Informe de enfoque por países: leyes e iniciativas de políticas relacionadas con Internet en China

Veni Markovski y Alexey Trepykhalin
31 enero 2022
GE-010 (actualizado)

ICANN

ÍNDICE

Introducción

Este documento cubre las iniciativas políticas relacionadas con Internet y las leyes/normas presentadas por China entre el 16 de diciembre de 2015 y el 5 de noviembre de 2021; asegurando que la comunidad de la ICANN disponga de la información necesaria para desarrollar una mejor comprensión de las deliberaciones que tienen lugar en la ONU, la UIT y otros organismos de las Naciones Unidas.

Esto forma parte de una serie periódica de informes específicos de cada país que ofrecen un resumen general de las actividades pertinentes para el ecosistema de Internet y la misión de la ICANN. El seguimiento de estas iniciativas es una responsabilidad fundamental del equipo de Participación de Gobiernos y Organizaciones Intergubernamentales (GE) de la organización de la ICANN, al mantener informada a la comunidad más amplia de la ICANN sobre cuestiones de importancia para la Internet global, única e interoperable y sus sistemas de identificadores únicos.[1]

Al igual que los anteriores documentos de GE, este informe se basa en textos de fuentes primarias relacionados con las políticas y tecnologías de Internet, como el Sistema de Nombres de Dominio (DNS), las direcciones de Protocolo de Internet (IP) y los parámetros de protocolo, entre otros. Además, este documento se basa en textos, declaraciones y disposiciones legales/normativas pertinentes sobre las posiciones de China en los mismos temas en las Naciones Unidas (ONU), en la Unión Internacional de Telecomunicaciones (UIT) y a nivel nacional.

Declaraciones e iniciativas en materia de política exterior de China

El 16 de diciembre de 2015, en un discurso en la Ceremonia de Apertura de la Segunda Conferencia Mundial de Internet en Wuzhen[2], el Presidente de la República Popular China, Xi Jinping, expresó lo siguiente: "...la comunidad internacional debe potenciar el diálogo y la cooperación sobre la base de la confianza y el respeto mutuos, promover la transformación del sistema de gobernanza mundial de Internet y trabajar juntos para fomentar un ciberespacio pacífico, seguro, abierto y cooperativo y poner en marcha un sistema de gobernanza mundial de Internet multilateral, democrático y transparente."[3]

Para lograrlo, el Pesidente Xi declaró que es necesario el "respeto a la cibersoberanía" de los países individuales, con la participación en la "gobernanza del ciberespacio internacional en pie

[1] "Planes operativos y financieros de la ICANN", p. 47, organización de la ICANN, diciembre de 2020, https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf.
[2] La Conferencia Mundial de Internet se celebra anualmente en la ciudad de Wuzhen, provincia de Zhejiang, a cargo de la Administración del Ciberespacio de China y el Gobierno Popular Provincial de Zhejiang http://www.wuzhenwic.org/2020-10/15/c_547699.htm. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: https://www.wicwuzhen.cn/.
[3] Comentarios de H.E. Xi Jinping, Presidente de la República Popular China, en la ceremonia de apertura de la Segunda Conferencia Mundial de Internet, Wuzhen, 16 de diciembre de 2015. https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.

de igualdad" como uno de los cuatro principios rectores.[4] President Xi also added that "International cyberspace governance should feature a multilateral approach with multi-party participation. Debe basarse en la consulta entre todas las partes, aprovechando la función de diversos actores, como gobiernos, organizaciones internacionales, empresas de Internet, comunidades tecnológicas, instituciones no gubernamentales y ciudadanos individuales. No debe haber unilateralidad. Las decisiones no deben tomarse con una sola parte que lleve la voz cantante o con unas pocas partes que debatan entre sí. Todos los países deben intensificar la comunicación y el intercambio, mejorar el diálogo y el mecanismo de consulta sobre el ciberespacio, y estudiar y formular las normas de gobernanza mundial de Internet, para que el sistema de gobernanza mundial de Internet sea más justo y razonable y refleje de forma más equilibrada la aspiración y los intereses de la mayoría de los países".[5]

El 7 de marzo de 2016, durante la sesión del Comité Asesor Gubernamental (GAC) de la ICANN, el representante de China subrayó que los "cuatro principios y las cinco propuestas" que presentó el Presidente Xi en la Segunda Conferencia Mundial de Internet de 2016 en Wuzhen "nos proporcionan una (indiscernible) relación del pensamiento y las posiciones de China para la gobernanza de Internet".[6]

El 27 de abril de 2016, China dio a conocer su Estrategia Nacional de Ciberseguridad,[7] y explicó la importancia que tiene para el país el "fortalecimiento de la cooperación internacional en el ciberespacio". Para ello, la estrategia detalla que esta cooperación debe "promover la reforma del sistema de gobernanza mundial de Internet" y "la internacionalización de la gestión de las direcciones de Internet, los servidores de nombres de dominio y otros recursos básicos de este tipo". En la estrategia también se expresó apoyo para que "las Naciones Unidas desempeñen una función de liderazgo, promuevan la formulación de normas internacionales para el ciberespacio que sean universalmente reconocidas por todas las partes, y un tratado internacional contra el terrorismo en el ciberespacio, completen los mecanismos de asistencia judicial para atacar la ciberdelincuencia, profundicen la cooperación internacional en ámbitos como las políticas y las leyes, la innovación tecnológica, los estándares y las normas, la respuesta a las emergencias, la protección de las infraestructuras críticas de información, etc.". También solicitó "establecer un sistema de gobernanza internacional de Internet multilateral, democrático y transparente".

El 2 de marzo de 2017, China publicó la Estrategia Internacional de Cooperación en el Ciberespacio.[8] It states that "China will push for institutional reform of the UN Internet Governance Forum to enable it to play a greater role in Internet governance, strengthen its

[4] Comentarios de H.E. Xi Jinping.
[5] Comentarios de H.E. Xi Jinping
[6] MARRAKECH – Reunión gubernamental de alto nivel del GAC, lunes 7 de marzo de 2016, ICANN55 | Marrakech, Marruecos, página 86 https://gac.icann.org/transcripts/public/transcript-icann55-gac-hl-governmental-meeting-2016-03-07.pdf.
[7] China Copyright and Media, Estrategia Nacional de Seguridad del Ciberespacio, actualizada el 27 de diciembre de 2016, Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm. https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/.
[8] Estrategia internacional de cooperación en el ciberespacio, China Daily, 2 de marzo de 2017, https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.china.org.cn/chinese/2017-03/07/content_40424606.htm.

decision-making capacity, secure steady funding, and introduce open and transparent procedures in its member election and report submission." La Estrategia Internacional de Cooperación en el Ciberespacio también afirma que China "participará en los debates internacionales sobre la distribución y gestión justas de los recursos críticos de Internet", y que "promoverá enérgicamente la reforma de la ICANN para convertirla en una institución internacional verdaderamente independiente, aumentar sus representaciones y garantizar una mayor apertura y transparencia en su proceso de toma de decisiones y funcionamiento".[9]

El 20 de abril de 2018, en la Conferencia Nacional de Trabajo sobre Ciberseguridad e Informatización en Pekín, el Presidente Xi dijo que "de cara al futuro, la reforma del sistema de gobernanza global de Internet es la tendencia general y una aspiración común". Agregó que "la gobernanza del ciberespacio internacional debe persistir en la participación multilateral y la participación de múltiples partes interesadas, dando rienda suelta a las funciones de todos los tipos de actores, incluidos los gobiernos, las organizaciones internacionales, las empresas de Internet, la comunidad técnica, las organizaciones civiles y los ciudadanos individuales. Debemos promover la gobernanza del ciberespacio en el marco de las Naciones Unidas y también debemos realizar un mejor trabajo para dar rienda suelta a la función positiva de todo tipo de actores no estatales".[10]

El 9 de julio de 2019, en sus presentaciones al Grupo de Trabajo de Composición Abierta (OEWG) sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional, China señaló lo siguiente: "Los Estados deben trabajar conjuntamente para crear un sistema de gobernanza mundial de Internet multilateral, democrático y transparente. La organización encargada de la gestión de recursos críticos, como los servidores raíz, debería ser realmente independiente del control de cualquier Estado para garantizar la amplia participación y la toma de decisiones conjunta de todos los Estados".[11]

En abril de 2020, China presentó la siguiente contribución al informe preliminar del OEWG de la ONU, en el que estableció lo siguiente: "Dada la cantidad limitada de tiempo que tenemos, también se debe llamar la atención para evitar la introducción en el informe de conceptos que aún no han obtenido un consenso global ("núcleo público", por ejemplo)", y también: "Durante las dos sesiones anteriores, las partes, incluida China, han presentado docenas de propuestas constructivas sobre cuestiones como la cibersoberanía, la seguridad de la cadena de suministro, la protección de la infraestructura crítica, la abstención de sanciones unilaterales y

[9] Estrategia internacional de cooperación en el ciberespacio, China Daily, 2 de marzo de 2017.
[10] New America, traducción: Discurso del 20 de abril de Xi Jinping en la Conferencia Nacional de Trabajo sobre Ciberseguridad e Informatización, 30 de abril de 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm.
[11] Presentaciones de China al Grupo de Trabajo de Composición Abierta sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional, 7 de julio de 2019. https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

la lucha contra el ciberterrorismo. Se espera que estas propuestas puedan incorporarse en el informe".[12]

El 8 de septiembre de 2020, el Ministerio de Asuntos Exteriores chino publicó una Iniciativa Global sobre Seguridad de Datos, en la que aborda la necesidad de que los Estados cooperen mejor en el ámbito de la seguridad de datos, la ciberdelincuencia, etc. El documento sugiere que "los gobiernos, las organizaciones internacionales, las empresas de TIC[13], las comunidades tecnológicas, las organizaciones civiles, las personas y todos los demás actores realicen esfuerzos concertados para promover la seguridad de los datos bajo el principio de amplia consulta, contribución conjunta y beneficios compartidos". El documento solicita a los Estados que, entre otras cosas, "traten la seguridad de los datos de forma exhaustiva, objetiva y basada en pruebas, y mantengan una cadena de suministro abierta, segura y estable de productos y servicios mundiales de TIC".[14]

En marzo de 2021, la conferencia legislativa anual "Dos sesiones" aprobó el 14.º Plan Quinquenal y la Visión 2035, en cuyo Capítulo 18 (Creación de un buen ecosistema digital), Sección 4 (Promover la construcción de una comunidad con un futuro compartido en el ciberespacio), se establece lo siguiente: "Impulsar los intercambios y la cooperación internacional en el ciberespacio, y promover la formulación de normas internacionales en materia digital y de ciberespacio dentro de las Naciones Unidas como canal principal y la Carta de las Naciones Unidas como principios básicos. Promover el establecimiento de un sistema de gobernanza mundial de Internet multilateral, democrático y transparente, y establecer un mecanismo de gobernanza de recursos e infraestructuras de red más justo y razonable".[15]

El 10 de marzo de 2021, durante las deliberaciones del OEWG en la ONU, China declaró: "Los Estados deberían participar en la gestión y distribución de los recursos internacionales de Internet en pie de igualdad".[16]

---

[12] Contribución de China al informe preliminar inicial del OEWG, 16 de abril de 2020 (fecha de las propiedades del PDF), https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf .

[13] TIC – tecnologías de la información y las comunicaciones, UNTERM - Base de datos terminológica de las Naciones Unidas, https://unterm.un.org/unterm/display/record/imo/na?OriginalId=551772be82184a22adaeb86841e335e6.

[14] Iniciativa mundial sobre la seguridad de los datos, sitio web del Ministerio de Asuntos Exteriores de China, 8 de septiembre de 2020, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202009/t20200908_599773.html y China lanza una iniciativa global de seguridad de datos para oponerse a la politización de las cuestiones de seguridad de datos, Reuters, 7 de septiembre de 2020, https://www.reuters.com/article/wangyi-global-digital-security-0908-idCNKBS25Z0AJ. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: https://www.fmprc.gov.cn/chn/pds/ziliao/tytj/t1827469.htm.

[15] Guancha, El "14.º Plan Quinquenal" y el esquema de objetivos a largo plazo para 2035 (texto completo), 13 de marzo de 2021, https://www.guancha.cn/politics/2021_03_13_583945_5.shtml.

[16] Grupo de Trabajo de Composición Abierta sobre los avances en el ámbito de la información y las telecomunicaciones en el contexto de la seguridad internacional, tercera sesión sustantiva, 8–12 de marzo de 2021, resumen del presidente del OEWG, documento de sala de conferencias, 10 de marzo de 2021, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

El 29 de junio de 2021, China y la Federación Rusa emitieron una declaración conjunta en la que acordaban ampliar el actual "Tratado de Buena Vecindad y Cooperación Amistosa" bilateral. En la declaración conjunta, acordaron "reafirmar su compromiso de reforzar la seguridad de la información internacional tanto a nivel bilateral como multilateral" y subrayaron "su unidad en cuestiones relacionadas con la gobernanza de Internet, que incluyen garantizar que todos los Estados tengan los mismos derechos a participar en la gobernanza de la red mundial, aumentar su papel en este proceso y preservar el derecho soberano de los Estados a regular el segmento nacional de Internet". Rusia y China hacen hincapié en la necesidad de potenciar la función de la Unión Internacional de Telecomunicaciones y reforzar la representación de ambos países en sus órganos de gobierno".[17]

El 1 de noviembre de 2021, la Federación de Rusia presentó su texto preliminar[18] de una propuesta de Convenio sobre la Ciberdelincuencia de las Naciones Unidas y anunció que el texto estaba copatrocinado por China.[19,20]

El 5 de noviembre de 2021, China presentó sus propuestas para la primera sesión del Comité Ad Hoc (AHC) de la ONU.[21] Entre otras cosas, el documento establece lo siguiente: "Se solicita a los Estados miembros que tipifiquen como delito la intrusión y la destrucción de instalaciones, sistemas, datos o infraestructura de información crítica de las TIC. Esto puede incluir el acceso ilegal a los sistemas de información informática, la interferencia ilegal con los sistemas computarizados de información, la adquisición ilegal de datos informáticos, la interferencia ilegal con los datos informáticos, la violación de la infraestructura de información crítica, etc."

Declaraciones, legislación y normativas nacionales

El 1 de julio de 2015 se aprobó la Ley de Seguridad Nacional. En ella, se establece lo siguiente (art. 59): "El Estado establece sistemas y mecanismos de gestión de revisión y supervisión de la seguridad nacional, llevando a cabo la revisión de la seguridad nacional de las inversiones comerciales extranjeras, artículos y tecnologías especiales, productos y servicios de tecnología de la información de Internet, proyectos que implican asuntos de seguridad nacional, así como otros asuntos y actividades importantes, que repercutan o puedan repercutir en la seguridad

[17] Embajada de la Federación Rusa en el Reino Unido de Irlanda del Norte y Gran Bretaña, Declaración conjunta de la Federación Rusa y la República Popular China en el vigésimo aniversario del Tratado de Buena Vecindad y Cooperación Amistosa entre la Federación Rusa y la República Popular China, 28 de junio de 2021, https://www.rusemb.org.uk/fnapr/7007. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.xinhuanet.com/2021-06/28/c_1127606620.htm.
[18] Convención de las Naciones Unidas sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, 27 de julio de 2021, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf .
[19] Nuevo Convenio de la ONU contra la ciberdelincuencia por entrar en vigor, fm4.orf.at, https://fm4.orf.at/stories/3019118/ .
[20] Konstantinos Komaitis, cuenta de Twitter, 1 de noviembre de 2021 y 19 de enero de 2022, https://twitter.com/i/web/status/1455217317504327683.
[21] Sugerencias de China sobre el alcance, los objetivos y la estructura (elementos) de la Convención de las Naciones Unidas sobre la Lucha contra la Utilización de las TIC con Fines Delictivos: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf.

nacional".[22] El Artículo 25 de la ley establece: "El Estado establece un sistema nacional de protección de la seguridad de la red y la información, [...] aumentando la administración de la red, manteniendo la soberanía del ciberespacio, la seguridad y los intereses de desarrollo".

