ieee.es
Instituto Español de Estudios Estratégicos

Documento
Informativo

01/2017 04 de enero de 2017

David Ramírez Morán

Ciberseguridad en China

Ciberseguridad en China

Resumen:

La Ley de Ciberseguridad promulgada el 7 de noviembre en la República Popular China regula, en tan solo 79 artículos, aspectos tan dispares como la protección de datos, las obligaciones de las empresas e incluso las posibles sanciones a aplicar, para lo que, en otros países, son necesarias varias leyes, reglamentos y códigos. Esta brevedad se consigue mediante una ambigüedad que se presta a la interpretación y que dota a su vez al Gobierno chino de mecanismos para la monitorización, la censura o el proteccionismo que han generado reacciones por parte de organizaciones de defensa de derechos humanos así como de las multinacionales del sector. Las cuestiones sobre derechos y obligaciones de ciudadanos y empresas se abordan desde una aproximación que centraliza la responsabilidad en el Estado, en línea con el modelo de gobernanza del ciberespacio que el país promueve internacionalmente, frente al modelo de cooperación público privada que promueven las normativas comparables de otros países.

Abstract:

The Cybersecurity Law promulgated on November 7th in the People's Republic of China regulates, with only 79 articles, aspects so uneven as data protection, business requirements and even the applicable sanctions, for what, in other countries, several laws, rules and codes are required. The brevity is achieved through ambiguity that also allows for interpretation and provides the Chinese Government with the tools for monitoring, censorship and protectionism that have raised reactions from human rights defence organizations as well as international businesses in the sector. Questions about the rights and obligations of the citizens and enterprises are dealt with using an approach that centralizes responsibility on the State, in alignment with the cyberspace governance model that the country promotes internationally, opposite to the public-private cooperation promoted by the comparable regulations of other countries.

Palabras clave: Ciberseguridad, China, Ley, Privacidad, Censura.

Keywords: Cybersecurity, China, Law, Privacy, Censorship

Introducción

La República Popular China es un país que está recibiendo una constante atención en cuestiones relacionadas con el ciberespacio. Las restricciones existentes a la libertad de expresión y al acceso libre a la información han sido temas controvertidos desde mucho antes de internet. Un gran número de ataques cibernéticos con fines diversos están siendo presuntamente atribuidos a profesionales de ese país. Incluso se ha firmado un acuerdo entre China y Estados Unidos[1] de cese del ciberespionaje comercial financiado por los Gobiernos.

Esta Ley genera el soporte legal que justifica las medidas de monitorización y control del tráfico de internet con las que cuenta actualmente el Gobierno chino. A modo de ejemplo, medidas como la recogida en el Art. 50 de descubrir la transmisión de información prohibida por la ley conlleva una infraestructura de intervención de las comunicaciones salientes del país. Bajo este mismo criterio, analizando las actividades no permitidas, es posible determinar las herramientas necesarias para la investigación y análisis del tráfico en las redes así como las limitaciones que estas imponen al uso libre de las redes.

El primer escollo a salvar para analizar esta ley es el del idioma pues la norma solo está publicada en lengua china. Por este motivo, la información recogida en este documento se basa en una traducción no oficial, tanto del documento final como de los borradores difundidos para comentarios, que se puede obtener en internet[2].

Su elaboración ha sido bastante rápida pues el primer borrador para comentarios se publicaba en el mes de junio, un segundo borrador se emitía en julio[3] y a primeros de octubre se publicaba el tercer borrador[4] que finalmente ha sido promulgado el 7 de noviembre. El texto incluye referencias explícitas al sistema político chino con la «diseminación de los principales valores socialistas» como recoge el Art. 6, o la prohibición del uso de la red para actividades que «inciten la subversión de la soberanía nacional, la caída del sistema socialista, el separatismo; mine la unidad nacional...» como se recoge en el Art. 12. Cabe destacar que del segundo al tercer borrador se han incorporado cuestiones importantes como el Art. 13 orientado a la protección de los

[1] http://internacional.elpais.com/internacional/2015/09/25/actualidad/1443207512_403683.html
[2] http://chinalawtranslate.com/cybersecuritylaw/?lang=en
[3] http://chinalawtranslate.com/cybersecurity2/?lang=en
[4] http://chinalawtranslate.com/%E3%80%8A%E7%BD%91%E7%BB%9C%E5%AE%89%E5%85%A8%E6%B3%95%E3%80%8B%E8%8D%89%E6%A1%88-%E4%B8%89%E6%AC%A1%E5%AE%A1%E8%AE%AE%E7%A8%BF%EF%BC%88%E5%85%A8%E6%96%87%EF%BC%89/?lang=en

menores, el Art. 46 por el que se responsabiliza a individuos u organizaciones de su uso de páginas web y se prohíbe la creación o explotación de redes con fines delictivos o que los promuevan o el Art. 75 que autoriza al Gobierno a congelar activos de individuos u organizaciones extranjeras involucradas en ataques a las infraestructuras críticas de información.

