobre la homosexualidad en China.En la actualidad es miembro del Foreign Correspondents Club of China

**Palabras clave:** ciberseguridad, internet, libertad de información, terrorismo.

**Texto:**

Las nuevas tecnologías están dando forma a un nuevo entorno mediático en China. El país cuenta con la mayor comunidad online del mundo, nada menos que –[1]668 millones de internautas, e internet se ha convertido en el lugar donde casi una tercera parte de los chinos construye relaciones, comercia y expresa sus opiniones. El control de lo que sucede en la red se ha convertido, por tanto, en un importante reto para las autoridades.

[1]Fuente: CNNIC http://www.cnnic.cn/gywm/xwzx/rdxw/2015/201507/t20150723_52626.htm

Con este panorama, en diciembre de 2015 China aprobó una controvertida Ley Antiterrorismo que levantó la alarma entre los defensores de la libertad de información y la protección de datos en internet. La ley, en el apartado dedicado a la ciberseguridad, requiere que las firmas tecnológicas colaboren a la hora de descifrar información, aunque no obliga a la creación de "puertas traseras", que permiten introducirse en los programas por puntos que no son los estándares o normales, como estaba planeado inicialmente. A pesar de que se ha eliminado un artículo presente en el borrador inicial que hubiera requerido a las compañías conservar los datos de los servidores y de los usuarios en China, las compañías del sector se verán obligadas a proporcionar información sensible a las autoridades si éstas lo demandan.

Tras recibir numerosas críticas en Occidente, donde el presidente de los Estados Unidos, Barack Obama, expresó su preocupación ante la posibilidad de que esta ley pueda perjudicar a las empresas foráneas, China se ha defendido argumentando que está haciendo, nada más y nada menos, lo mismo que otras naciones, entre ellas Estados Unidos: pedir a sus firmas tecnológicas que colaboren en la lucha contra el terrorismo.

Precisamente, en septiembre del año pasado el gobierno chino anunciaba haber llegado a un consenso con Washington en materia de ciberseguridad, después de años de acusaciones mutuas de espionaje informático. La Casa Blanca ha culpado en numerosas ocasiones a Pekín de perpetrar ciberataques, calificándolos de "inaceptables", en tanto que las autoridades del país asiático han asegurado estar en contra de los ciberataques y del ciberespionaje, agregando que "castigarán" a cualquiera que lleve a cabo una acción de este tipo.

A través del acuerdo, ambos países se comprometen a responder proporcionando información y asistencia en relación a las actividades maliciosas que tengan lugar en el ciberespacio. Las dos partes, igualmente, acceden a cooperar, de acuerdo a sus respectivas leyes y obligaciones internacionales, en la investigación de los cibercrímenes, recabando pruebas electrónicas y mitigando los ciberataques que puedan producirse en sus territorios. Entre otras cuestiones, el pacto también obliga a que tanto Estados Unidos como China cesen de llevar a cabo o respaldar deliberadamente el uso indebido de la propiedad intelectual, incluyendo información mercantil o empresarial, con la intención de obtener ventajas de tipo comercial.

En lo que a ciberseguridad se refiere, en China, a la Ley Antiterrorismo se suma la Ley de Seguridad Nacional adoptada en el mes de julio del año pasado, y que exige que todas las infraestructuras y sistemas de información sean "seguras y controlables". Para el gobierno chino, estas medidas se hacen necesarias a tenor de la creciente amenaza terrorista que a la que se enfrenta el país, especialmente proveniente de los denominados grupos de "Turkestán del Este", terminología con la que el oficialismo de la República Popular se refiere a los movimientos separatistas que operan en la región de Xinjiang. La ley también se extiende a los medios de comunicación, restringiendo el derecho de estos de informar sobre los detalles de los ataques terroristas, y haciendo énfasis en aquéllos actos que puedan ser imitados o que muestren escenas "crueles e inhumanas".

Surge, en este punto, el temor a que, en China, tanto la Ley de Seguridad Nacional como la Ley Antiterrorista, en nombre de la seguridad del Estado, representen una amenaza contra las ya de por sí limitadas libertad de información y expresión, no sólo de los medios de comunicación sino de toda la población.