El 1 de junio de 2017, entró en vigencia la Ley de Ciberseguridad (CSL). Estipula que el Estado es responsable de "promover un ciberespacio pacífico, seguro, abierto y cooperativo, y establecer un sistema de gobernanza de Internet multilateral, democrático y transparente". La ley también establece una disposición para almacenar los datos de Internet en el "territorio continental de China". El Artículo 31 de la ley define el alcance de la infraestructura crítica de información para incluir un "sistema de protección multinivel de ciberseguridad para los servicios públicos de comunicación e información, energía, tráfico, recursos hídricos, finanzas, servicio público, gobierno electrónico y otra infraestructura crítica de información". El Artículo 37 de la ley establece que "cuando, debido a los requisitos de la empresa, sea realmente necesario proporcionarla [información personal, datos importantes] fuera de la región continental, [los operadores de infraestructuras críticas de información] seguirán las medidas formuladas conjuntamente por los departamentos de ciberseguridad e informatización del Estado y los departamentos pertinentes del Consejo de Estado para llevar a cabo una evaluación de la seguridad; cuando las leyes y las normas administrativas lo dispongan de otro modo, seguirán dichas disposiciones".[23] (Las disposiciones pertinentes se proporcionan en el Apéndice 1 del presente documento).

El 24 de agosto de 2017, el Ministerio de Industria y Tecnología de la Información de China (MIIT) publicó una versión revisada de las Medidas sobre la administración de los nombres de dominio de Internet. [24] (Las disposiciones pertinentes se proporcionan en el Apéndice 2 del presente documento).

El 29 de enero de 2018, el MIIT anunció, sobre la base del Artículo 5 de sus nuevas medidas mencionadas anteriormente, el Sistema Chino de Nombres de Dominio de Internet adaptado.[25] (The relevant provisions are provided in Appendix 3 to this paper.)

El 13 de junio de 2019, las Medidas sobre la evaluación de la seguridad de la transferencia transfronteriza de información personal propusieron lo siguiente en el Artículo 2: "Los

[22]China Law Translate, Ley de Seguridad Nacional de la República Popular China, 1 de julio de 2015, https://www.chinalawtranslate.com/en/2015nsl/. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm.

[23] New America, Traducción: Ley de Ciberseguridad de la República Popular China (en vigencia a partir del 1 de junio de 2017), 29 de junio de 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

[24] Ministerio de Industria y Tecnología de la Información, Medidas sobre la administración de los nombres de dominio de Internet, 24 de agosto de 2017 https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.cac.gov.cn/2017-09/28/c_1121737753.htm.

[25] La URL a la fuente china no funciona al 19 de agosto de 2021, en inglés: https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://xn--eqrt2g.xn--vuq861b/#.

operadores de redes que proporcionen información personal recopilada en el curso de las operaciones dentro del territorio continental de la República Popular China (en lo sucesivo, denominada transferencia saliente de información personal), realizarán evaluaciones de seguridad de conformidad con estas Medidas. Si la evaluación de seguridad determina que la transferencia saliente de información personal puede afectar a la seguridad nacional o perjudicar el interés público, o que la seguridad de la información personal es difícil de proteger eficazmente, dicha información no podrá salir del país. Cuando el Estado tenga otras disposiciones sobre la transferencia saliente de información personal, se aplicarán dichas disposiciones". [26]

El 10 de junio de 2021, la 29.ª reunión del Comité Permanente de la 13.ª Asamblea Popular Nacional adoptó la Ley de Seguridad de Datos (DSL).[27] (See relevant texts from the law in Appendix 4 to this paper.)

El 30 de julio de 2021, se publicó el nuevo Reglamento sobre la protección de la seguridad de las infraestructuras críticas de información (tras su adopción por parte del Consejo de Estado de China el 27 de abril de 2021). El Reglamento define el alcance de la Infraestructura crítica de información, proporciona disposiciones para que las "industrias y sectores" proporcionen más detalles sobre el alcance, y define los requisitos de notificación de estos organismos a las autoridades centrales de cibernética en caso de un "incidente de ciberseguridad especialmente grave", como la filtración de información personal "relativamente a gran escala".[28] El Reglamento entró en vigencia el 1 de septiembre de 2021. (Los artículos pertinentes del Reglamento se proporcionan en el Apéndice 6 del presente documento).

El 20 de agosto de 2021, el Comité Permanente de la Asamblea Popular Nacional de la República Popular China aprobó la Ley de Protección de la Información Personal (PIPL). La ley entró en vigencia el 1 de noviembre de 2021. La ley "está formulada [...] para proteger los derechos e intereses de la información personal, estandarizar las actividades de tratamiento de información personal y promover el uso racional de la información personal". La información

[26] New America, traducción: Nueva versión preliminar de normas sobre la transferencia transfronteriza de información personal fuera de China, 13 de junio de 2019, "Medidas de evaluación de la seguridad de la transferencia saliente de información personal (versión preliminar para comentarios)", 13 de junio de 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.cac.gov.cn/2019-06/13/c_1124613618.htm.

[27] Inside Privacy, traducción no oficial de Covington: Medidas de evaluación de la seguridad de la transferencia transfronteriza de información personal (versión preliminar para comentarios), 13 de junio de 2019, https://www.insideprivacy.com/wp-content/uploads/sites/51/2019/06/Measures-for-Security-Assessment-of-the-Cross-Border-Transfer-of-Personal-Information_bilingual.pdf, y New America, traducción: Nueva versión preliminar de normas sobre la transferencia transfronteriza de información personal fuera de China, "Medidas de evaluación de la seguridad de la transferencia saliente de información personal (versión preliminar para comentarios)", junio de 2019 https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.cac.gov.cn/2019-06/13/c_1124613618.htm.

[28] Orden del Consejo de Estado de la República Popular China n.º 745, del 30 de julio de 2021, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1, según traducción de DigiChina: https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept.

personal "de las personas físicas recibe protección legal; ninguna organización o persona puede infringir los derechos e intereses de información personal de las personas físicas". Esta ley "se aplica a las organizaciones y personas que gestionan actividades de tratamiento de información personal de personas físicas dentro de las fronteras de la República Popular China". "Cuando se presente una de las siguientes circunstancias en la gestión de actividades fuera de las fronteras de la República Popular China de tratamiento de información personal de personas físicas dentro de las fronteras de la República Popular China, esta Ley también se aplica" en los siguientes casos: (1) "Cuando el propósito sea proporcionar productos o servicios a personas físicas dentro de las fronteras"; (2) "Cuando se analicen o evalúen actividades de personas físicas dentro de las fronteras"; (3) "Otras circunstancias previstas en leyes o normas administrativas". La ley también define la información personal y lo que se incluye en su tratamiento: "La información personal es todo tipo de información registrada por medios electrónicos o de otro tipo relacionada con personas físicas identificadas o identificables, sin incluir la información después del tratamiento de anonimización. El tratamiento de información personal incluye la recopilación, el almacenamiento, el uso, el procesamiento, la transmisión, el suministro, la publicación, la supresión, etc. de la información personal".[29] (El texto completo de la ley se incluye en el Apéndice 5 del presente documento).

Conclusión

China está participando activamente en todos los debates relevantes relacionados con la cibernética en la ONU. Las contribuciones internacionales y nacionales de China tienen el potencial de afectar a la misión de la ICANN. La organización de la ICANN, a través de su Equipo de Participación Gubernamental, seguirá proporcionando información a la comunidad de la ICANN cuando dichas declaraciones o propuestas sean relevantes para la gobernanza técnica de Internet o para la misión de la ICANN.

[29] Ley de Protección de Información Personal de la República Popular China, (aprobada en la 30.ª reunión del Comité Permanente de la 13.ª Asamblea Popular Nacional el 20 de agosto de 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

Apéndice 1
Ley de Ciberseguridad de la República Popular China[30]
Aprobada el 6 de noviembre de 2016. Vigente a partir del 1 de junio de 2017.

1. Índice

Capítulo I: Disposiciones Generales
Artículo 1: Esta Ley se formula con el fin de: garantizar la ciberseguridad; proteger la soberanía del ciberespacio y la seguridad nacional, y los intereses sociales y públicos; proteger los derechos e intereses legítimos de los ciudadanos, las personas jurídicas y otras organizaciones; y promover el desarrollo saludable de la informatización de la economía y la sociedad.
Artículo 2: Esta Ley es aplicable a la construcción, la operación, el mantenimiento y la utilización de las redes, así como a la supervisión y gestión de la ciberseguridad en el territorio continental de la República Popular China.
Artículo 3: El Estado persiste en insistir por igual en la ciberseguridad y el desarrollo de la informatización, y cumple con los principios de uso activo, desarrollo científico, gestión conforme a la ley y garantía de la seguridad. El Estado avanza en la construcción de la infraestructura de red y la interconectividad, fomenta la innovación y la aplicación de la tecnología de red, apoya la formación de personal cualificado en ciberseguridad, establece un sistema completo para salvaguardar la ciberseguridad y aumenta la capacidad para proteger la ciberseguridad.
Artículo 4: El Estado formula y mejora continuamente la estrategia de ciberseguridad, aclara los requisitos fundamentales y los objetivos primordiales para garantizar la ciberseguridad, y propone políticas, tareas y procedimientos de ciberseguridad para los sectores clave.
Artículo 5: El Estado toma medidas para monitorear, prevenir y gestionar los riesgos y amenazas en materia de ciberseguridad que surgen tanto dentro como fuera del territorio continental de la República Popular China. El Estado protege la infraestructura crítica de información contra los ataques, las intrusiones, las interferencias y la destrucción; el Estado castiga las actividades cibernéticas ilegales y delictivas de acuerdo con la ley, preservando la seguridad y el orden del ciberespacio.

[30] NewAmerica, traducción: Ley de Ciberseguridad de la República Popular China (en vigencia a partir del 1 de junio de 2017), 29 de junio de 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

Artículo 6: El Estado aboga por una conducta en línea sincera, honesta, sana y civilizada; promueve la difusión de los valores socialistas fundamentales, adopta medidas para elevar la conciencia y el nivel de ciberseguridad de toda la sociedad, y formula un buen entorno para que toda la sociedad participe conjuntamente en el avance de la ciberseguridad.

Artículo 7: El Estado lleva a cabo activamente intercambios y cooperación internacional en los ámbitos de la gobernanza del ciberespacio, investigación y desarrollo de tecnologías de red, formulación de normas, lucha contra la ciberdelincuencia y la ilegalidad, y otros ámbitos similares; promueve la construcción de un ciberespacio pacífico, seguro, abierto y cooperativo, y el establecimiento de un sistema de gobernanza de Internet multilateral, democrático y transparente.

Artículo 8: Los departamentos de ciberseguridad e informatización del Estado son responsables de planificar y coordinar exhaustivamente las iniciativas en materia de ciberseguridad y las iniciativas de supervisión y gestión relacionadas. Los departamentos del Consejo de Estado para las telecomunicaciones, la seguridad pública y otros órganos pertinentes, son responsables de las iniciativas de protección, supervisión y gestión de la ciberseguridad en el ámbito de sus responsabilidades, de acuerdo con las disposiciones de esta Ley y las leyes y las normas administrativas pertinentes.

Las obligaciones de protección, supervisión y gestión de la ciberseguridad de los departamentos pertinentes de los gobiernos populares a nivel de condado o superior se determinarán mediante las normativas nacionales pertinentes.

Artículo 9: Los operadores de redes que realicen actividades comerciales y de servicios deben cumplir con las leyes y las normas administrativas, respetar la moral social, cumplir con la ética comercial, ser honestos y confiables, cumplir con las obligaciones de protección de la ciberseguridad, aceptar la supervisión del gobierno y del público, y asumir la responsabilidad social.

Artículo 10: La construcción y el funcionamiento de las redes, o la prestación de servicios a través de las mismas, se realizará: de acuerdo con las disposiciones de las leyes y las normas administrativas, y con los requisitos obligatorios de las normas nacionales; adoptando las medidas técnicas y otras medidas necesarias para proteger la ciberseguridad y la estabilidad operativa; respondiendo eficazmente a los incidentes de ciberseguridad; previniendo los ciberdelitos y las actividades ilícitas; y preservando la integridad, el secreto y la capacidad de uso de los datos en línea.

Artículo 11: Las organizaciones pertinentes de la industria de Internet, de acuerdo con sus Escrituras de Constitución, reforzarán la autodisciplina de la industria, formularán normas de comportamiento en materia de ciberseguridad, guiarán a sus miembros en el fortalecimiento de la protección de la ciberseguridad conforme a la ley, elevarán el nivel de protección de la ciberseguridad y estimularán el desarrollo saludable de la industria.

Artículo 12: El Estado protege los derechos de los ciudadanos, las personas jurídicas y otras organizaciones para utilizar las redes de acuerdo con la ley; promueve el acceso generalizado a las redes, eleva el nivel de los servicios de red, proporciona servicios de red seguros y convenientes para la sociedad y garantiza la circulación legal, ordenada y libre de la información de la red.

Toda persona y organización que utilice las redes deberá cumplir la Constitución y las leyes, preservar el orden público y respetar la moral social; no debe poner en peligro la ciberseguridad y no debe utilizar Internet para realizar actividades que pongan en peligro la seguridad nacional, el honor nacional y los intereses nacionales; no deben incitar a la subversión de la soberanía nacional, al derrocamiento del sistema socialista, al separatismo, a la ruptura de la unidad nacional, a la apología del terrorismo o del extremismo, a la apología del odio étnico y

de la discriminación étnica, a la difusión de información violenta, obscena o sexual, a la creación o difusión de información falsa que perturbe el orden económico o social, o de información que atente contra la reputación, la intimidad, la propiedad intelectual u otros derechos e intereses legítimos de terceros, y otros actos similares.
Artículo 13: El Estado fomenta la investigación y el desarrollo de productos y servicios de red que favorezcan la educación saludable de los menores; el Estado sancionará legalmente el uso de las redes para realizar actividades que pongan en peligro el bienestar psicológico y físico de los menores; y el Estado proporcionará un entorno de red seguro y saludable para los menores.
Artículo 14: Todas las personas y organizaciones tienen derecho a denunciar conductas que pongan en peligro la ciberseguridad a los departamentos de ciberseguridad e informatización, telecomunicaciones y seguridad pública, entre otros. Los departamentos que reciban las denuncias las tramitarán sin demora de acuerdo con la ley; cuando los asuntos no sean competencia de ese departamento, los trasladarán sin demora al departamento facultado para tratarlos.
Los departamentos pertinentes preservarán la confidencialidad de la información de los informantes y protegerán los derechos e intereses legítimos de los informantes.

Capítulo II: Apoyo y promoción de la ciberseguridad

Artículo 15: El Estado establece y mejora un sistema de estándares de ciberseguridad. Los departamentos administrativos de estandarización del Consejo de Estado y otros departamentos pertinentes del Consejo de Estado, en base a sus responsabilidades individuales, organizarán la formulación y la revisión oportuna de los estándares nacionales e industriales pertinentes para la gestión de la ciberseguridad, así como para la seguridad de los productos, servicios y operaciones de la red.
El Estado apoya a las empresas, las instituciones de investigación, las escuelas de enseñanza superior y las organizaciones industriales relacionadas con las redes para que participen en la formulación de estándares nacionales e industriales en materia de ciberseguridad.
Artículo 16: El Consejo de Estado y los gobiernos populares de las provincias, las regiones autónomas y los municipios gobernados directamente deberán: realizar una planificación exhaustiva; ampliar las inversiones; apoyar las industrias y los programas de tecnología de la ciberseguridad clave; apoyar la investigación y el desarrollo, la aplicación y la divulgación de la tecnología de ciberseguridad; promover productos y servicios de red seguros y confiables; proteger los derechos de propiedad intelectual de las tecnologías de red; y apoyar a las instituciones de investigación y desarrollo, las escuelas de enseñanza superior, etc., para que participen en los programas estatales de innovación en tecnología de la ciberseguridad.
Artículo 17: El Estado impulsa el establecimiento de sistemas de servicios socializados para la ciberseguridad, alentando a las empresas e instituciones pertinentes a llevar a cabo certificaciones de ciberseguridad, pruebas, evaluación de riesgos y otros servicios de seguridad de este tipo.
Artículo 18: El Estado fomenta el desarrollo de tecnologías de protección y utilización de la seguridad de los datos de la red, impulsando la apertura de los recursos de datos públicos y promoviendo la innovación técnica y el desarrollo económico y social.
El Estado apoya los métodos innovadores de gestión de la ciberseguridad, utilizando las nuevas tecnologías de red para mejorar el nivel de protección de la ciberseguridad.
Artículo 19: Todos los niveles de los gobiernos populares y sus departamentos pertinentes organizarán y llevarán a cabo periódicamente la publicidad y la educación en materia de ciberseguridad, y orientarán y estimularán a las unidades pertinentes para que lleven a cabo adecuadamente la labor de publicidad y educación en materia de ciberseguridad.
Los medios de comunicación llevarán a cabo actividades de publicidad y educación en materia de ciberseguridad dirigidas al público.