La Ley se puede considerar *holística* por cuanto persigue regular de forma general la seguridad de la información. A título comparativo, sin ser exhaustivos, los contenidos de esta Ley aparecen distribuidos en los articulados de las siguientes normas españolas:

Ley Orgánica de Protección de datos

Reglamento de desarrollo de la LOPD

Ley de Servicios de la Sociedad de la Información

Ley General de Telecomunicaciones

Ley de Protección de Infraestructuras Críticas

Código civil

Código penal

Esquema nacional de seguridad

Estrategia nacional de ciberseguridad

Es evidente que esta situación se produce porque el criterio para definir el objeto de la Ley no ha perseguido la regulación de materias específicas sino que ha abordado directamente el componente transversal de soporte que suponen a día de hoy los sistemas de información. Se trata de una aproximación singular que no se aproxima a ninguno de los modelos legislativos con los que se está abordando la ciberseguridad en otros países[5].

[5]https://www.rsaconference.com/writable/presentations/file_upload/law-w04-global_cybersecurity_laws_regulations_and_liability.pdf

Estructura de la norma

La norma se divide en siete capítulos que contienen un total de setenta y nueve artículos:

Capítulo 1 Provisiones generales (Arts. 1-14)

Capítulo 2 Soporte y promoción de la seguridad de la red (Arts. 15-20)

Capítulo 3 Seguridad de las operaciones en red (Arts. 21-39)

- Sección 1 Provisiones generales (Arts. 21-30)
- Sección 2 Seguridad de operaciones para infraestructuras de información crítica (Arts. 31-39)

Capítulo 4 Seguridad de la información en red (Arts. 40-50)

Capítulo 5 Monitorización, alerta temprana y respuesta a incidentes (Arts. 51-58)

Capítulo 6 Responsabilidad legal (Arts. 59-75)

Capítulo 7 Provisiones suplementarias (Arts. 76-79)

En el primer capítulo comienza con la descripción del objeto de la Ley y su marco de aplicación al territorio principal de China. A continuación, deposita en el Estado todas las responsabilidades relativas a la seguridad de los sistemas.

El capítulo 3 es el más controvertido en lo que respecta a las medidas consideradas como proteccionistas dado que impone serias restricciones a las tecnologías que se pueden incorporar a las infraestructuras de información.

El capítulo 6 se desvía considerablemente del modelo legislativo continental porque introduce en una ley la tipificación de delitos así como las penas o sanciones que resultan de aplicación. En el caso de España, son el Código Civil y el Código Penal las normas en las que vienen recogidas las penas correspondientes por la comisión de un delito. La mayor parte de las sanciones son puramente económicas y permiten la gradación dentro de unos márgenes definidos en la propia Ley para adecuarlas a la gravedad del delito.

Para las empresas se imponen sanciones como el cierre de páginas web, interrupciones de la actividad de las empresas e incluso la cancelación de permisos y licencias de operación, mientras que para los individuos se prevén también detenciones de hasta 5

días o separación de funciones de gestión u operación de redes por plazos de hasta cinco años e incluso de por vida para los condenados por causas criminales.

De naturaleza más diversa, el capítulo 7 incluye una breve lista de términos y definiciones usados a lo largo del documento, se dicta que esta Ley resulta de aplicación para las protecciones de seguridad de operación de redes para el almacenamiento y el procesamiento de información secreta, además de otras leyes y normas administrativas sobre secretos, asigna a la Comisión Central Militar la formulación de las protecciones de seguridad de las redes militares y fija como fecha de entrada en vigor de la norma el 1 de junio de 2017.

De los derechos de los cibernautas

Como se mencionaba previamente, la libertad de expresión se encuentra vetada por la prohibición de tratar ciertos temas.

Se impone a través del artículo 21 un sistema de monitorización por el que los registros de actividad de red deben guardarse durante un periodo de 6 meses.

El Art. 24 trata también los requerimientos de identificación con los datos reales de los usuarios a los operadores que proporcionen servicios de comunicación, ya sea acceso telefónico fijo o móvil, capacidad de publicar información o sistemas de mensajería instantánea.

El Gobierno cuenta, por tanto, con todos los mecanismos necesarios para la investigación de las actividades llevadas a cabo por sus ciudadanos y empresas, si bien es cierto que artículos como el 30 presentan un doble filo pues se puede interpretar como una salvaguarda de la privacidad a la vez que supone la constatación de la implantación de potentes medidas de monitorización de la red.