El informe sobre la libertad de prensa en China durante 2014 elaborado por la Federación Internacional de Periodistas (FIP), bajo el título China's Media War: Censorship, Corruption & Control, dedica un capítulo a la censura en internet en el país asiático. El texto señala que, en una reunión celebrada el 15 de abril de aquel año, la Comisión Nacional de Seguridad de China (NSC por sus siglas en inglés) concluyó que "el sistema nacional de seguridad debería cubrir once campos, ente ellos la cultura y la información". El presidente del organismo, el presidente chino Xi Jinping, indicó que el rol del NSC debería ser "integral y autoritario" para proteger la seguridad interna y externa de China. Xi Jinping había asegurado anteriormente que "sin ciberseguridad, no hay seguridad nacional".

La ciberseguridad es, indudablemente, uno de los caballos de batalla del gobierno chino pero, ¿qué hay detrás de el control del ciberespacio? Especialistas como Amy Chang, investigadora asociada del Center for a New American Security, consideran que "a pesar de que los desarrollos de la seguridad nacional tienen un nivel de opacidad, está claro que las prioridades de la seguridad en internet de China están motivadas, al igual

que todas las prioridades de modernización militar de China, por el objetivo fundamental del Partido Comunista de mantener su propio gobierno en el poder". (Chang 2014)

Durante 2014 se emprendieron campañas contra la difusión de contenidos pornográficos en internet y contra la publicación de "rumores" que pudieran "fomentar el pánico o perturbar el orden social". También se anunció la obligación de los usuarios de registrarse usando el nombre real en blogs, servicios de microblogs como el popular Sina Weibo y en las secciones de comentarios en la red. En esta misma línea, la FIP denunció la orden dada por la Oficina Estatal de Información de Internet a Phoenix New Media, empresa de medios online, para que corrigiera su sitio web después de que la citada oficina recibiera 1300 quejas en relación a "mensajes dañinos" emitidos desde el mes de enero de 2015. La oficina apuntó que el 16% de las quejas se referían a mensajes políticamente ofensivos y el 38% era de contenido pornográfico, aunque no se especificó cómo esta página web había violado las normas.

La Federación Internacional de Periodistas también hacía un llamamiento a la revisión del borrador de Ley de Ciberseguridad, desvelado por las autoridades chinas el 6 de julio de 2015, al entender que el texto suprimía aún más la libertad de prensa, negando a los ciudadanos el derecho a la información. La FIP, en su crítica al documento, alude a los artículos que obligan al registro de los usuarios en internet mediante su nombre real, así como a la autorización a todos los niveles de gobierno a implementar limitaciones temporales en el uso de internet y de los sistemas de comunicación. Otros observadores también han coincidido en señalar que el borrador restringe el espacio de libertades en internet. Según los analistas, la Administración del Ciberespacio de China y su director, Lu Wei, aglutina más poderes, siendo responsable de planificar y coordinar los esfuerzos de seguridad en internet, así como su gestión y supervisión.

En un artículo publicado por King & Wood Mallesons en julio del año pasado se indica cómo el borrador, compuesto de 68 artículos, ha sido elaborado con el fin de salvaguardar la soberanía del ciberespacio nacional, abarcando las siguientes áreas: construcción, operación, mantenimiento y uso de las redes; y la supervisión y administración de la ciberseguridad dentro del territorio chino. De este modo, establece un régimen regulatorio integral en asuntos de ciberseguridad, crea responsabilidades

legales para los operadores y los proveedores de servicios y define algunos conceptos básicos.

El borrador, por primera vez, introduce el concepto de Critical Information Infraestructures (CII), que incluye redes y sistemas en áreas sensibles como los que proporcionan servicios de comunicación pública y transmisión de televisión; los relacionados con las industrias clave como energía, recursos naturales y seguridad social; ejército y actividades del gobierno. De este modo, se requiere que los operadores de CII firmen un acuerdo de confidencialidad con cualquier proveedor de productos en internet, siendo susceptibles de someterse a revisiones de seguridad por parte de las autoridades. La Oficina Estatal de Información de Internet es responsable de la coordinación de la vigilancia y administración de la seguridad en la red, junto con el Ministerio de Industria Informática y el Ministerio de Seguridad Pública, además de otros ministerios relacionados.