Artículo 20: El Estado apoya a las empresas y a las instituciones de educación o formación, como las escuelas de enseñanza superior y las escuelas de formación profesional, para que lleven a cabo la formación y la capacitación relacionadas con la ciberseguridad, y emplea múltiples métodos para formar personal cualificado en materia de ciberseguridad y promover la interacción de los profesionales de la ciberseguridad.

Capítulo III: Seguridad de operaciones de redes

Sección 1: Disposiciones ordinarias

Artículo 21: El Estado implementa un sistema de protección multinivel de ciberseguridad [MLPS]. Los operadores de redes realizarán las siguientes tareas de protección de la seguridad de acuerdo con los requisitos del sistema de protección multinivel de ciberseguridad para garantizar que la red no tenga ninguna interferencia, daño o acceso no autorizado, y para evitar la fuga, el robo o la falsificación de datos de la red:

(1) Formular sistemas de gestión de la seguridad interna y normas de funcionamiento, determinar las personas responsables de la ciberseguridad e implementar la responsabilidad de protección de la ciberseguridad.

(2) Adoptar medidas técnicas para prevenir virus informáticos, ciberataques, intrusiones en la red y otras acciones que pongan en peligro la ciberseguridad.

(3) Adoptar medidas técnicas para monitorear y registrar los estados operativos de la red y los incidentes de ciberseguridad, y seguir las disposiciones para almacenar los registros de la red durante al menos seis meses.

(4) Adoptar medidas como la clasificación de los datos, la realización de copias de seguridad de los datos importantes y el cifrado.

(5) Otras obligaciones previstas por la ley o las normas administrativas.

Artículo 22: Los productos y servicios de red deberán cumplir con los requisitos nacionales y obligatorios pertinentes. Los proveedores de productos y servicios de red no deben instalar programas maliciosos; cuando descubran que sus productos y servicios tienen vulnerabilidades o fallos de seguridad, adoptarán inmediatamente medidas correctivas, y seguirán las disposiciones para informar rápidamente a los usuarios e informar a los departamentos competentes.

Los proveedores de productos y servicios de red proporcionarán mantenimiento de seguridad para sus productos y servicios, y no deberán poner fin a la prestación de mantenimiento de seguridad durante los plazos o períodos acordados con los clientes.

Si un producto o servicio de red tiene la función de recopilar información del usuario, su proveedor deberá indicarlo claramente y obtener el consentimiento del usuario; y si esto implica información personal del usuario, el proveedor también deberá cumplir con las disposiciones de esta ley y las leyes y las normas administrativas pertinentes sobre la protección de la información personal.

Artículo 23: Los equipos de red críticos y los productos de ciberseguridad especializados deberán seguir las normas nacionales y los requisitos obligatorios, y estar certificados en materia de seguridad por un establecimiento cualificado o cumplir los requisitos de una inspección de seguridad, antes de ser vendidos o suministrados. Los departamentos estatales de ciberseguridad e informatización, junto con los departamentos pertinentes del Consejo de Estado, formularán y publicarán un catálogo de equipos críticos de red y productos especializados de ciberseguridad, y promoverán el reconocimiento recíproco de las certificaciones de seguridad y los resultados de las inspecciones de seguridad para evitar la duplicación de certificaciones e inspecciones.

Artículo 24: Los operadores de redes que gestionen el acceso a la red y los servicios de registración de nombres de dominio para los usuarios, que gestionen el acceso a la red de

telefonía fija o móvil, o que proporcionen a los usuarios servicios de publicación de información o de mensajería instantánea, exigirán a los usuarios que proporcionen información sobre su identidad real cuando firmen acuerdos con los usuarios o confirmen la prestación de servicios. En caso de que los usuarios no proporcionen información sobre su identidad real, los operadores de redes no deben prestarles los servicios correspondientes.
El Estado aplica una estrategia de credibilidad de la identidad en la red y apoya la investigación y el desarrollo de tecnologías de autenticación de la identidad electrónica seguras y convenientes, promoviendo la aceptación recíproca entre los diferentes métodos de autenticación de identidad electrónica.
Artículo 25: Los operadores de redes formularán planes de respuesta de emergencia para incidentes de ciberseguridad y abordarán inmediatamente las vulnerabilidades del sistema, los virus informáticos, los ciberataques, las intrusiones en la red y otros riesgos de ciberseguridad de este tipo. Cuando se produzcan incidentes de ciberseguridad, los operadores de redes deberán poner en marcha inmediatamente un plan de respuesta ante emergencias, adoptar las medidas correctivas correspondientes e informar a los departamentos competentes de acuerdo con las disposiciones pertinentes.
Artículo 26: Aquellos que lleven a cabo certificaciones de ciberseguridad, pruebas, evaluaciones de riesgo u otras actividades similares, o que publiquen información sobre ciberseguridad, como vulnerabilidades del sistema, virus informáticos, ataques a la red o incursiones en la red, deberán cumplir con las disposiciones nacionales pertinentes.
Artículo 27: Los individuos y las organizaciones no deben realizar intrusiones ilegales en las redes de otras partes, perturbar el funcionamiento normal de las redes de otras partes, o robar datos de la red o participar en otras actividades que pongan en peligro la ciberseguridad; no deben proporcionar programas, o herramientas especialmente utilizadas en las intrusiones en la red, que perturben el funcionamiento normal de la red y las medidas de protección, roben datos de la red o realicen otros actos que pongan en peligro la ciberseguridad; y cuando tengan conocimiento claramente de que otras personas realizarán acciones que pongan en peligro la ciberseguridad, no deben proporcionar ayuda, como apoyo técnico, publicidad y promoción, o pago de gastos.
Artículo 28: Los operadores de redes deberán prestar apoyo técnico y asistencia a los órganos de seguridad pública y a los órganos de seguridad nacional que estén protegiendo la seguridad nacional e investigando actividades delictivas de acuerdo con la ley.
Artículo 29: El Estado apoya la cooperación entre los operadores de redes en ámbitos como la recopilación, el análisis, la notificación y el tratamiento de emergencia de la información sobre ciberseguridad, aumentando la capacidad de protección de la seguridad de los operadores de redes.
Las organizaciones industriales pertinentes deben establecer y completar los mecanismos de estandarización y coordinación de la ciberseguridad para su industria, fortalecer su análisis y evaluación de la ciberseguridad, y realizar periódicamente advertencias de riesgo, apoyo y coordinación para los miembros en respuesta a los riesgos de ciberseguridad.
Artículo 30: La información obtenida por los departamentos de ciberseguridad e informatización y los departamentos pertinentes que desempeñan funciones de protección de la ciberseguridad solo puede utilizarse en la medida necesaria para la protección de la ciberseguridad, y no debe utilizarse de otra manera.

Sección 2: Seguridad de operaciones para la infraestructura crítica de información
Artículo 31: El Estado implementa la protección clave sobre la base del sistema de protección multinivel de la ciberseguridad para los servicios públicos de comunicación e información, la energía, el tráfico, los recursos hídricos, las finanzas, el servicio público, el gobierno electrónico y otras infraestructuras críticas de información que, si se destruyen, sufren la pérdida de una

función o experimentan una fuga de datos, podrían poner en grave peligro la seguridad nacional, el bienestar nacional, el sustento de la población o el interés público. El Consejo de Estado formulará el alcance específico y las medidas de protección de la seguridad de las infraestructuras críticas de información.
El Estado recomienda a los operadores de redes ajenas a los sistemas de infraestructuras críticas de información [designados] que participen voluntariamente en el sistema de protección de infraestructuras críticas de información.
Artículo 32: De acuerdo con los deberes y la división del trabajo proporcionados por el Consejo de Estado, los departamentos responsables del trabajo de protección de la seguridad de la infraestructura crítica de información deben compilar y organizar por separado los planes de implementación de la seguridad para la infraestructura crítica de información de su industria o sector, y guiar y supervisar los esfuerzos de protección de la seguridad para las operaciones de la infraestructura crítica de información.
Artículo 33: Los responsables de la construcción de infraestructuras críticas de información deben garantizar que éstas tengan la capacidad de apoyar la estabilidad comercial y las operaciones sostenidas, y asegurar la planificación sincrónica, el establecimiento sincrónico y la aplicación sincrónica de las medidas técnicas de seguridad.
Artículo 34: Además de lo dispuesto en el Artículo 21 de la presente Ley, los operadores de infraestructuras críticas de información también deberán realizar las siguientes tareas de protección de la seguridad:
(1) Establecer órganos especializados de gestión de la seguridad y personas responsables de la gestión de la seguridad, y realizar comprobaciones de los antecedentes de seguridad de las personas responsables y del personal en puestos críticos.
(2) Llevar a cabo periódicamente la educación en ciberseguridad, la formación técnica y la evaluación de las habilidades de los empleados.
(3) Realizar copias de seguridad de recuperación ante desastres de los sistemas y bases de datos importantes.
(4) Formular planes de respuesta ante emergencias para incidentes de ciberseguridad y organizar periódicamente simulacros.
(5) Otras obligaciones previstas por la ley o las normas administrativas.
Artículo 35: Los operadores de infraestructuras críticas de información que adquieran productos y servicios de red que puedan afectar a la seguridad nacional deberán someterse a una revisión de seguridad nacional organizada por los departamentos de ciberseguridad e informatización del Estado y los departamentos pertinentes del Consejo de Estado.

Artículo 36: Los operadores de infraestructuras críticas de información que adquieran productos y servicios de red deberán seguir las disposiciones pertinentes y firmar un acuerdo de seguridad y confidencialidad con el proveedor, en el que se aclaren las obligaciones y responsabilidades en materia de seguridad y confidencialidad.
Artículo 37: Los operadores de infraestructuras críticas de información que recojan o produzcan información personal o datos importantes durante sus operaciones dentro del territorio continental de la República Popular China, deberán almacenarlos dentro de la región continental de China. Cuando, debido a los requisitos de la empresa, sea realmente necesario proporcionarla fuera de la región continental, seguirán las medidas formuladas conjuntamente por los departamentos de ciberseguridad e informatización del Estado y los departamentos pertinentes del Consejo de Estado para llevar a cabo una evaluación de la seguridad; cuando las leyes y las normas administrativas lo dispongan de otro modo, seguirán dichas disposiciones.
Artículo 38: Al menos una vez al año, los operadores de infraestructuras críticas de información deberán realizar una inspección y evaluación de la seguridad de sus redes y de los

riesgos que puedan existir, ya sea por su cuenta o mediante la contratación de una organización de servicios de ciberseguridad; los operadores de infraestructura crítica de información (CII) deberán presentar un informe de ciberseguridad sobre las circunstancias de la inspección y la evaluación, así como las medidas de mejora, que se enviará al departamento pertinente responsable de los esfuerzos de protección de la seguridad de las infraestructuras críticas de información.

Artículo 39: Los departamentos de ciberseguridad e informatización del Estado coordinarán a los departamentos pertinentes en el empleo de las siguientes medidas para la protección de la seguridad de las infraestructuras críticas de información:

(1) Llevar a cabo pruebas puntuales de los riesgos de seguridad de las infraestructuras de información críticas, proponer medidas de mejora y, cuando sea necesario, pueden contratar una organización de servicios de ciberseguridad para llevar a cabo las pruebas y la evaluación de los riesgos de ciberseguridad.

(2) Organizar periódicamente a los operadores de infraestructuras críticas de información para que lleven a cabo simulacros de respuesta ante emergencias en materia de ciberseguridad, aumentando el nivel, la coordinación y la capacidad de respuesta a los incidentes de ciberseguridad.

(3) Promover el intercambio de información sobre ciberseguridad entre los departamentos pertinentes, los operadores de infraestructuras de información críticas y también las instituciones de investigación y las organizaciones de servicios de ciberseguridad pertinentes.

(4) Proporcionar apoyo y asistencia técnica para la gestión y recuperación de emergencias de ciberseguridad, etc.

Capítulo IV: Seguridad de la información de redes

Artículo 40: Los operadores de redes mantendrán estrictamente la confidencialidad de la información de los usuarios que recopilen, y establecerán y completarán sistemas de protección de la información de los usuarios.

Artículo 41: Los operadores de redes que recopilen y utilicen información personal deberán respetar los principios de legalidad, corrección y necesidad; publicarán normas de recopilación y uso, indicando explícitamente los fines, los medios y el alcance de la recopilación o el uso de la información, y deberán obtener el consentimiento de las personas cuyos datos se recopilen. Los operadores de redes no deben recopilar información personal que no esté relacionada con los servicios que prestan; no deben infringir las disposiciones de las leyes, los reglamentos administrativos o los acuerdos entre las partes para recopilar o utilizar la información personal; y seguirán las disposiciones de las leyes, las normas administrativas y los acuerdos con los usuarios para procesar la información personal que hayan almacenado.

Artículo 42: Los operadores de redes no deben revelar, manipular ni destruir la información personal que recopilan; y, sin el consentimiento de la persona cuya información fue recopilada, no deben proporcionar información personal a terceros. Sin embargo, esto es así con la excepción de que la información puede ser proporcionada si después del procesamiento no hay manera de identificar a un individuo específico, y no se puede recuperar la identidad.

Los operadores de redes adoptarán las medidas técnicas y otras medidas necesarias para garantizar la seguridad de la información personal que recopilen y evitar que la información personal se filtre, se destruya o se pierda. Cuando se produzca, o pueda haberse producido, la filtración, destrucción o pérdida de información personal, se adoptarán inmediatamente medidas correctivas y se seguirán las disposiciones para informar rápidamente a los usuarios y presentar un informe a los departamentos competentes de acuerdo con la normativa.

Artículo 43: Cuando las personas descubran que los operadores de redes han infringido las disposiciones legales, administrativas o los acuerdos entre las partes para recopilar o utilizar su información personal, tendrán derecho a exigir que los operadores de redes eliminen su

información personal; cuando descubran que la información personal recopilada o almacenada por los operadores de redes tiene errores, tendrán derecho a exigir que los operadores de redes la corrijan. Los operadores de redes deberán emplear medidas para la eliminación y la corrección.

Artículo 44: Los individuos u organizaciones no deben robar ni utilizar otros métodos ilegales para adquirir información personal, y no deben vender ni proporcionar ilegalmente la información personal a otros.

Artículo 45: Los departamentos que tienen legalmente funciones de supervisión y gestión de la ciberseguridad, así como su personal, deben mantener de manera estrictamente confidencial la información personal, la información privada y los secretos comerciales de los que tengan conocimiento en el desempeño de sus funciones, y no deben filtrarlos, venderlos ni facilitarlos ilícitamente a terceros.

Artículo 46: Todas las personas y organizaciones serán responsables del uso que hagan de los sitios web y no deberán crear sitios web o grupos de comunicación para utilizarlos en la comisión de fraudes, la difusión de métodos delictivos, la creación o venta de artículos prohibidos o controlados, u otras actividades ilícitas, y los sitios web no deberán ser explotados para publicar información relacionada con la comisión de fraudes, la creación o venta de artículos prohibidos.

Artículo 47: Los operadores de redes reforzarán la gestión de la información publicada por los usuarios y, al descubrir información que la ley o las normas administrativas prohíben publicar o transmitir, detendrán inmediatamente la transmisión de dicha información, emplearán medidas de tratamiento como la supresión de la información, evitarán que la información se difunda, guardarán los registros pertinentes e informarán a los departamentos competentes correspondientes.