En su objetivo de filtrar el acceso desde su territorio a la red de forma transparente, son varias las aproximaciones que se han venido aplicando. El denominado Golden Shield es el conjunto de infraestructuras con las que el Gobierno impide la conexión a ciertas páginas web. Ante esta situación, las soluciones tecnológicas que permiten hacer una navegación cifrada pasaron a ser utilizadas tanto por los disidentes del propio país como por los habitantes extranjeros que allí habitan. A lo largo de los años se ha producido una competición permanente entre la utilización de herramientas cada vez más avanzadas

para esquivar la acción del Golden Shield y el desarrollo de nuevas funcionalidades con las que detectar, interceptar e impedir su correcto funcionamiento.

Se trata de un sistema con una potencia considerable, como queda reflejado por las consecuencias que se produjeron cuando las capacidades tecnológicas de Golden Shield se utilizaron para atacar a diversas páginas web. La magnitud de los ataques alcanzó tal magnitud que se pasó a denominar Grand Canyon en referencia a la potencia de los ataques de DDoS atribuidos.

Del proteccionismo

El Art. 22 resulta especialmente importante en un contexto como el actual en el que la falta de actualización de los sistemas se convierte en una grave brecha de seguridad debido a las vulnerabilidades que no pueden subsanarse por no existir nuevas versiones del software. El artículo requiere tomar medidas inmediatas ante la detección de un fallo o vulnerabilidad, así como informar al usuario y a los departamentos competentes. En un segundo párrafo también establece la obligatoriedad de mantenimiento de seguridad de los equipos en el plazo pactado con los clientes.

El artículo 23 requiere que los equipamientos críticos y especializados estén certificados por un establecimiento cualificado incluso antes de poder ser vendidos o proporcionados.

La Ley incide también en la creciente preocupación de los Estados por que los datos de sus ciudadanos permanezcan en su territorio persiguiendo el doble fin de que su seguridad esté sometida a la legislación nacional y que las autoridades tengan acceso a esa información de acuerdo a la legislación local. Se hace frente así a uno de los problemas que dificultan la atribución de hechos delictivos a su autor, al eliminar las fronteras para acceder a la información de un ciudadano. Esto queda recogido en el Art. 37, por el que «la información personal y otros datos importantes [sic] recopilados o producidos por operadores de infraestructuras críticas de información ...» deben ser almacenados en el territorio principal de China. La transgresión de esta norma está severamente penada por el Árt. 50 con multas de 50.000 a 500.000 renmimbi a la empresa y de 10.000 hasta 100.000 al o a los empleados responsables, así como la posibilidad de suspender las operaciones, el negocio, el cierre de páginas web o la revocación de permisos e incluso las licencias de negocio.

Conclusiones

No cabe duda de que esta Ley, por sí sola, resulta insuficiente para la regulación de un contexto tan complejo como el ciberespacio en China. El desarrollo de esta norma resulta imprescindible para su aplicación. Esto se puede producir bajo varios modelos que van desde la creación de jurisprudencia a partir de los fallos de los juicios por vulneración de los preceptos de esta norma, hasta la elaboración de reglamentos o documentos de referencia sobre los principios y criterios de aplicación de cada precepto. En el primer caso se genera una situación de inseguridad en tanto en cuanto no se resuelvan un número significativo de casos, mientras que en el segundo caso se corre el mismo riesgo que se ha producido durante la elaboración de esta norma y que se puede achacar a haber primado la soberanía nacional: no se ha prestado ninguna atención a las advertencias sobre los problemas identificados por terceras partes.

El trasfondo técnico que es posible identificar en esta ley recoge una serie de normas, medidas y prácticas que, en muchos casos, se encuentran totalmente alineadas con las que se están aplicando globalmente para la protección de los sistemas de información y comunicaciones. La implantación de medidas de protección, la obligación de informar ante un ataque, el almacenamiento de los metadatos de las comunicaciones, el fomento de la compartición de información entre organismos y organizaciones o la necesidad de concienciación y formación de usuarios y profesionales son contenidos que aparecen tanto en esta Ley como en las regulaciones de Estados que apuestan por un modelo de gobernanza depositado en las partes interesadas y no en los Estados. Es a la hora de determinar la autoridad encargada de imponer las leyes así como el órgano responsable de garantizar los derechos e infraestructuras necesarias cuando surgen las principales diferencias.

La enorme distancia que separa la cultura del país asiático de la cultura occidental limita la posibilidad de poder utilizar esta norma como referencia para el desarrollo de nuevas normativas nacionales en otros países. Sin embargo, no es esfuerzo fútil recorrer el articulado para identificar problemas latentes que deben ser tratados con las distintas aproximaciones compatibles con el sistema legislativo del país en cuestión.

David Ramírez Morán
Analista principal del IEEE