En cuanto a las penas que se exponen en el borrador ante el no cumplimiento de sus obligaciones, los operadores de CII, proveedores de productos y servicios en internet y otras entidades o individuales se incluyen avisos, órdenes de rectificación, confiscación de ingresos ilegales, suspensión del negocio y cierre de páginas web. Igualmente, cualquier violación del borrador de la Ley de Ciberseguridad que cause perjuicios a terceros conllevará responsabilidades civiles, mientras que si el quebrantamiento constituye un crimen estará considerado como un acto criminal.

Otros de los puntos que más preocupan del borrador es el hecho de que se obliga a los operadores de internet a que garanticen la debida protección de sus redes, incluyendo la formulación de protocolos internos de seguridad, la adopción de medidas técnicas para defenderse de ciberataques y el seguimiento de eventos relacionados con la seguridad, además de la copia y encriptación de datos. Es más, se requiere que los operadores suministren programas “no maliciosos” a los usuarios, obtengan su consentimiento para recabar datos sobre sus actividades en internet y les informen cuando se producen casos de riesgos para la seguridad. Los operadores no podrán proporcionar ningún servicio a los usuarios que no faciliten un nombre, teléfono y nombre de dominio reales, entre otros datos.

En realidad, muchas de las de las provisiones no son nuevas, ya que las autoridades chinas llevan largo tiempo restringiendo contenidos y uso de internet. Incluso las medidas más restrictivas del borrador ya se han puesto en marcha en alguna ocasión, como el hecho de poder inhibir el servicio en momentos y regiones concretas con la intención de "salvaguardar la seguridad nacional, la estabilidad social y gestionar algún incidente que pueda amenazar la seguridad social". Así sucedió en 2009, durante las revueltas que tuvieron lugar en la provincia de Xinjiang.

Tras la publicación del borrador de ley, el diario británico Financial Times informaba de que el gobierno chino comenzaría a estacionar oficiales de policía en las principales compañías de internet del país, como el gigante del comercio electrónico Alibaba o el omnipresente Tencent. Según la noticia, estos agentes buscarán pruebas de "actividad ilegal en internet".

Las dos compañías, sin embargo, estarían ya colaborando con las autoridades chinas en la creación de un sistema universal de evaluación de la reputación de los ciudadanos chinos en función de sus hábitos en internet. Dicha evaluación, que puede llegar a ser obligatoria en 2020, iría ligada al número de identidad de cada ciudadano y estaría basada en su actividad política, sus aficiones, sus hábitos de compra e, incluso, en si juega con videojuegos.Según el artículo "Reputation Economy Dystopia: China's new "Citizen Scores", publicado en internet, el programa estará administrado, precisamente, por Alibaba y Tencent. Las puntuaciones, que serán públicas, se generarán no sólo a raíz de las actividades de cada individuo, sino también a partir del comportamiento de los círculos de amistades en las redes sociales, y podría representar un perjuicio, por ejemplo, a la hora de obtener visados para viajar al extranjero.

En una entrevista realizada por International Business Times a Roger Creemers, creador del blog sobre política y legislación sobre medios en China "The Law and Policy of Media in China", éste considera que el programa de puntuación chino está pensado "para crear un nuevo ciudadano", ya que se premian y castigan determinados tipos de comportamiento. Indica Creemers que "éste es un esfuerzo deliberado realizado por el gobierno chino para promover entre los ciudadanos los ¨principales valores socialistas" como el patriotismo, el respeto a los mayores, trabajar duro y evitar el consumo extravagante". Por otra parte, añade, aísla y castiga públicamente a quienes no cumplen

con el modelo de conducta diseñado por las autoridades, en función de sus propios intereses, retomando viejos modelos de represión.

Sea como fuere, es previsible que la ciberseguridad continúe siendo, a medio y largo plazo, una de las prioridades del gobierno chino. Restará ver cómo las medidas que se apliquen representen o no mayores injerencias a la libertad de movimiento de las compañías del sector, tanto chinas como extranjeras, así como dentro de la esfera privada de los usuarios de la red.