Artículo 48: La información electrónica enviada, o el software de aplicación proporcionado por cualquier persona u organización, no deben instalar programas maliciosos, y no debe contener información que las leyes y las normas administrativas prohíban publicar o transmitir.

Los proveedores de servicios de distribución de información electrónica y los proveedores de servicios de descarga de software de aplicación deberán llevar a cabo tareas de gestión de la seguridad; cuando tengan conocimiento de que sus usuarios han incurrido en las conductas previstas en el párrafo anterior, deberán: emplear medidas como la interrupción de la prestación de servicios y la eliminación de información o programas maliciosos; almacenar los registros pertinentes; e informar a los departamentos competentes pertinentes.

Artículo 49: Los operadores de redes establecerán sistemas de reclamación y notificación en materia de seguridad de la información de la red, divulgarán públicamente información como los métodos para presentar reclamos o denuncias, y aceptarán y tratarán rápidamente los reclamos y las denuncias relacionados con la seguridad de la información de la red.

Los operadores de redes deberán cooperar con los departamentos de ciberseguridad e informatización y los departamentos pertinentes para llevar a cabo la supervisión y las inspecciones de acuerdo con la ley.

Artículo 50: Los departamentos de ciberseguridad e informatización del Estado y los departamentos pertinentes llevarán a cabo las responsabilidades de supervisión y gestión de la seguridad de la información de la red de acuerdo con la ley; y cuando descubran la publicación o transmisión de información prohibida por las leyes o normas administrativas, solicitarán a los operadores de la red que detengan la transmisión, que empleen medidas de disposición como la eliminación y que almacenen los registros pertinentes; en el caso de la información descrita anteriormente que proceda de fuera de la región continental de la República Popular China, notificarán a la organización pertinente que adopte medidas técnicas y otras medidas necesarias para bloquear la transmisión.

Capítulo V: Monitoreo, alerta temprana y respuesta ante emergencias

Artículo 51: El Estado establecerá un sistema de monitoreo, alerta temprana y comunicación de la información en materia de ciberseguridad. Los departamentos de ciberseguridad e informatización del Estado realizarán una coordinación general de los departamentos pertinentes para reforzar los esfuerzos de recopilación, análisis y comunicación de la información sobre ciberseguridad, y seguirán la normativa para la publicación unificada de la información de monitoreo y alerta temprana sobre ciberseguridad.

Artículo 52: Los departamentos responsables de los esfuerzos de protección de la infraestructura crítica de información establecerán y completarán los sistemas de monitoreo, alerta temprana y notificación de información en materia de ciberseguridad para su respectiva industria o sector, y comunicarán la información de alerta temprana y monitoreo de la ciberseguridad de acuerdo con la normativa.

Artículo 53: Los departamentos de ciberseguridad e informatización del Estado se coordinarán con los departamentos pertinentes para establecer y completar mecanismos de evaluación de riesgos de ciberseguridad y esfuerzos de respuesta ante emergencias, formularán planes de respuesta de emergencia a incidentes de ciberseguridad y organizarán periódicamente simulacros.

Los departamentos responsables de las iniciativas de protección de la infraestructura crítica de información formularán planes de respuesta de emergencia a incidentes de ciberseguridad para su respectiva industria o sector, y organizarán periódicamente simulacros.

Los planes de respuesta de emergencia a incidentes de ciberseguridad deberán clasificar los incidentes de ciberseguridad sobre la base de factores como el grado de daño después de que se produzca el incidente y el alcance del impacto, y proporcionar las correspondientes medidas de gestión de respuestas ante emergencias.

Artículo 54: Cuando el riesgo de incidentes de ciberseguridad aumente, los departamentos pertinentes de los gobiernos populares a nivel provincial y superior seguirán el alcance de la autoridad y los procedimientos previstos, y emplearán las siguientes medidas sobre la base de las características del riesgo de ciberseguridad y el daño que podría causar:

(1) Exigir que los departamentos, instituciones y personal pertinentes recopilen y comuniquen rápidamente la información pertinente, y reforzar el monitoreo de la aparición de riesgos de ciberseguridad.

(2) Organizar a los departamentos, instituciones y personal especializado pertinentes para que lleven a cabo el análisis y la evaluación de la información sobre el riesgo de ciberseguridad, y prevean la probabilidad de que se produzca un incidente, el alcance del impacto y el nivel de daños.

(3) Emitir advertencias de riesgo de ciberseguridad al público, y publicar medidas para evitar o reducir los daños.

Artículo 55: Cuando se produzca un incidente de ciberseguridad, se pondrá en marcha inmediatamente el plan de respuesta de emergencia a incidentes de ciberseguridad, se realizará una evaluación y valoración del incidente de ciberseguridad, se solicitará a los operadores de redes que adopten las medidas técnicas y otras necesarias, se eliminarán los posibles riesgos de seguridad, se evitará que la amenaza se expanda y se publicarán rápidamente las advertencias pertinentes para el público.

Artículo 56: Cuando, en el ejercicio de las funciones de supervisión y gestión de la ciberseguridad, los departamentos pertinentes de los gobiernos populares a nivel provincial o superior descubran que las redes presentan un riesgo de seguridad relativamente grande o la ocurrencia de un incidente de seguridad, podrán llamar al representante legal o a la parte responsable del operador de dicha red para realizar entrevistas de acuerdo con el alcance de la autoridad y los procedimientos previstos. Los operadores de redes deberán seguir los requisitos para emplear los procedimientos, realizar correcciones y eliminar los peligros ocultos.

Artículo 57: Cuando se produzcan emergencias repentinas o accidentes de seguridad de la producción como resultado de incidentes de ciberseguridad, se tratarán de acuerdo con las disposiciones de la "Ley de Respuesta ante Emergencias de la República Popular China", la "Ley de Seguridad de la Producción de la República Popular China" y otras leyes y normas administrativas pertinentes.
Artículo 58: Para cumplir con la necesidad de proteger la seguridad nacional y el orden público social, y para responder a los requisitos de incidentes de seguridad importantes dentro de la sociedad, es posible, según lo estipulado o aprobado por el Consejo de Estado, tomar medidas temporales con respecto a las comunicaciones de red en una región especialmente designada, como la limitación de dichas comunicaciones.

Capítulo VI: Responsabilidad jurídica

Artículo 59: Cuando los operadores de redes no cumplan con las obligaciones de protección de la ciberseguridad previstas en los Artículos 21 y 25 de la presente Ley, los departamentos competentes ordenarán correcciones y realizarán advertencias; cuando se rechacen las correcciones o se produzcan perjuicios a la ciberseguridad u otras consecuencias de este tipo, se impondrá una multa de entre RMB 10 000 y 100 000; y el personal directivo directamente responsable será multado con entre RMB 5000 y 50 000.
Cuando los operadores de infraestructuras críticas de información no cumplan con las obligaciones de protección de la ciberseguridad previstas en los Artículos 33, 34, 36 y 38 de la presente Ley, los departamentos competentes ordenarán correcciones y realizarán advertencias; cuando se rechacen las correcciones o se produzcan perjuicios a la ciberseguridad u otras consecuencias de este tipo, se impondrá una multa de entre RMB 100 000 y 1 000 000; y el personal directivo directamente responsable será sancionado con una multa de entre RMB 10 000 y 100 000.
Artículo 60: Cuando se infrinja el Artículo 22, Párrafos 1 y 2, o el Artículo 48, Párrafo 1, de la presente Ley por alguna de las siguientes conductas, los departamentos competentes pertinentes ordenarán correcciones y realizarán advertencias; en caso de que se rechacen las correcciones o se cause un daño a la ciberseguridad u otras consecuencias, se impondrá una multa de entre RMB 50 000 y 500 000; y los responsables directos recibirán una multa de entre RMB 10 000 y 100 000:
(1) Instalar programas maliciosos.
(2) No tomar inmediatamente medidas para remediar los fallos de seguridad o las vulnerabilidades que existen en los productos o servicios, o no informar a los usuarios e informar a los departamentos competentes de acuerdo con la normativa.
(3) Poner fin sin autorización a la prestación de mantenimiento de seguridad de sus productos o servicios.
Artículo 61: A los operadores de redes que infrinjan el Párrafo 1 del Artículo 24 de la presente Ley al no exigir a los usuarios que faciliten información sobre su identidad real o al prestar servicios pertinentes a usuarios que no faciliten información sobre su identidad real, se les ordena realizar correcciones por el departamento competente correspondiente; cuando se rechacen las correcciones o las circunstancias sean graves, se impondrá una multa de entre RMB 50 000 y 500 000, y el departamento competente pertinente podrá ordenar la suspensión temporal de las operaciones, la suspensión de la actividad para realizar correcciones, el cierre de los sitios web, la cancelación de los permisos de operación pertinentes o la cancelación de las licencias comerciales; las personas que estén directamente a cargo y el resto del personal directamente responsable serán multados por un valor entre RMB 10 000 y 100 000.
Artículo 62: Cuando se infrinja el Artículo 26 de esta Ley al realizar certificaciones, pruebas o evaluaciones de riesgo en materia de ciberseguridad, o al publicar información sobre ciberseguridad, como vulnerabilidades del sistema, virus informáticos, ciberataques o

incursiones en la red, se ordenarán correcciones y se hará una advertencia; cuando se denieguen las correcciones o las circunstancias sean graves, se impondrá una multa de entre RMB 10 000 y 100 000, y el departamento competente pertinente podrá ordenar la suspensión temporal de las operaciones, la suspensión de la actividad comercial para las correcciones, el cierre de los sitios web, la cancelación de los permisos de operaciones pertinentes o la cancelación de las licencias comerciales; las personas que estén directamente a cargo y otro personal directamente responsable serán multados por un valor entre RMB 5000 y 50 000.

Artículo 63: Cuando se infrinja el Artículo 27 de la presente Ley al realizar actividades que perjudiquen la ciberseguridad, o al proporcionar software o herramientas especializadas utilizadas en la realización de actividades que perjudiquen la ciberseguridad, o al proporcionar a otros que realicen actividades que perjudiquen la ciberseguridad asistencia como apoyo técnico, publicidad y promociones, o pago de gastos, y cuando esto no constituya un delito, los organismos de seguridad pública confiscarán las ganancias ilícitas e impondrán hasta 5 días de detención, y podrán imponer una multa de entre RMB 50 000 y 500 000; y cuando las circunstancias sean graves, impondrán entre 5 y 15 días de detención, y podrán imponer una multa de entre RMB 100 000 y 1 000 000.

Cuando las unidades hayan incurrido en la conducta del párrafo anterior, los organismos de seguridad pública confiscarán las ganancias ilícitas e impondrán una multa de entre RMB 100 000 y 1 000 000, y los responsables directos y otro personal directamente responsable serán multados de acuerdo con el párrafo anterior.

Cuando se infrinja el Artículo 27 de la presente Ley, las personas que reciban sanciones administrativas de seguridad pública no deberán dedicarse a la gestión de la ciberseguridad ni a los puestos clave de operaciones de red durante 5 años; las que reciban sanciones penales estarán sujetas a la prohibición de por vida de dedicarse a la gestión de la ciberseguridad y a los puestos clave de operaciones de red.

Artículo 64: Los operadores de redes y los proveedores de productos o servicios de red que infrinjan el Artículo 22, Párrafo 3, o los Artículos 41-43 de esta Ley, infringiendo la información personal que está protegida conforme a la ley, recibirán una orden de corrección por parte del departamento competente pertinente y podrán, de forma independiente o simultánea, recibir advertencias, ser objeto de confiscación de las ganancias ilícitas y/o recibir una multa de entre 1 y 10 veces el importe de las ganancias ilícitas; cuando no haya ganancias ilícitas, la multa será de hasta RMB 1 000 000, y se impondrá una multa de entre RMB 10 000 y 100 000 a los responsables directos y al resto del personal directamente responsable; cuando las circunstancias sean graves, el departamento competente pertinente podrá ordenar la suspensión temporal de las operaciones, la suspensión de la actividad para realizar correcciones, el cierre de los sitios web, la cancelación de los permisos de operaciones pertinentes o la cancelación de las licencias comerciales.

Cuando se infrinja el artículo 44 de esta Ley al robar o utilizar otros medios ilegales para obtener, vender ilegalmente o proporcionar ilegalmente a otros información personal, y esto no constituya un delito, los organismos de seguridad pública confiscarán las ganancias ilícitas e impondrán una multa de entre 1 y 10 veces el importe de las ganancias ilícitas, y cuando no haya ganancias ilícitas, impondrán una multa de hasta RMB 1 000 000.

Artículo 65: Cuando los operadores de infraestructuras críticas de información infrinjan el Artículo 35 de la presente Ley utilizando productos o servicios de red que no hayan sido sometidos a inspecciones de seguridad o que no hayan superado las inspecciones de seguridad, el departamento competente pertinente ordenará el cese del uso e impondrá una multa de entre 1 y 10 veces el precio de compra; las personas que estén directamente a cargo y otro personal directamente responsable serán multados con entre RMB 10 000 y 100 000.

Artículo 66: En caso de que los operadores de infraestructuras críticas de información infrinjan el Artículo 37 de la presente Ley almacenando datos de red fuera del territorio continental, o

proporcionando datos de red a quienes se encuentran fuera del territorio continental, el departamento competente pertinente: ordenará medidas correctivas, realizará una advertencia, confiscará las ganancias ilícitas e impondrá multas de entre RMB 50 000 y 500 000; y podrá ordenar la suspensión temporal de las operaciones, la suspensión de las actividades para la adopción de medidas correctivas, el cierre de los sitios web, la revocación de los permisos de operaciones pertinentes o la cancelación de las licencias comerciales. Los responsables directos y el resto del personal directamente responsable serán sancionados con una multa de entre RMB 10 000 y 100 000.

Artículo 67: Cuando se infrinja el Artículo 46 de esta Ley estableciendo un sitio web o un grupo de comunicaciones utilizado para la comisión de actividades ilegales o delictivas, o se utilice la red para publicar información relacionada con la comisión de actividades ilegales o delictivas, pero no se haya cometido un delito, los organismos de seguridad pública impondrán hasta 5 días de detención y podrán imponer una multa de entre RMB 10 000 y 15 000; y cuando las circunstancias sean graves, podrán imponer entre 5 y 15 días de detención, y podrán imponer una multa de entre RMB 50 000 y 500 000. También pueden cerrar sitios web y grupos de comunicación utilizados para actividades ilegales o delictivas.

Cuando las unidades hayan incurrido en las conductas contempladas en el párrafo anterior, los organismos de seguridad pública impondrán una multa de entre RMB 100 000 y 500 000, y los principales gestores responsables y otro personal directamente responsable serán multados de acuerdo con el párrafo anterior.

Artículo 68: En caso de que los operadores de redes infrinjan el Artículo 47 de la presente Ley al no detener la transmisión de información cuya transmisión y publicación estén prohibidas por las leyes o normas administrativas, al no emplear medidas de disposición tales como la supresión o al no conservar los registros pertinentes, el departamento competente pertinente ordenará la corrección, hará una advertencia y confiscará las ganancias ilícitas; cuando se rechace la corrección o las circunstancias sean graves, se impondrán multas por un valor de entre RMB 100 000 y 500 000, y se podrá ordenar la suspensión temporal de las operaciones, la suspensión de la actividad para llevar a cabo la corrección, el cierre de los sitios web, la cancelación de los permisos de operaciones pertinentes o la cancelación de las licencias comerciales; y se impondrán multas por valores de entre RMB 10 000 y 100 000 a los responsables directos y a otro personal directamente responsable.

Cuando los proveedores de servicios de información electrónica y los proveedores de servicios de descarga de software de aplicación no cumplan con sus deberes de gestión de la seguridad previstos en el Párrafo 2 del Artículo 48 de la presente Ley, la sanción se ajustará a lo dispuesto en el apartado anterior.

Artículo 69: Los operadores de redes que infrinjan las disposiciones de la presente Ley y que presenten alguna de las siguientes conductas, recibirán la orden de realizar correcciones por parte de los departamentos competentes pertinentes; en caso de que las correcciones se rechacen o las circunstancias sean graves, se impondrá una multa de entre RMB 50 000 y 500 000, y el personal de gestión directamente responsable y otro personal directamente responsable recibirá una multa de entre RMB 10 000 y 100 000:

(1) No seguir los requisitos de los departamentos pertinentes para adoptar medidas de disposición, como dejar de difundir o borrar información cuya publicación o difusión está prohibida por las leyes o normas administrativas.

(2) Negarse u obstruir la actuación de los departamentos competentes en su supervisión e inspección legales.

(3) Negarse a prestar apoyo y asistencia técnica a los órganos de seguridad pública y a los órganos de seguridad del Estado.

Artículo 70: La publicación o transmisión de información prohibida por el Artículo 12, Párrafo 2, de esta Ley o por otras leyes o normas administrativas será sancionada de acuerdo con las disposiciones de las leyes y normas administrativas pertinentes.
Artículo 71: Cuando haya una conducta que infrinja las disposiciones de esta Ley, se registrará en los archivos de créditos y se hará pública de acuerdo con las leyes y normas administrativas pertinentes.
Artículo 72: Cuando los operadores de redes de asuntos gubernamentales de las organizaciones estatales no realicen las tareas de protección de la ciberseguridad según lo dispuesto en esta Ley, la organización del nivel superior o las organizaciones pertinentes ordenarán correcciones; se impondrán sanciones a los directivos directamente responsables y a otro personal directamente responsable.
Artículo 73: Cuando los departamentos de ciberseguridad e informatización y otros departamentos pertinentes infrinjan las disposiciones del Artículo 30 de la presente Ley al utilizar información personal adquirida durante el desempeño de las funciones de protección de la ciberseguridad para otros fines, se impondrán sanciones a los responsables directos y a otro personal directamente responsable.
Cuando el personal de los departamentos de ciberseguridad e informatización y de otros departamentos pertinentes descuide sus deberes, abuse de su autoridad, muestre favoritismo, y ello no constituya un delito, se impondrán sanciones de acuerdo con la ley.
Artículo 74: Cuando las infracciones de las disposiciones de esta Ley causen daños a terceros, la responsabilidad civil se asumirá de acuerdo con la ley.
Cuando se infrinjan las disposiciones de esta Ley, constituyendo una infracción de la gestión del orden público, se impondrán sanciones administrativas de orden público conforme a la ley; cuando se constituya un delito, se perseguirá la responsabilidad penal conforme a la ley.
Artículo 75: En caso de que instituciones, organizaciones o personas extranjeras realicen ataques, intrusiones, interferencias, daños u otras actividades que pongan en peligro la infraestructura de información crítica de la República Popular China y causen graves consecuencias, se perseguirá la responsabilidad legal conforme a la ley; los departamentos de seguridad pública dependientes del Consejo de Estado y los departamentos pertinentes también podrán decidir congelar los activos de las instituciones, organizaciones o individuos o tomar otras medidas punitivas necesarias.

Capítulo VII: Disposiciones complementarias

Artículo 76: En esta ley, los términos que se indican a continuación tienen el siguiente significado:

(1) "Red" [网络, también "ciber"] se refiere a un sistema compuesto por computadoras u otros terminales de información y equipos relacionados que sigue ciertas reglas y procedimientos para la recopilación, almacenamiento, transmisión, intercambio y procesamiento de información.

(2) "Ciberseguridad" [网络安全, también "seguridad de la red"] se refiere a la adopción de las medidas necesarias para evitar los ciberataques, las intrusiones, las interferencias, la destrucción y el uso ilícito, así como los accidentes inesperados, para colocar las redes en un estado de funcionamiento estable y confiable, así como para garantizar la capacidad de que los datos de la red sean completos, confidenciales y utilizables.

(3) "Operadores de redes" [网络运营者] se refiere a los propietarios de redes, administradores y proveedores de servicios de redes.

(4) "Datos de red" [网络数据] se refiere a todo tipo de datos electrónicos recopilados, almacenados, transmitidos, procesados y producidos a través de redes.

(5) "Información personal" [个人信息] se refiere a todo tipo de información, registrada electrónicamente o a través de otros medios, que, por sí sola o junto con otra información, es suficiente para identificar la identidad de una persona física, incluidos, entre otros, los nombres completos de las personas físicas, las fechas de nacimiento, los números de identificación nacional, la información biométrica personal, las direcciones, los números de teléfono, etc.

Artículo 77: La protección de la seguridad operativa de las redes que almacenan o procesan información que afecta a los secretos nacionales se ajustará a la presente Ley y también respetará las disposiciones de las leyes y las normas administrativas relativas a la protección de información confidencial.

Artículo 78: Las normas de protección de la seguridad de las redes militares son formuladas por la Comisión Militar Central.

Artículo 79: Esta Ley entrará en vigencia el 1 de junio de 2017**.**

Apéndice 2
Medidas de gestión de nombres de dominio de Internet del Ministerio de Industria y Tecnología de la Información de China[31] (extractos).

Artículo 3 de las medidas designadas por el Ministerio de Industria y Tecnología de la Información para llevar a cabo la "supervisión y gestión sobre los servicios de nombres de dominio a nivel nacional, sus principales tareas son: (1) formular las normas y políticas de gestión de los nombres de dominio de Internet; (2) formular un sistema de nombres de dominio de Internet y un plan de desarrollo de los recursos de nombres de dominio; (3) gestionar los organismos nacionales de gestión de servidores raíz de los nombres de dominio y los organismos de registro y gestión de los nombres de dominio; (4) ser responsable de la gestión de la seguridad de la red y de la información del sistema de nombres de dominio; (5) proteger la información personal de los usuarios y los derechos e intereses legítimos conforme a la ley; (6) ser responsable de la coordinación internacional relativa a los nombres de dominio; (7) gestionar los servicios nacionales de resolución de nombres de dominio; (8) gestionar otras actividades relativas a los servicios de nombres de dominio".
El **Artículo 10** de las medidas establecía que "quienes soliciten el establecimiento de un servidor raíz de nombres de dominio o de un organismo gestor de servidores raíz de nombres de dominio, deberán cumplir las siguientes condiciones: (1) el servidor raíz de nombres de dominio se establecerá dentro de las fronteras, y se ajustará a los correspondientes planes de desarrollo de Internet y a los requisitos de funcionamiento seguro y estable del sistema de nombres de dominio".
Artículo 11: Quienes soliciten la creación de un organismo de registración y gestión de nombres de dominio deberán cumplir las siguientes condiciones:
(1) el sistema de gestión de nombres de dominio de alto nivel debe establecerse dentro de las fronteras, y los nombres de dominio de alto nivel que posean deben ajustarse a las leyes y normas pertinentes, así como a los requisitos de funcionamiento seguro y estable del sistema de nombres de dominio;

(2) [deberán] ser personas jurídicas legalmente establecidas dentro de las fronteras, dicha persona jurídica y sus principales inversores, personal operativo y directivo principal deben tener un buen historial crediticio;

(3) deberán disponer de perfectos planes de desarrollo profesional y planes tecnológicos, así como de instalaciones, finanzas y personal especializado adecuados para dedicarse a las operaciones y la gestión de los nombres de dominio de alto nivel, así como de sistemas de gestión de la información que se ajusten a los requisitos del organismo de gestión de las telecomunicaciones;

(4) deberán disponer de medidas completas de gestión de la seguridad de la red y de la información, incluido el personal de gestión, las estructuras de gestión de la seguridad de la red

[31] Ministerio de Industria y Tecnología de la Información, Medidas sobre la administración de nombres de dominio de Internet, 24 de agosto de 2017 https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/ (traducción no oficial). Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.cac.gov.cn/2017-09/28/c_1121737753.htm.

y de la información, los planes de procesamiento de respuestas ante emergencias y las correspondientes medidas tecnológicas y de gestión;

(5) deberán tener la capacidad de realizar la verificación de la información de la identidad real y la protección de la información personal de los usuarios, la capacidad de proporcionar servicios a largo plazo, así como mecanismos completos de procesamiento de retirada de servicios;

(6) deberán disponer de estructuras completas de gestión de servicios de registración de nombres de dominio y de mecanismos de supervisión de los organismos de servicios de registración de nombres de dominio;

(7) otros requisitos previstos en las leyes y normas administrativas.
Artículo 12: Quienes soliciten la creación de un organismo de servicios de registración de nombres de dominio deberán cumplir las siguientes condiciones:
(1) el sistema de servicio de registración de nombres de dominio, la base de datos de registración y los sistemas de resolución deben establecerse dentro de las fronteras;
(2) [deberán] ser personas jurídicas legalmente establecidas dentro de las fronteras, dicha persona jurídica y sus principales inversores, personal operativo y directivo principal deberán tener buenos antecedentes crediticios;
(3) disponer de locales, finanzas y personal especializado adecuados para dedicarse a los servicios de registración de nombres de dominio, así como de sistemas de gestión de la información conformes a los requisitos del organismo de gestión de las telecomunicaciones;
(4) tener la capacidad de realizar la verificación de la información de identidad real y la protección de la información personal de los usuarios, la capacidad de proporcionar servicios a largo plazo, así como mecanismos completos de procesamiento de retirada de servicios;
(5) disponer de estructuras completas de gestión del servicio de registración de nombres de dominio y de mecanismos de supervisión de los organismos de registración de nombres de dominio;
(6) disponer de medidas completas de gestión de la seguridad de la red y de la información, incluido el personal de gestión, las estructuras de gestión de la seguridad de la red y de la información, los planes de procedimientos de respuesta ante emergencias y las correspondientes medidas tecnológicas y de gestión.
(7) otros requisitos previstos en las leyes y normas administrativas.
Artículo 13: Quienes soliciten el establecimiento de un servidor raíz de nombres de dominio y de un organismo de gestión de servidores raíz, o de un organismo de gestión de registración de nombres de dominio, deberán presentar los materiales de solicitud al Ministerio de Industria y Tecnología de la Información. Quienes soliciten el establecimiento de un organismo de servicios de registración de nombres de dominio deberán presentar los materiales de solicitud al departamento de gestión de telecomunicaciones local, provincial, autonómico o municipal. Los materiales de solicitud deberán incluir:
(1) las circunstancias básicas de la unidad de trabajo solicitante;
(2) materiales de certificación para la gestión eficaz de los servicios de nombres de dominio, incluidos los materiales de certificación de los sistemas e instalaciones pertinentes, así como las capacidades de servicio, las estructuras de gestión y los acuerdos celebrados con otros organismos;
(3) estructuras y medidas de protección de la seguridad de la red y la información;
(4) materiales que certifiquen la reputación de la unidad de trabajo solicitante;
(5) una carta de compromiso, firmada por el representante legalmente designado, para realizar la actividad comercial de forma honesta y conforme a la ley".

Artículo 37: "En la prestación de servicios de resolución de nombres de dominio, la información de resolución no puede ser distorsionada sin autorización. La resolución de nombres de dominio no debe ser redirigida maliciosamente hacia direcciones IP de otras personas por ninguna organización o persona".
El **Artículo 41** de las medidas establece que "Cuando sea necesario debido a la seguridad nacional o para hacer frente a incidentes de emergencia, los organismos de gestión de servidores raíz de nombres de dominio, los organismos de gestión de registración de nombres de dominio y los organismos de servicio de registración de nombres de dominio deberán obedecer el mando y la coordinación unificados de los organismos de gestión de telecomunicaciones, y respetar los requisitos de gestión de los organismos de gestión de telecomunicaciones".
Artículo 46: "Los organismos de gestión de telecomunicaciones establecerán estructuras de registro de créditos para los organismos que gestionan los servidores raíz de nombres de dominio, los organismos de gestión de registración de nombres de dominio y los organismos de servicio de registración de nombres de dominio, y registrarán en el archivo de créditos sus infracciones de estas Medidas, así como la sanción administrativa que reciban".

Apéndice 3
Sistema chino de nombres de dominio de Internet[32] (extractos)

I. Todos los niveles de nombre de dominio de Internet en nuestra nación pueden estar compuestos por letras (A-Z, a-z, siendo equivalentes las mayúsculas y las minúsculas), números (0-9), guiones (-) o caracteres chinos; y todos los dominios deben utilizar el punto (.) como conectores, y todos los niveles de nombres de dominio en idioma chino deben utilizar los puntos o el punto chino (。) como conectores.

II. Además de los dominios de alto nivel ".CN" y ".中国", el sistema de nombres de dominio de Internet de nuestra nación establece múltiples dominios de alto nivel en inglés y chino, de los cuales los dominios de primer nivel "政务" [.gov] y ".公益" [.org - literalmente interés público] serán dominios de alto nivel especializados en idioma chino para los grupos y órganos del Partido y el Gobierno de la nación y todos los niveles de otros departamentos de asuntos gubernamentales, así como para instituciones sin ánimo de lucro. El diagrama del sistema de dominios de Internet de nuestro país puede encontrarse en http://中国互联网域名体系.中国""http://中国互联网域名体系.政务"o "http://中国互联网域名体系.信息".

III. Bajo el dominio de alto nivel nacional ".CN", se establecen dos tipos de dominios de segundo nivel, los "dominios de categoría" y los "dominios de región administrativa". Se establecen nueve "dominios de categoría", a saber: "政务" utilizado para los grupos y órganos del Partido y del gobierno a todos los niveles y otros departamentos de asuntos gubernamentales; "公益" utilizado para las organizaciones sin fines de lucro; "GOV", utilizado para los organismos gubernamentales; "ORG", utilizado para las organizaciones sin fines de lucro; "AC", utilizado para las instituciones de investigación científica; "COM", utilizado para las empresas industriales, comerciales, financieras y otras; "EDU", utilizado para los organismos educativos; "MIL", utilizado para las instituciones de defensa nacional; y "NET", utilizado para las instituciones que prestan servicios de Internet.
Se establecen 34 "dominios de regiones administrativas", que se utilizarán para cada una de las provincias, regiones autónomas, municipios de gobierno directo y organizaciones de regiones administrativas especiales de la nación [...].

IV. Se puede presentar una solicitud para registrar directamente nombres de dominio de segundo nivel bajo los dominios nacionales de alto nivel ".CN" y ".中国".

[32] China Law Translate, Sistema de Nombres de Dominio de Internet de China, 5 de marzo de 2018 https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/ (traducción no oficial). Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://xn--eqrt2g.xn--vuq861b/#.

Apéndice 4
Ley de Seguridad de Datos de la República Popular China (DSL)[33] (Extractos)

Artículo 3: El término "datos", tal y como se utiliza en esta Ley, se refiere a cualquier registro de información en formato electrónico o de otro tipo.
- El tratamiento de datos incluye la recopilación, el almacenamiento, el uso, el procesamiento, la transmisión, el suministro, la divulgación, etc., de datos.
- La seguridad de los datos se refiere al empleo de las medidas necesarias para garantizar la protección efectiva de los datos y su uso legal, así como la capacidad de garantizar un estado de seguridad sostenido.

Artículo 7: El Estado debe proteger los derechos e intereses de las personas y organizaciones en relación con los datos; fomentar el uso legal, razonable y eficaz de los datos; garantizar la libre circulación legal y ordenada de los datos; y promover el desarrollo de una economía digital con los datos como factor clave.

Artículo 11: El Estado llevará a cabo activamente intercambios y cooperación internacional en los sectores de la gobernanza de la seguridad de los datos y el desarrollo y uso de datos, participará en la formulación de reglas y normas internacionales relacionadas con la seguridad de los datos y promoverá el flujo seguro y libre de datos a través de las fronteras.

Artículo 14: El Estado debe poner en marcha una estrategia de macrodatos, para avanzar en el establecimiento de una infraestructura de datos y fomentar y apoyar las aplicaciones innovadoras de los datos en cada industria y campo.

Artículo 17: El Estado debe avanzar en el establecimiento de un sistema de estándares para las tecnologías de desarrollo y explotación de datos y la seguridad de los datos. En el ámbito de sus respectivas funciones, los departamentos del Consejo de Estado encargados de la estandarización y otros departamentos pertinentes del Consejo de Estado deben organizar la formulación y la revisión adecuada de los estándares relacionados con la tecnología y los productos para el desarrollo y la explotación de datos y con la seguridad de los datos. El Estado debe apoyar a las empresas y grupos sociales, organismos educativos o de investigación, etc., para que participen en la elaboración de los estándares.

Artículo 21: Los datos relacionados con la seguridad nacional, el sustento de la economía nacional, el sustento de personas importantes, los intereses públicos principales y otros pertenecen a los datos básicos nacionales, y deberán aplicarse a un sistema de gestión más estricto.

Artículo 25: El Estado debe aplicar controles de exportación de acuerdo con la ley para los datos que son artículos controlados, relacionados con la preservación de la seguridad nacional y el cumplimiento de las obligaciones internacionales.

Artículo 26: Cuando alguna nación o región emplee medidas discriminatorias, restrictivas u otras similares contra la República Popular China en ámbitos como la inversión o el comercio de datos y la tecnología para la explotación y el desarrollo de datos, la República Popular China podrá emplear medidas iguales contra esa nación o región en función de las circunstancias reales.

---

[33] Ley de Seguridad de Datos de la República Popular China, 11 de junio de 2021, traducida en el siguiente enlace: https://www.secrss.com/articles/31844 (traducción no oficial, la publicación original se encuentra aquí: http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm). Este documento se tradujo a varios idiomas a título informativo únicamente. El texto original y autoritativo (en idioma chino) se encuentra disponible aquí: http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm.

Artículo 27: La realización de actividades de tratamiento de datos a través de redes de información, es decir, Internet, deberá cumplir con los deberes de protección de la seguridad de los datos sobre la base del sistema de protección multinivel para la ciberseguridad.
Artículo 31: Las disposiciones de la Ley de Ciberseguridad de la República Popular China se aplican a la gestión de la seguridad para la exportación de datos del territorio [continental] que hayan sido recopilados o producidos por operadores de infraestructuras críticas de información dentro del territorio [continental] de la República Popular China; las medidas de gestión de la seguridad para la exportación de datos importantes del territorio continental que hayan sido recopilados o producidos por otros responsables del tratamiento de datos dentro del territorio [continental] de la República Popular China deben ser redactadas por el departamento de información de Internet del Estado junto con los departamentos pertinentes del Consejo de Estado.
Artículo 32: Toda organización o persona que recopile datos deberá emplear métodos legales y apropiados y no deberá robar ni obtener datos mediante otros métodos ilegales. En los casos en que las leyes y las normas administrativas contengan disposiciones sobre la finalidad o el alcance de la recopilación y el uso de los datos, éstas deberán recopilarse o utilizarse dentro de la finalidad y el alcance previstos en dichas leyes y normas administrativas.
Artículo 33: Cuando las instituciones dedicadas a los servicios de intermediación de transacciones de datos presten servicios, exigirán a la parte que proporciona los datos que explique las fuentes de los datos, verifique las identidades de ambas partes de la transacción y guarde un registro de la revisión y la transacción.
Artículo 36: Los órganos estatales competentes de la República Popular China, en virtud de las disposiciones de las leyes y los tratados o acuerdos celebrados o en los que participa la República Popular China, o en virtud del principio de igualdad y beneficios mutuos, tramitarán la solicitud de suministro de datos por parte de un organismo de cumplimiento de la ley o judicial extranjero. Sin la aprobación de los órganos estatales competentes de la República Popular China, las organizaciones o las personas que se encuentren en el territorio [continental] de la República Popular China no podrán proporcionar datos dentro de la República Popular China a un organismo de cumplimiento de la ley o judicial extranjero.
Artículo 38: El desempeño de los órganos del Estado de las funciones legalmente prescritas que requieren la recopilación y el uso de datos deberá enmarcarse dentro del ámbito de las funciones legalmente prescritas y proceder de acuerdo con los requisitos y procedimientos de las leyes y las normas administrativas; en el desempeño de las funciones para conocer la privacidad personal, la información personal, los secretos comerciales, la información comercial confidencial y otros datos se mantendrán confidenciales de acuerdo con la ley, y no se divulgarán ni se proporcionarán ilegalmente a terceros.
Artículo 40: Los órganos del Estado que confíen a otros la creación o el mantenimiento de sistemas electrónicos de asuntos gubernamentales o el almacenamiento o el tratamiento de datos de asuntos gubernamentales, deberán someterse a estrictos procedimientos de aprobación y supervisar el cumplimiento de las correspondientes obligaciones de protección de datos por parte de las partes encargadas. La parte encargada cumplirá las obligaciones de protección de la seguridad de los datos de acuerdo con las disposiciones de las leyes y normas y los acuerdos contractuales, y no retendrá, utilizará, divulgará ni proporcionará los datos de asuntos gubernamentales a terceros sin autorización.
Artículo 44: Cuando los departamentos reguladores pertinentes que desempeñan las funciones de supervisión y gestión de la seguridad de los datos descubran que las actividades de tratamiento de datos presentan mayores riesgos para la seguridad, podrán dar una charla a las organizaciones y personas pertinentes y exigirles que empleen procedimientos, hagan correcciones y eliminen los peligros ocultos de acuerdo con la autoridad y los procedimientos previstos.

Artículo 49: Cuando los órganos del Estado no cumplan con las obligaciones de protección de la seguridad de los datos previstas en la presente ley, los directivos y demás personal directamente responsable deberán ser sancionados de acuerdo con la ley.
Artículo 52: Cuando las infracciones de las disposiciones de esta ley causen daños a terceros, la responsabilidad civil se asumirá de acuerdo con la ley.

Apéndice 5
Ley de Protección de Información Personal de la República Popular China[34]

(aprobada en la 30.ª reunión del Comité Permanente de la 13.ª Asamblea Popular Nacional el 20 de agosto de 2021)

Capítulo I: Disposiciones Generales

Artículo 1: Esta Ley está formulada, sobre la base de la Constitución, para proteger los derechos e intereses de la información personal, estandarizar las actividades de tratamiento de información personal y promover el uso racional de la información personal.

Artículo 2: La información personal de las personas físicas recibe protección legal; ninguna organización o persona puede infringir los derechos e intereses de información personal de las personas físicas.

Artículo 3: Esta Ley se aplica a las actividades de tratamiento de información personal de personas físicas dentro de las fronteras de la República Popular China.

La presente Ley se aplica también a las actividades de tratamiento fuera de las fronteras de la República Popular China de información personal de personas físicas dentro de las fronteras de la República Popular China cuando se da una de las circunstancias siguientes:

1. Cuando el objetivo sea proporcionar productos o servicios a personas físicas dentro de las fronteras.
2. Cuando se analicen o evalúen actividades de personas físicas dentro de las fronteras.
3. Otras circunstancias previstas en las leyes o normas administrativas.

Artículo 4: La información personal es todo tipo de información registrada por medios electrónicos o de otro tipo relacionada con personas físicas identificadas o identificables, sin incluir la información después del tratamiento de anonimización.

[34] Ley de Protección de Información Personal de la República Popular China, (aprobada en la 30.ª reunión del Comité Permanente de la 13.ª Asamblea Popular Nacional el 20 de agosto de 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml, según traducción de DigiChina en el siguiente enlace: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021

El tratamiento de información personal incluye la recopilación, el almacenamiento, el uso, el procesamiento, la transmisión, el suministro, la divulgación, la supresión, etc. de la información personal.
Artículo 5: En el tratamiento de la información personal, se respetarán los principios de legalidad, corrección, necesidad y honestidad. Se prohíbe el tratamiento de información personal en forma de estafa, engañosa, coercitiva o de otro tipo.
Artículo 6: El tratamiento de información personal debe tener un propósito claro y razonable, y debe estar directamente relacionado con el propósito del tratamiento, mediante el uso de un método que ejerza la menor influencia en los derechos e intereses individuales.
La recopilación de información personal se limitará al menor alcance posible para realizar el propósito del tratamiento, y se prohíbe la recopilación excesiva de información personal.
Artículo 7: En el tratamiento de información personal, se respetarán los principios de apertura y transparencia, se revelarán las normas para el tratamiento de información personal y se indicará claramente el propósito, el método y el alcance del tratamiento.
Artículo 8: El tratamiento de información personal garantizará la calidad de la información personal y evitará los efectos adversos sobre los derechos e intereses individuales de la información personal inexacta o incompleta.
Artículo 9: Los responsables del tratamiento de información personal serán responsables de sus actividades de tratamiento de información personal y adoptarán las medidas necesarias para proteger la seguridad de la información personal que manejan.
Artículo 10: Ninguna organización o persona puede recopilar, utilizar, procesar o transmitir ilegalmente información personal de otras personas, ni vender, comprar, proporcionar o divulgar ilegalmente información personal de otras personas, ni participar en actividades de tratamiento de información personal que perjudiquen la seguridad nacional o el interés público.
Artículo 11: El Estado establece una estructura de protección de la información personal, para prevenir y sancionar los actos que perjudican los derechos e intereses de la información personal, fortalecer la propaganda y la educación en materia de protección de la información personal, y promover la creación de un buen entorno para la protección de la información personal, con la participación conjunta del gobierno, las empresas, las organizaciones sociales pertinentes y el público en general.
Artículo 12: El Estado participa enérgicamente en la formulación de reglas [o normas] internacionales para la protección de la información personal, estimula el intercambio y la cooperación internacional en el ámbito de la protección de la información personal y promueve el reconocimiento mutuo de las reglas [o normas], estándares, etc., de protección de la información personal, con otros países, regiones y organizaciones internacionales.

Capítulo II: Normas sobre el tratamiento de la información personal

Sección 1: Disposiciones ordinarias

Artículo 13: Los responsables del tratamiento de información personal solo pueden tratar la información personal cuando se ajustan a una de las circunstancias siguientes:

1. Obtención del consentimiento de las personas.
2. Cuando sea necesario para celebrar o cumplir un contrato en el que la persona sea parte interesada, o cuando sea necesario para llevar a cabo la gestión de los recursos humanos de acuerdo con las normas y estructuras laborales legalmente formuladas y los contratos colectivos legalmente celebrados.
3. Cuando sea necesario para cumplir con los deberes y responsabilidades legales o con las obligaciones legales.

4. Cuando sea necesario para responder a incidentes repentinos de salud pública o para proteger la vida y la salud de las personas físicas, o la seguridad de sus bienes, en condiciones de emergencia.
5. El tratamiento de información personal dentro de un ámbito razonable para llevar a cabo reportajes de noticias, supervisión de la opinión pública y otras actividades de este tipo para el interés público.
6. Cuando se trate de información personal revelada por las propias personas o que ya haya sido revelada legalmente, dentro de un alcance razonable de acuerdo con las disposiciones de esta Ley.
7. Otras circunstancias previstas en las leyes y normas administrativas.

De acuerdo con otras disposiciones pertinentes de esta Ley, cuando se esté tratando información personal, se deberá obtener el consentimiento individual. Sin embargo, la obtención del consentimiento individual no es necesaria en las condiciones de los apartados 2 a 7 anteriores.

Artículo 14: Cuando el tratamiento de información personal se base en el consentimiento individual, dicho consentimiento deberá ser otorgado por las personas bajo la condición previa de pleno conocimiento y en una declaración voluntaria y explícita. Cuando las leyes o normas administrativas establezcan que se debe obtener un consentimiento aparte o un consentimiento por escrito para tratar la información personal, se seguirán dichas disposiciones.

Cuando se produzca un cambio en la finalidad del tratamiento de la información personal, en el método de tratamiento o en las categorías de información personal tratada, deberá obtenerse de nuevo el consentimiento de la persona.

Artículo 15: Cuando el tratamiento de información personal se base en el consentimiento individual, las personas tienen derecho a revocar su consentimiento. Los responsables del tratamiento de información personal proporcionarán una forma conveniente de retirar el consentimiento.

Si una persona revoca su consentimiento, ello no afectará a la eficacia de las actividades de tratamiento de información personal realizadas sobre la base del consentimiento individual antes de su revocación.

Artículo 16: Los responsables del tratamiento de información personal no podrán negarse a suministrar productos o servicios basándose en que una persona no consiente el tratamiento de su información personal o revoca su consentimiento, excepto cuando el tratamiento de información personal sea necesario para el suministro de productos o servicios.

Artículo 17: Los responsables del tratamiento de información personal deberán, antes de tratar la información personal, notificar explícitamente a las personas de forma veraz, precisa y completa los siguientes elementos, utilizando un lenguaje claro y fácilmente comprensible:

1. La denominación o nombre personal y la forma de contacto del responsable del tratamiento de la información personal.
2. La finalidad del tratamiento de información personal y los métodos de tratamiento, las categorías de información personal tratada y el período de retención.
3. Los métodos y procedimientos para que las personas ejerzan los derechos previstos en esta Ley.
4. Los demás elementos que las leyes o normas administrativas prevean deberán ser notificados.

Cuando se produzca un cambio en las cuestiones previstas en el párrafo anterior, dicho cambio se deberá notificar a las personas.

Cuando los responsables del tratamiento de información personal notifiquen las cuestiones previstas en el Párrafo 1 mediante el método de formulación de normas de tratamiento de información personal, las normas de tratamiento se harán públicas [se divulgarán] y serán fáciles de leer y almacenar.

Artículo 18: Los responsables del tratamiento de información personal podrán no notificar a las personas los asuntos previstos en el Párrafo 1 del Artículo anterior en los casos en que las leyes o normas administrativas establezcan que se debe preservar la confidencialidad o que la notificación no es necesaria.
En circunstancias de emergencia, cuando sea imposible notificar a las personas de manera oportuna para proteger la vida, la salud y la seguridad de los bienes de las personas físicas, los responsables del tratamiento de información personal deberán notificarlas una vez concluidas las circunstancias de emergencia.
Artículo 19: Salvo que las leyes o normas administrativas dispongan lo contrario, los períodos de retención de la información personal serán los más breves que sean necesarios para cumplir con la finalidad del tratamiento de la información personal.
Artículo 20: Cuando dos o más responsables del tratamiento de información personal decidan conjuntamente la finalidad y el método de tratamiento de información personal, deberán acordar los derechos y obligaciones de cada uno. Sin embargo, dicho acuerdo no influye en los derechos de una persona a exigir que uno de los responsables del tratamiento de información personal cumpla con las disposiciones de esta Ley.
Cuando los responsables del tratamiento de información personal que estén tratando información personal de forma conjunta perjudiquen los derechos e intereses de la información personal, lo cual suponga daños y perjuicios, asumen solidariamente la responsabilidad de acuerdo con la ley.
Artículo 21: Cuando los responsables del tratamiento de información personal encomiendan el tratamiento de la información personal, deberán celebrar un acuerdo con la persona encomendada sobre el objetivo del tratamiento, el plazo, el método de tratamiento, las categorías de información personal, las medidas de protección, así como los derechos y deberes de ambas partes, etc., y deberán llevar a cabo la supervisión de las actividades de tratamiento de la información personal por parte de la persona encomendada.
Las personas encomendadas deberán tratar la información personal de acuerdo con el contrato; no podrán tratar la información personal con fines de tratamiento o con métodos de tratamiento, etc., que excedan lo acordado. Si el contrato de encargo no tiene efecto, es nulo, se ha cancelado o se ha rescindido, la persona encomendada deberá devolver la información personal al responsable del tratamiento de información personal o deberá eliminarla, y no podrá conservarla.
Sin el consentimiento del responsable del tratamiento de información personal, la persona encargada no podrá encomendar el tratamiento de la información personal a otras personas.
Artículo 22: Cuando sea necesario transferir información personal debido a fusiones, separaciones, disoluciones, declaraciones de quiebra y otras razones similares, los responsables del tratamiento de información personal deberán notificar a las personas la denominación o nombre personal y el método de contacto de la parte receptora. La parte receptora deberá seguir cumpliendo con las obligaciones del responsable del tratamiento de la información personal. Cuando la parte receptora cambie la finalidad original del tratamiento o el método de tratamiento, deberá notificarlo de nuevo a la persona según lo dispuesto en esta Ley.
Artículo 23: Cuando los responsables del tratamiento de información personal proporcionen a otros responsables del tratamiento de información personal la información personal que manejan, deberán notificar a las personas la denominación o nombre personal del receptor, su método de contacto, la finalidad del tratamiento, el método de tratamiento y las categorías de información personal, y deberán obtener el consentimiento por separado de la persona. Los receptores tratarán la información personal dentro del ámbito mencionado de los fines del tratamiento, los métodos de tratamiento, las categorías de información personal, etc. Cuando

los receptores cambien la finalidad o los métodos de tratamiento originales, deberán obtener de nuevo el consentimiento de la persona.
Artículo 24: Cuando los responsables del tratamiento de información personal utilicen la información personal para tomar decisiones automatizadas, se garantizará la transparencia de la toma de decisiones y la equidad y justicia del resultado del tratamiento, y no podrán realizar un tratamiento diferenciado e irrazonable de las personas en las condiciones comerciales, como el precio comercial, etc.
Quienes realicen envíos de información o ventas comerciales a particulares mediante métodos automatizados de toma de decisiones deberán ofrecer simultáneamente la opción de no fijar como objetivo las características de la persona, o proporcionarle un método conveniente para negarse.
Cuando el uso de la toma de decisiones automatizada produzca decisiones con una influencia importante en los derechos e intereses de la persona, ésta tiene derecho a exigir a los responsables del tratamiento de información personal que expliquen el asunto, y tiene derecho a negarse a que los responsables del tratamiento de información personal tomen decisiones únicamente mediante métodos de toma de decisiones automatizada.
Artículo 25: Los responsables del tratamiento de información personal no pueden revelar la información personal que manejan, excepto si obtienen un consentimiento por separado.
Artículo 26: La instalación de equipos de recopilación de imágenes o de reconocimiento de la identidad personal en lugares públicos se realizará de acuerdo con las necesidades para proteger la seguridad pública y respetar la normativa pertinente del Estado, y se instalarán señalizaciones indicativas claras. Las imágenes personales recopiladas y la información sobre características de identidad personal pueden utilizarse únicamente para proteger la seguridad pública; no pueden utilizarse para otros fines, salvo que se obtenga el consentimiento por separado de las personas.
Artículo 27: Los responsables del tratamiento de información personal pueden, dentro de un ámbito razonable, tratar la información personal que ya haya sido revelada por la propia persona o que haya sido revelada legalmente de otra manera, excepto cuando la persona se niegue claramente. Los responsables del tratamiento de información personal que manejen información personal que ya haya sido revelada, cuando haya una influencia importante en los derechos e intereses individuales, deberán obtener el consentimiento personal de acuerdo con las disposiciones de esta Ley.

Sección II: Normas para el tratamiento de información personal sensible

Artículo 28: Información personal sensible significa la información personal que, una vez filtrada o utilizada ilegalmente, puede causar fácilmente un daño a la dignidad de las personas físicas o un daño grave a la seguridad personal o patrimonial, incluida la información sobre características biométricas, creencias religiosas, estatus especialmente designado, salud médica, cuentas financieras, seguimiento de la localización individual, etc., así como la información personal de los menores de 14 años.
Los responsables del tratamiento de información personal podrán tratar información personal sensible únicamente cuando exista una finalidad específica y una necesidad que cumplir, y en circunstancias de estrictas medidas de protección.
Artículo 29: Para tratar información personal sensible, se deberá obtener el consentimiento por separado de la persona. Cuando las leyes o normas administrativas establezcan que se debe obtener un consentimiento por escrito para tratar la información personal sensible, se seguirán dichas disposiciones.
Artículo 30: Los responsables del tratamiento de información personal sensible, además de lo establecido en el Artículo 17, Párrafo 1, de la presente Ley, deberán notificar a las personas la

necesidad y la influencia del tratamiento de la información personal sensible sobre sus derechos e intereses, excepto cuando la presente Ley establezca que está permitido no notificar a las personas.
Artículo 31: Cuando los responsables del tratamiento de información personal traten información personal de menores de 14 años, deberán obtener el consentimiento de los padres o tutores del menor.
Cuando los responsables del tratamiento de información personal traten información personal de menores de 14 años, deberán formular normas especializadas para el tratamiento de la información personal.
Artículo 32: Cuando las leyes o normas administrativas establezcan que se debe obtener licencias administrativas pertinentes o que se aplican otras restricciones para el tratamiento de la información personal sensible, se seguirán dichas disposiciones.

Sección III: Disposiciones específicas sobre los órganos del Estado que tratan información personal

Artículo 33: La presente Ley se aplica a las actividades de los órganos del Estado en materia de tratamiento de información personal; en los casos en que esta Sección contiene disposiciones específicas, se aplican las disposiciones de esta Sección.
Artículo 34: Los órganos del Estado que manejen información personal para cumplir con sus obligaciones y responsabilidades legales las llevarán a cabo de acuerdo con las facultades y procedimientos previstos en las leyes o normas administrativas; no podrán exceder el alcance o la extensión necesaria para cumplir con sus obligaciones y responsabilidades legales.
Artículo 35: Los órganos del Estado que traten información personal con el fin de cumplir con sus obligaciones y responsabilidades legales deberán cumplir con la obligación de notificación, excepto cuando se den las circunstancias previstas en el Artículo 18, Párrafo I, de la presente Ley, o cuando la notificación impida a los órganos del Estado cumplir con sus obligaciones y responsabilidades legales.
Artículo 36: La información personal tratada por los órganos del Estado se almacenará dentro del territorio continental de la República Popular China. En los casos en los que sea realmente necesario proporcionarla en el extranjero, se llevará a cabo una evaluación de seguridad. Se podrá solicitar a las autoridades competentes que brinden apoyo y colaboración en la evaluación de la seguridad.
Artículo 37: Las disposiciones de esta Ley relativas al tratamiento de la información personal por parte de los órganos del Estado se aplican al tratamiento de la información personal para cumplir con las obligaciones legales por parte de las organizaciones autorizadas por las leyes y normas para gestionar las funciones de los asuntos públicos.

Capítulo III: Normas sobre el suministro transfronterizo de información personal

Artículo 38: Cuando los responsables del tratamiento de información personal necesiten realmente proporcionar información personal fuera de las fronteras de la República Popular China por motivos comerciales u otros requisitos similares, deberán cumplir una de las siguientes condiciones:

1. Superar una evaluación de seguridad organizada por el departamento de ciberseguridad e informatización del Estado de acuerdo con el Artículo 40 de esta Ley.
2. Someterse a una certificación de protección de la información personal realizada por un organismo especializado de acuerdo con las disposiciones del departamento de ciberseguridad e informatización del Estado.

3. Celebrar un contrato con la parte receptora extranjera de acuerdo con un contrato estándar formulado por el departamento de ciberespacio e informatización del Estado, acordando los derechos y responsabilidades de ambas partes.
4. Otras condiciones previstas en las leyes o normas administrativas o por el departamento de ciberespacio e informatización del Estado.

Cuando los tratados o acuerdos internacionales que la República Popular China haya celebrado o a los que se haya adherido contengan disposiciones pertinentes, como las condiciones sobre el suministro de datos personales fuera de las fronteras de la República Popular China, dichas disposiciones podrán aplicarse.

Los responsables del tratamiento de información personal adoptarán las medidas necesarias para garantizar que las actividades de tratamiento de información personal de los receptores extranjeros alcancen el nivel de protección de la información personal previsto en la presente Ley.

Artículo 39: Cuando los responsables del tratamiento de información personal proporcionen información personal fuera de las fronteras de la República Popular China, deberán notificar a la persona la denominación o nombre personal, el método de contacto, el propósito del tratamiento, los métodos de tratamiento y las categorías de información personal de la parte receptora extranjera, así como las formas o procedimientos para que las personas ejerzan los derechos previstos en esta Ley con la parte receptora extranjera, y otros asuntos similares, y obtener el consentimiento de las personas por separado.

Artículo 40: Los operadores de infraestructuras críticas de información y los responsables del tratamiento de información personal que alcancen las cantidades proporcionadas por el departamento de ciberseguridad e informatización del Estado almacenarán la información personal recopilada y producida dentro de las fronteras de la República Popular China a nivel nacional. Cuando necesiten proporcionarla en el extranjero, deberán superar una evaluación de seguridad organizada por el departamento de ciberseguridad e informatización del Estado; cuando las leyes o normas administrativas y las disposiciones del departamento de ciberseguridad e informatización del Estado permitan que no se lleve a cabo la evaluación de seguridad, se seguirán dichas disposiciones.

Artículo 41: Las autoridades competentes de la República Popular China, de acuerdo con las leyes y los tratados pertinentes o los acuerdos internacionales que la República Popular China haya celebrado o a los que se haya adherido, o de acuerdo con el principio de igualdad y beneficio mutuo, deben gestionar las solicitudes de las autoridades extranjeras encargadas del cumplimiento de la ley o judiciales en relación con el suministro de información personal almacenada a nivel nacional. Sin la aprobación de las autoridades competentes de la República Popular China, los responsables del tratamiento de información personal no pueden proporcionar información personal almacenada en el territorio continental de la República Popular China a organismos de cumplimiento de la ley o judiciales extranjeros.

Artículo 42: Cuando las organizaciones o personas extranjeras realicen actos de tratamiento de información personal que infrinjan los derechos e intereses de los ciudadanos de la República Popular China en materia de información personal, o que perjudiquen la seguridad nacional o el interés público de la República Popular China, el departamento de ciberseguridad e informatización del Estado podrá incluirlas en una lista que limite o prohíba el suministro de información personal, emitir una advertencia y adoptar medidas como limitar o prohibir el suministro de información personal a las mismas, etc.

Artículo 43: Cuando algún país o región adopte prohibiciones, limitaciones u otras medidas similares discriminatorias contra la República Popular China en el ámbito de la protección de la información personal, la República Popular China podrá adoptar medidas recíprocas contra dicho país o región en función de las circunstancias reales.

Capítulo IV: Derechos de las personas en las actividades de tratamiento de información personal

Artículo 44: Las personas tienen derecho a saber y a decidir sobre su información personal, y tienen derecho a limitar o rechazar el tratamiento de su información personal por parte de terceros, a menos que las leyes o normas administrativas estipulen lo contrario.

Artículo 45: Las personas tienen derecho a consultar y copiar su información personal de los responsables del tratamiento de información personal, excepto en las circunstancias previstas en el Artículo 18, Párrafo 1, o en el Artículo 35 de esta Ley.

Cuando las personas soliciten consultar o copiar su información personal, los responsables del tratamiento de información personal deberán proporcionársela de manera oportuna.

Cuando los individuos soliciten que su información personal sea transferida a un responsable del tratamiento de información personal que ellos designen, previo cumplimiento de las condiciones del departamento de ciberseguridad e informatización del Estado, los responsables del tratamiento de información personal deberán proporcionar un canal para transferirla.

Artículo 46: Cuando las personas descubran que su información personal es incorrecta o está incompleta, tienen derecho a solicitar a los responsables del tratamiento de información personal que la corrijan o la completen. Cuando las personas soliciten que se corrija o complete su información personal, los responsables del tratamiento de información personal verificarán la información personal y la corregirán o completarán de manera oportuna.

Cuando las personas soliciten que se corrija o complemente su información personal, los responsables del tratamiento de información personal verificarán la información personal y la corregirán o completarán de manera oportuna.

Artículo 47: Los responsables del tratamiento de información personal eliminarán proactivamente la información personal cuando tenga lugar una de las circunstancias siguientes; si el responsable del tratamiento de información personal no la ha eliminado, las personas tienen derecho a solicitar su eliminación:

1. La finalidad del tratamiento se ha alcanzado, es imposible de alcanzar, o [la información personal] ya no es necesaria para alcanzar la finalidad del tratamiento.
2. Los responsables del tratamiento de información personal dejan de suministrar productos o servicios, o el período de conservación ha caducado.
3. La persona revoca el consentimiento.
4. Los responsables del tratamiento de información personal han tratado la información personal infringiendo las leyes, las normas administrativas o los acuerdos.
5. Otras circunstancias previstas en las leyes o normas administrativas.

Cuando el período de retención previsto por las leyes o normas administrativas no haya caducado, o la eliminación de la información personal sea técnicamente difícil de realizar, los responsables del tratamiento de información personal dejarán de tratarla, salvo para almacenarla y tomar las medidas de protección de seguridad necesarias.

Artículo 48: Las personas tienen derecho a solicitar a los responsables del tratamiento de información personal que les expliquen las normas de tratamiento de la información personal.

Artículo 49: Cuando una persona física haya fallecido, sus familiares podrán, en aras de sus propios intereses legítimos y legales, ejercer los derechos previstos en este capítulo para consultar, copiar, corregir, eliminar, etc., la información personal del fallecido, salvo que éste haya dispuesto lo contrario antes de su muerte.

Artículo 50: Los responsables del tratamiento de información personal establecerán mecanismos convenientes para aceptar y tramitar las solicitudes de las personas para el ejercicio de sus derechos. Cuando rechacen las solicitudes de las personas para ejercer sus derechos, deberán explicar el motivo.

En caso de que los responsables del tratamiento de información personal rechacen las solicitudes de las personas para ejercer sus derechos, las personas podrán presentar una demanda ante un tribunal popular de acuerdo con la ley.

Capítulo V: Obligaciones de los responsables del tratamiento de información personal

Artículo 51: Los responsables del tratamiento de información personal, en base a la finalidad del tratamiento de información personal, los métodos de tratamiento, las categorías de información personal, así como la influencia en los derechos e intereses de las personas, los posibles riesgos de seguridad existentes, etc., adoptarán las siguientes medidas para garantizar que el tratamiento de información personal se ajuste a las disposiciones de las leyes y las normas administrativas, y evitar el acceso no autorizado, así como la filtración, distorsión o pérdida de información personal:

2. Formular estructuras de gestión interna y normas de funcionamiento.
3. Implementar una gestión categorizada de la información personal.
4. Adoptar las correspondientes medidas técnicas de seguridad, como el cifrado, la desidentificación, etc.
5. Determinar razonablemente los límites operativos para el manejo de la información personal, y llevar a cabo la formación y la capacitación en materia de seguridad para los empleados de forma periódica.
6. Formular y organizar la implementación de planes de respuesta ante incidentes de seguridad de la información personal.
7. Otras medidas previstas en las leyes o normas administrativas.

Artículo 52: Los responsables del tratamiento de información personal que alcanzan las cantidades de información personal estipuladas por el departamento de ciberseguridad e informatización del Estado deben nombrar funcionarios de protección de la información personal, que serán responsables de supervisar las actividades de tratamiento de la información personal, así como las medidas de protección adoptadas, etc.

Los responsables del tratamiento de información personal deberán revelar los métodos de contacto con los responsables de la protección de la información personal, e informar de los nombres personales de los responsables y de los métodos de contacto a los departamentos que cumplen con las obligaciones y responsabilidades de la protección de la información personal.

Artículo 53: Los responsables del tratamiento de información personal fuera de las fronteras de la República Popular China, según lo dispuesto en el Artículo 3, Párrafo 2, de la presente Ley, establecerán una entidad dedicada o nombrarán a un representante dentro de las fronteras de la República Popular China para que sea responsable de los asuntos relacionados con la información personal que manejan, y deberán comunicar el nombre de la entidad correspondiente o el nombre personal del representante y el método de contacto, etc., a los departamentos que cumplen con las obligaciones y responsabilidades de protección de la información personal.

Artículo 54: Los responsables del tratamiento de información personal deberán realizar periódicamente auditorías sobre el tratamiento de información personal y el cumplimiento de las leyes y las normas administrativas.

Artículo 55: Cuando se presente una de las circunstancias siguientes, los responsables del tratamiento de información personal deberán realizar una evaluación previa del impacto de la protección de la información personal y registrar la situación del tratamiento:

1. Tratamiento de información personal sensible.
2. Utilización de información personal para la toma de decisiones automatizada.

3. Encomendar el tratamiento de información personal, proporcionar información personal a otros responsables del tratamiento de información personal o divulgar información personal.
4. Suministro de información personal al extranjero.
5. Otras actividades de tratamiento de información personal con una influencia significativa sobre las personas.

Artículo 56: El contenido de la evaluación del impacto de la protección de la información personal deberá incluir:

1. Si la finalidad del tratamiento de la información personal, el método de tratamiento, etc., son legales, legítimos y necesarios.
2. La influencia sobre los derechos e intereses de las personas y los riesgos de seguridad.
3. Si las medidas de protección adoptadas son legales, eficaces y adecuadas al grado de riesgo.

Los informes de evaluación del impacto de la protección de la información personal y los registros del estado del tratamiento se conservarán durante al menos tres años.

Artículo 57: Cuando se produzca o pueda producirse una fuga, distorsión o pérdida de información personal, los responsables del tratamiento de información personal adoptarán inmediatamente medidas correctivas y lo notificarán a los departamentos que cumplan con las obligaciones y responsabilidades de protección de la información personal y a las personas. La notificación deberá incluir los siguientes elementos:

1. Las categorías de información, las causas y los posibles daños causados por la fuga, la distorsión o la pérdida que se haya producido o pueda haberse producido.
2. Las medidas correctivas adoptadas por el responsable del tratamiento de información personal y las medidas que los particulares pueden adoptar para mitigar el daño.
3. El método de contacto del responsable del tratamiento de información personal.

Cuando los responsables del tratamiento de información personal adopten medidas que puedan evitar eficazmente el daño generado por las fugas, la distorsión o la pérdida de información, los responsables del tratamiento de información personal están autorizados a no notificar a las personas; sin embargo, cuando los departamentos que cumplen con las obligaciones y responsabilidades de protección de la información personal consideren que se puede haber generado un daño, pueden exigir a los responsables del tratamiento de información personal que lo notifiquen.

Artículo 58: Los responsables del tratamiento de información personal que presten importantes servicios de plataforma de Internet, que tengan una gran cantidad de usuarios y cuyos modelos de negocio sean complejos, deberán cumplir las siguientes obligaciones:

1. Establecer y completar sistemas y estructuras de cumplimiento de la protección de la información personal de acuerdo con la normativa del Estado, y establecer un organismo independiente compuesto principalmente por miembros externos para supervisar las circunstancias de la protección de la información personal.
2. Respetar los principios de apertura, equidad y justicia; formular reglas de la plataforma; y aclarar los estándares para el tratamiento de la información personal por parte de los proveedores de productos o servicios dentro de la plataforma y sus obligaciones de protección de la información personal.
3. Dejar de prestar servicios a los proveedores de productos o servicios de la plataforma que infrinjan gravemente las leyes o normas administrativas en el tratamiento de la información personal.
4. Publicar periódicamente informes de responsabilidad social sobre la protección de la información personal y aceptar la supervisión de la sociedad.

Artículo 59: Las personas encargadas que acepten el tratamiento de información personal deberán, conforme a las disposiciones de esta Ley y las leyes y las normas administrativas

pertinentes, tomar las medidas necesarias para proteger la seguridad de la información personal que manejan, y ayudar a los responsables del tratamiento de información personal a cumplir con las obligaciones previstas en esta Ley.

8. **Capítulo VI: Departamentos que cumplen con los deberes y responsabilidades de protección de la información personal**

Artículo 60: El departamento de ciberseguridad e informatización del Estado es responsable de la planificación y coordinación global del trabajo de protección de la información personal y del trabajo de supervisión y gestión correspondiente. Los departamentos pertinentes del Consejo de Estado son responsables del trabajo de protección, supervisión y gestión de la información personal dentro de su respectivo ámbito de funciones y responsabilidades, conforme a las disposiciones de esta Ley y las leyes y las normas administrativas pertinentes. Las obligaciones y responsabilidades de los departamentos competentes de los gobiernos populares a nivel de condado y superior en materia de protección, supervisión y gestión de la información personal se determinan de acuerdo con las disposiciones pertinentes del Estado. Los departamentos mencionados en los dos párrafos anteriores se denominan todos como departamentos que cumplen con las obligaciones y responsabilidades de protección de la información personal.

Artículo 61: Los departamentos que cumplen con las obligaciones y responsabilidades de protección de la información personal cumplen con las siguientes obligaciones y responsabilidades de protección de la información personal:

1. Llevar a cabo la propaganda y la formación sobre la protección de la información personal, así como orientar y supervisar el trabajo de los responsables del tratamiento de información personal en materia de protección de la información personal.
2. Aceptar y tramitar los reclamos y denuncias relacionados con la protección de la información personal.
3. Organizar la evaluación de la situación de la protección de la información personal, como los procedimientos utilizados y la publicación de los resultados de la evaluación.
4. Investigar y abordar las actividades ilícitas de tratamiento de la información personal.
5. Otras obligaciones o responsabilidades previstas en las leyes o normas administrativas.

Artículo 62: El departamento de ciberseguridad e informatización del Estado coordina en general los siguientes trabajos de protección de la información personal por parte de los departamentos pertinentes:

1. Formular reglas y estándares concretos de protección de la información personal.
2. Formular reglas y estándares especializados de protección de la información personal para los responsables del tratamiento de información personal a pequeña escala y las nuevas tecnologías y aplicaciones para el tratamiento de la información personal sensible, el reconocimiento facial, la inteligencia artificial, etc.
3. Apoyar la investigación, el desarrollo y la adopción generalizada de la tecnología de autenticación de identidad electrónica segura y conveniente, y promover la construcción de servicios públicos de autenticación de identidad en línea.
4. Impulsar la construcción de sistemas de servicios para socializar la protección de la información personal y apoyar a las organizaciones pertinentes para iniciar servicios de evaluación y certificación de la protección de la información personal.
5. Perfeccionar los mecanismos de trabajo de reclamos y denuncias sobre la protección de la información personal.

Artículo 63: En el cumplimiento de las obligaciones y responsabilidades de la protección de la información personal, los departamentos que cumplen con las obligaciones y responsabilidades de la protección de la información personal pueden adoptar las siguientes medidas:

1. Entrevistar a las partes interesadas pertinentes e investigar las circunstancias relacionadas con las actividades de tratamiento de información personal.

2. Consultar y reproducir los contratos, registros y recibos de la parte interesada, así como otro material pertinente relacionado con las actividades de tratamiento de información personal.
3. Realizar inspecciones in situ y llevar a cabo investigaciones sobre presuntas actividades ilícitas de tratamiento de información personal.
4. Inspeccionar el equipo y los artículos relacionados con las actividades de tratamiento de información personal; y cuando haya pruebas de que el equipo o los artículos se utilizan para realizar actividades ilegales de tratamiento de información personal, tras informar por escrito al principal responsable de su departamento y recibir la aprobación, podrán precintarlos o confiscarlos.

Cuando los departamentos que cumplen con las obligaciones y responsabilidades de protección de la información personal cumplen con sus obligaciones y responsabilidades de acuerdo con la ley, las partes interesadas deben proporcionar asistencia y cooperación y no pueden obstruir ni impedir sus actuaciones.

Artículo 64: Cuando los departamentos que cumplen con las obligaciones y responsabilidades de protección de la información personal descubren que existen riesgos relativamente grandes en las actividades de tratamiento de la información personal o que se producen incidentes de seguridad de la información personal, pueden llevar a cabo una conversación con el representante legal del responsable del tratamiento de información personal o la persona principal responsable de acuerdo con las facultades y procedimientos reglamentarios, o exigir a los responsables del tratamiento de información personal que encomienden a instituciones especializadas la realización de auditorías de cumplimiento de sus actividades de tratamiento de la información personal. Los responsables del tratamiento de información personal adoptarán medidas de acuerdo con los requisitos para corregir el asunto y eliminar la vulnerabilidad.

Cuando los departamentos que cumplen con las obligaciones y responsabilidades de protección de la información personal descubran, en el curso de sus funciones, el tratamiento ilegal de información personal que presuntamente constituya un delito, deberán transferir rápidamente el asunto a las autoridades de seguridad pública para que lo procesen de acuerdo con la ley.

Artículo 65: Cualquier organización o persona tiene derecho a presentar un reclamo o denuncia sobre actividades ilegales de tratamiento de información personal ante los departamentos que cumplen con las obligaciones y responsabilidades de protección de la información personal. Los departamentos que reciban reclamos o denuncias deberán tramitarlas con prontitud y de acuerdo con la ley, y deben notificar a la parte reclamante o a la persona que haya presentado la denuncia el resultado de la tramitación.

Los departamentos que cumplen con las obligaciones y responsabilidades de protección de la información personal publicarán métodos de contacto para aceptar reclamos y denuncias.

Capítulo VII: Responsabilidad legal

Artículo 66: En caso de que la información personal se trate infringiendo esta Ley o se trate sin cumplir con las obligaciones de protección de información personal de acuerdo con las disposiciones de esta Ley, los departamentos que cumplen con las obligaciones y responsabilidades de protección de información personal deben ordenar la corrección, confiscar los ingresos ilegales y ordenar la suspensión provisional o el cese de la prestación de servicios de los programas de aplicación que traten ilegalmente la información personal; en caso de que se rechace la corrección, se impondrá adicionalmente una multa de no más de 1 millón de yuanes; el responsable directo y el resto del personal directamente responsable serán sancionados con una multa de entre 10 000 y 100 000 yuanes.

Cuando las circunstancias de los actos ilícitos mencionados en el párrafo anterior sean graves, los departamentos provinciales o de nivel superior que cumplan con las obligaciones y responsabilidades de protección de la información personal ordenarán la corrección, confiscarán los ingresos ilícitos e impondrán una multa de no más de 50 millones de yuanes, o el 5 % de los ingresos anuales. También pueden ordenar la suspensión de las actividades comerciales relacionadas o el cese de las mismas para su rectificación, e informar al departamento competente pertinente para la cancelación de las licencias administrativas correspondientes o la cancelación de las licencias comerciales. El responsable directo y el resto del personal directamente responsable serán sancionados con una multa de entre 100 000 y 1 millón de yuanes, y también se podrá decidir prohibirles ocupar cargos de director, supervisor, gerente de alto nivel o responsable de la protección de información personal durante un periodo determinado.

Artículo 67: Cuando se produzcan los actos ilícitos previstos en esta Ley, se introducirán en los archivos de créditos conforme a lo dispuesto en las leyes y las administrativas pertinentes, y se publicarán.

Artículo 68: Cuando los órganos del Estado no cumplan con las obligaciones de protección de la información personal previstas en esta Ley, sus órganos superiores o los departamentos que cumplan con las obligaciones y responsabilidades de protección de la información personal ordenarán su corrección; el responsable directo y otros responsables directos serán sancionados de acuerdo con la ley.

Cuando el personal de los departamentos que cumplen con las obligaciones de protección de la información personal, en el cumplimiento de sus obligaciones, comete una negligencia, abusa de su poder o incurre en favoritismo, pero no constituye todavía un delito, será sancionado de acuerdo con la ley.

Artículo 69: Cuando el tratamiento de la información personal infrinja los derechos e intereses de la información personal y provoque un daño, y los responsables del tratamiento de información personal no puedan demostrar que no son culpables, deberán asumir la indemnización y otras responsabilidades por la infracción.

En la cláusula anterior, la responsabilidad de indemnizar por la infracción se determinará en función de la consiguiente pérdida para la persona o de los beneficios resultantes para el responsable del tratamiento de la información personal. Cuando la pérdida para la persona y los beneficios del responsable del tratamiento de la información personal sean difíciles de determinar, se determinará la indemnización de acuerdo con las condiciones prácticas.

Artículo 70: En caso de que los responsables del tratamiento de información personal infrinjan las disposiciones de la presente Ley, vulnerando los derechos y beneficios de muchas personas, las fiscalías populares, las organizaciones de consumidores designadas por ley y las organizaciones designadas por el departamento de ciberseguridad e informatización del Estado podrán presentar una demanda ante un tribunal popular de acuerdo con la ley.

Artículo 71: Cuando la infracción de las disposiciones de esta Ley constituya una infracción de la gestión de la seguridad pública, se impondrán sanciones de gestión de la seguridad pública de acuerdo con la ley; cuando constituya un delito, se investigará la responsabilidad penal de acuerdo con la ley.

Capítulo VIII: Disposiciones complementarias

Artículo 72: La presente Ley no se aplica a las personas físicas responsables del tratamiento de información personal para asuntos personales o familiares.

Cuando la ley contenga disposiciones sobre el tratamiento de información personal por parte de los gobiernos populares a todos los niveles y sus departamentos y organizaciones pertinentes que realicen actividades de gestión estadística y de archivos, se aplicarán dichas disposiciones.

Artículo 73: Los siguientes términos utilizados en esta Ley se definen como se indica a continuación:

1. "Responsable del tratamiento de información personal" se refiere a las organizaciones y personas que, en las actividades de tratamiento de información personal, deciden de forma autónoma los fines y los métodos de tratamiento.
2. "Toma de decisiones automatizada" se refiere a la actividad de utilizar programas informáticos para analizar o evaluar automáticamente los comportamientos, hábitos, intereses o aficiones personales, o la situación financiera, de salud, crediticia o de otro tipo, y tomar decisiones [basadas en ello].
3. "Desidentificación" se refiere al proceso de tratamiento de la información personal para garantizar la imposibilidad de identificar a personas físicas concretas sin el apoyo de información adicional.
4. "Anonimización" se refiere al proceso de tratamiento de la información personal para que sea imposible distinguir a personas físicas concretas y sea imposible de restaurar.

Artículo 74: Esta Ley entrará en vigencia el lunes 1 de noviembre de 2021.

Apéndice 6
Normas de protección de la infraestructura crítica de información.[35] (Extractos)

Artículo 2: La infraestructura crítica de información, tal como se menciona en estas normas, se refiere a la infraestructura de red importante, los sistemas de información, etc., en industrias y sectores importantes como los servicios públicos de telecomunicaciones e información, la energía, el transporte, el agua, las finanzas, los servicios públicos, la administración electrónica, la ciencia, la tecnología y la industria de la defensa nacional, etc., así como en los casos en que su destrucción, la pérdida de funcionalidad o la fuga de datos puede perjudicar gravemente la seguridad nacional, la economía nacional y el sustento de las personas o el interés público.
Artículo 8: Los departamentos competentes y los departamentos de supervisión y gestión de las industrias y sectores importantes mencionados en el Artículo 2 de estas Normas son los departamentos responsables de los trabajos de protección de la seguridad de las infraestructuras críticas de información (en adelante, abreviados como "departamentos de trabajos de protección").
Artículo 9: Los departamentos de trabajos de protección deben formular normas de identificación de infraestructuras críticas de información en integración con la situación real de sus industrias y sectores, y comunicarlas al departamento de seguridad pública del Consejo de Estado para su archivo.
A la hora de formular las normas de identificación, se tendrán en cuenta principalmente los siguientes factores:

1. El grado de importancia de la infraestructura de red, el sistema de información, etc., para las actividades críticas y fundamentales de la industria o el sector.
2. El grado de daño que podría ocasionar la infraestructura de red, el sistema de información, etc., si se destruye, pierde funcionalidad o se filtran sus datos.
3. La influencia asociada en otras industrias y sectores.

Artículo 18: Cuando se produzcan incidentes importantes de ciberseguridad o se descubran amenazas importantes de ciberseguridad en la infraestructura crítica de información, los operadores informarán del asunto al departamento de trabajo de protección y a las autoridades de seguridad pública de acuerdo con la normativa pertinente.
En caso de que la infraestructura crítica de información deje de funcionar por completo o sus funciones principales se vean obstaculizadas, se filtre información básica nacional u otros datos importantes, se filtre información personal a una escala relativamente grande, se produzca un daño económico relativamente grande, se difunda información ilegal a una escala relativamente grande, o se produzcan otros incidentes de ciberseguridad especialmente graves, o se descubran amenazas de ciberseguridad especialmente graves, el departamento de trabajo de protección, después de recibir el informe, informará rápidamente del asunto al departamento nacional de ciberseguridad e informatización y al departamento de seguridad pública del Consejo de Estado.

[35] Orden del Consejo de Estado de la República Popular China n.º 745, del 30 de julio de 2021, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1, según traducción de DigiChina: https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept