تقرير خاص بدولة:
مبادرات وقوانين الصين ذات الصلة بالإنترنت

ڤيني ماركوڤسكي وأليكسي تريبخالين
31 كانون الثاني 2022
GE-010 (تحديث)

ICANN

قائمة المحتويات

مقدمة

تغطي هذه الدراسة مبادرات وقوانين/أنظمة السياسات ذات الصلة بالإنترنت والتي طرحتها الصين في الفترة ما بين 16 ديسمبر/كانون الأول 2015 و5 نوفمبر/تشرين الثاني 2021؛ بما يضمن حصول مجتمع ICANN على المعلومات اللازمة لتطوير فهم أفضل حول المداولات الجارية في الأمم المتحدة والاتحاد الدولي للاتصالات وغير ذلك من الوكالات التابعة للأمم المتحدة.

ويعتبر هذا جزءًا من سلسلة دورية من التقارير الخاصة بكل بلد والتي تقدم لمحة عامة حول الأنشطة ذات الصلة بمنظومة الإنترنت ومهمة ICANN. كما أن مراقبة مثل هذه المبادرات تمثل مسئولية أساسية على عاتق فريق مشاركة الحكومات والمنظمات الدولية الحكومية (GE) في منظمة ICANN (والمشار إليها بلفظ منظمة ICANN) من حيث إبقاء مجتمع ICANN الأوسع على علم ودراية بالقضايا ذات الأهمية بخصوص إنترنت عالمي واحد وقابل للتشغيل المتبادل ونظام المعرّفات الفريد الخاص به.[1]

كما هو الحال في الأبحاث السابقة لقسم المشاركة الحكومية، تستند التحليلات إلى نصوص المصدر الأولية المتعلقة بسياسات وتقنيات الإنترنت، مثل نظام أسماء النطاقات (DNS)، وعناوين بروتوكول الإنترنت (IP)، ومعلمات البروتوكولات، على سبيل المثال لا الحصر. بالإضافة إلى ذلك، يعتمد هذا البحث على النصوص ذات الصلة والبيانات والأحكام القانونية/التشريعية حول مواقف الصين حيال نفس القضايا في الأمم المتحدة (U.N) والاتحاد الدولي للاتصالات (ITU) وأيضًا على المستوى المحلي.

بيانات ومبادرات السياسة الأجنبية في الصين

في 16 ديسمبر/كانون الأول 2015، وفي كلمة ألقيت في مراسم افتتاح المؤتمر الدولي الثاني للإنترنت في مدينة أووجن[2]، قال رئيس جمهورية الصين الشعبية، شي جين بينغ: "...يجب على المجتمع الدولي دعم الحوار والتعاون على أساس الاحترام والثقة المتبادلين، وتعزيز تحول نظام حوكمة الإنترنت العالمي، والعمل معًا من أجل دعم ومؤازرة فضاء إلكتروني سلمي وآمن ومنفتح وتعاوني إضافة إلى تفعيل نظام حوكمة إنترنت عالمي متعدد الأطراف وقائم على أسس الديمقراطية والشفافية".[3]

ولتحقيق ذلك، فقد شدد الرئيس شي على أن "احترام السيادة الإلكترونية" لكل دولة على حدة، مع المشاركة في "حوكمة الفضاء الإلكتروني الدولي على قدم المساواة" أمر ضروري باعتباره أحد المبادئ الإرشادية الأربعة.[4] وأضاف الرئيس شي كذلك قائلاً "يجب أن تتخذ الحوكمة الدولية للفضاء الإلكتروني منهجًا متعدد الأطراف مع المشاركة متعددة الأطراف. ويجب أن تقوم على أساس التشاور فيما بين جميع الأطراف، مع الاستفادة القصوى من دور مختلف الجهات الفاعلة، بما في ذلك الحكومات والمنظمات الدولية وشركات الإنترنت والمجتمعات التكنولوجية والمؤسسات غير الحكومية والمواطنين الأفراد. ويجب الابتعاد عن الأحادية في هذا الصدد. ويجب ألا تتخذ القرارات من جانب طرف واحد يكون هو من يتولى اتخاذ القرارات أو القليل من الأطراف التي تجري مناقشات فيما بينها. ويجب على جميع الدول تعزيز وتطوير الاتصال والحوار، وتحسين تبادل الآراء والأفكار وآلية للتشاور حول الفضاء الإلكتروني، بالإضافة إلى دراسة وصياغة قواعد حوكمة الإنترنت العالمية، بحيث يصبح نظام حوكمة الإنترنت العالمي أكثر عدلاً ومعقولية وبحيث يعكس طموحات ومصالح غالبية الدول بطريقة أكثر اتزانًا".[5]

في 7 مارس/آذار 2016، وخلال جلسة اللجنة الاستشارية الحكومية (GAC) التابعة لـ ICANN، شدد ممثل الصين على أن "المبادئ الأربعة والمقترحات الخمسة" التي طرحها الرئيس شي في المؤتمر العالمي الثاني للإنترنت لعام 2016 في أووجن "توفر لنا (يتعذر تمييز الصوت) قدرًا من التفكير ومواقف الصين حيال مسألة حوكمة الإنترنت".[6]

---

[1] "خطط ICANN التشغيلية والمالية"، الصفحة 47، منظمة ICANN، في ديسمبر/كانون الأول 2020، https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf.

[2] يعقد المؤتمر العالمي للإنترنت في مدينة أووجن، بمقاطعة شيجيانغ، سنويًا من خلال إدارة الفضاء الإلكتروني بالصين وحكومة شيجيانغ الشعبية الإقليمية http://www.wuzhenwic.org/2020-10/15/c_547699.htm. تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: https://www.wicwuzhen.cn/.

[3] تعليقات صاحب الفخامة. شي جين بينغ، رئيس جمهورية الصين الشعبية، في مراسم افتتاح المؤتمر الثاني للإنترنت العالمي، أووجن، في 16 ديسمبر/كانون الأول 2015 https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.

[4] تعليقات صاحب الفخامة. شي جين بينغ.

[5] تعليقات صاحب الفخامة. شي جين بينغ

[6] اجتماع مراكش - الاجتماع الحكومي رفيع المستوى للجنة الاستشارية الحكومية GAC يوم الإثنين الموافق 7 مارس/آذار 2016، اجتماع ICANN55 | مراكش، المغرب، الصفحة 86 https://gac.icann.org/transcripts/public/transcript-icann55-gac-hl-governmental-meeting-2016-03-07.pdf.

في 27 أبريل/نيسان 2016، أصدرت الصين استراتيجيتها القومية للفضاء الإلكتروني،[7] تشرح فيها أهمية "تقوية التعاون الدولي في الفضاء الإلكتروني" بالنسبة للدولة. وفي سبيل هذه الغاية، توضح الاستراتيجية بالتفصيل أن هذا التعاون يجب "أن يعزز من إصلاح نظام حوكمة الإنترنت العالمية" وأيضًا "تدويل إدارة عناوين الإنترنت وخوادم أسماء النطاقات وغير ذلك من الموارد الأساسية". كما عبّرت الاستراتيجية كذلك عن دعم "لعب الأمم المتحدة دورًا قياديًا، وتعزيز تشكيل معايير دولية من أجل الفضاء الإلكتروني تعترف بها جميع الأطراف اعترافًا عامًا، بالإضافة إلى معاهدة دولية حول مكافحة الإرهاب في الفضاء الإلكتروني، وآليات كاملة للمساعدة القضائية للقضاء على الجريمة الإلكترونية، وتعميل التعاون الدولي في بعض النواحي مثل السياسات والقوانين، والابتكار التكنولوجي، والمعايير والأعراف، والاستجابة للطوارئ، وحماية البنية التحتية للمعلومات الأساسية، إلخ". كما نادت الاستراتيجية "بوضع منظومة دولية متعددة الأطراف تتميز بالديمقراطية والشفافية لحوكمة الإنترنت".

في 2 مارس/آذار 2017، نشرت الصين الاستراتيجية الدولية للتعاون في الفضاء الإلكتروني.[8] وتنص على أن "الصين سوف تدفع باتجاه إصلاح مؤسسي لمنتدى حوكمة الإنترنت بالأمم المتحدة من أجل تمكينه من تأدية دور أكبر في حوكمة الإنترنت، وتقوية قدرته على اتخاذ القرارات، وتأمين تمويل ثابت، وطرح إجراءات منفتحة وشفافية في اختيار أعضائها وتقديم التقارير". كما تؤكد الاستراتيجية الدولية للتعاون في الفضاء الإلكتروني أيضًا على أن الصين "سوف تشارك في المناقشات الدولية بخصوص التوزيع العادل والإدارة لموارد الإنترنت الحيوية"، وأنها "سوف تعزز بقوة من إصلاح ICANN لجعلها مؤسسة دولية مستقلة فعلية، وزيادة مستويات التمثيل الخاصة بها وضمان مستوى أكبر من الانفتاح والشفافية في اتخاذها للقرارات وفي تعاونها".[9]

في 20 أبريل/نيسان 2018، وفي المؤتمر القومي للأمن الإلكتروني والعمل المعلوماتي في بكين، قال الرئيس شي أنه "بعد ذلك في المستقبل، فإن إصلاح منظومة حوكمة الإنترنت العالمية هو الاتجاه العام وأنه يمثل طموحًا مشتركاً". وأردف قائلاً أن "حوكمة الفضاء الإلكتروني الدولي يجب أن تصر على المشاركة متعددة الأطراف ومشاركة أصحاب المصلحة المتعددين، بما يوفر أدوارًا لجميع أنواع الجهات الفاعلة، بما في ذلك الحكومات والمنظمات الدولية ومؤسسات الإنترنت والمجتمع الفني والمؤسسات المدنية والمواطنين الأفراد. ويجب علينا أيضًا تعزيز حوكمة الفضاء الإلكتروني ضمن إطار عمل الأمم المتحدة، والقيام أيضًا بعمل جيد في إتاحة الفرصة للدور الإيجابي لجميع أنواع الجهات الفاعلة غير الحكومية".[10]

وفي 9 يوليو/تموز 2019/ أشارت الصين فيما قدمته إلى مجموعة العمل مفتوحة النهاية (OEWG) حول التطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي، إلى: "يجب على الدول أن تعمل معًا من أجل إنشاء نظام حوكمة إنترنت متعدد الأطراف وديمقراطي وشفاف. كما أن المؤسسة المنوط بها إدارة الموارد الحيوية مثل خوادم الجذر يجب أن تكون مستقلة استقلالاً حقيقيًا عن أي سيطرة أو رقابة للدولة من أجل ضمان المشاركة الواسعة وتضامن جميع الدول في اتخاذ القرارات".[11]

قدمت الصين في أبريل/نيسان 2020 المشاركة التالية في المسودة المسبقة لتقرير مجموعة العمل مفتوحة النهاية بالأمم المتحدة، والذي أكدت فيه على ما يلي: "نظرًا لمحدودية ما لدينا من وقت، ينبغي أيضًا توجيه الانتباه لتجنب إدخال مفاهيم لم تحظ إلى الآن بتوافق عالمي (كلفظ "النواة العامة" على سبيل المثال) في التقرير"، وأيضًا: "خلال الجلستين السابقتين، طرحت أطراف -شملت الصين- عشرات

---

[7] هيئة حقوق النشر والوسائط بالصين، الاستراتيجية القومية لأمن الفضاء الإلكتروني، تم التحديث في 27 ديسمبر/كانون الأول 2016، https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/. تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.

[8] الاستراتيجية الدولية للتعاون في الفضاء الإلكتروني، جريدة China Daily، في 2 مارس/آذار 2017، https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm. تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.china.org.cn/chinese/2017-03/07/content_40424606.htm.

[9] الاستراتيجية الدولية للتعاون في الفضاء الإلكتروني، جريدة China Daily، في 2 مارس/آذار 2017.

[10] دار New America، ترجمة: كلمة شي جين بينغ في 20 أبريل/نيسان في المؤتمر القومي للأمن الإلكتروني والعمل المعلوماتي، 30 أبريل/نيسان 2018، https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/. تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm.

[11] ملاحظات الصين المقدمة إلى مجموعة العمل مفتوحة النهاية المعنية بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي، 7 يوليو/تموز 2019. https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

المقترحات البناءة بشأن قضايا مثل السيادة السيبرانية، وأمن سلسلة التوريد، وحماية البنية التحتية الحيوية، والامتناع عن العقوبات أحادية الجانب، ومكافحة الإرهاب السيبراني. ومن المؤمل أن يتم دمج هذه المقترحات في التقرير".[12]

في 8 سبتمبر/أيلول 2020، نشرت وزارة الخارجية الصينية مبادرة عالمية حول أمن البيانات، وتناولت فيه ضرورة تحقيق الدول تعاونًا أفضل في مجال أمن البيانات والجريمة الإلكترونية، إلخ. وتقترح الوثيقة بأن "تجري الحكومات والمنظمات الدولية وشركات تقنية المعلومات والاتصالات[13] والمجتمعات التكنولوجية والمنظمات المدنية والأفراد وجميع القطاعات الأخرى جهودًا لتعزيز أمن المعلومات بموجب مبادئ التشاور الموسع والإسهام التضامني والمزايا المشتركة". وتدعُ الوثيقة الدول إلى عدة أمور من بينها على سبيل المثال لا الحصر "معالجة أمن البيانات بطريقة شاملة وموضوعية وقائمة على الأدلة، بالإضافة إلى الحفاظ على سلسلة توريد منفتحة وآمنة ومستقرة لمنتجات وخدمات تقنية المعلومات والاتصالات العالمية".[14]

في مارس/آذار 2021، اجتاز مؤتمر "الجلستين" السنوي التشريعي الخطة الخمسية الرابعة عشر ورؤية 2035، والذي يؤكد الفصل 18 (إنشاء منظومة رقمية جيدة) القسم 4 (تعزيز إنشاء مجتمع بمستقبل مشترك في فضاء الإنترنت) على ما يلي: "تطوير الحوار والتعاون الدولي في فضاء الإنترنت، وتعزيز صياغة قواعد الفضاء الإلكتروني والرقمي الدولية ضمن الأمم المتحدة باعتبارها القناة الرئيسية وميثاق الأمم المتحدة باعتباره المبادئ الأساسية. تعزيز إنشاء منظومة عالمية لحوكمة الإنترنت متعددة الأطراف وديمقراطية وشفافة، إضافة إلى إنشاء بنية تحتية للشبكات أكثر عدلاً ومعقولية مع آلية لحوكمة الموارد".[15]

وبتاريخ 10 مارس/آذار 2021، وخلال مداولات مجموعة العمل مفتوحة النهاية في الأمم المتحدة، أكدت الصين على ما يلي: "ينبغي أن تشارك الدول في إدارة وتوزيع موارد الإنترنت الدولية على قدم المساواة".[16]

أصدرت كل من الصين وروسيا الاتحادية بيانًا مشتركًا في 29 يونيو/حزيران 2021 بالموافقة على تمديد "معاهدة حسن الجوار والتعاون الودي" الثنائية الحالية. وقد اتفقا في البيان المشترك على "تشديد وتأكيد التزامهما بتقوية أمن المعلومات الدولي على المستويين الثنائي والمتعدد" وأكدا على "اتفاقهما فيما يخص المشكلات ذات الصلة بحوكمة الإنترنت، والتي تشتمل على ضمان حصول جميع الدول على حقوق متساوية في المشاركة في حوكمة الشبكات العالمية، وزيادة دورها في هذه العملية والحفاظ على الحق السيادي للدول في تنظيم الشريحة الوطنية في الإنترنت. وتؤكد روسيا والصين على الحاجة إلى تعزيز دور الاتحاد الدولي للاتصالات وتقوية تمثيل الدولتين في هيئاتها الحاكمة".[17]

---

[12] مساهمة الصين في المسودة الأولية لتقرير مجموعة العمل مفتوحة النهاية، 16 أبريل/نيسان 2020 (مؤرخة كما في خصائص ملف PDF)، https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf.

[13] ICT – تقنية المعلومات والاتصالات، UNTERM – قاعدة مصطلحات الأمم المتحدة، https://unterm.un.org/unterm/display/record/imo/na?OriginalId=551772be82184a22adaeb86841e335e6.

[14] المبادرة العالمية لأمن البيانات، موقع وزارة الخارجية الصينية على الويب، 8 سبتمبر/أيلول 2020، https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202009/t202009 08_599773.html وتطلق الصين مبادرة أمن البيانات العالمية من أجل معارضة تسييس قضايا أمن البيانات، وكالة رويترز، 7 سبتمبر/أيلول 2020، https://www.reuters.com/article/wangyi-global-digital-security-0908-idCNKBS25Z0AJ.
تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: https://www.fmprc.gov.cn/chn/pds/ziliao/tytj/t1827469.htm.

[15] غوانشا، "الخطة الخمسية الرابعة عشرة"، وتوضيح الأهداف طويلة الأجل للعام 2035 (النص الكامل)، 13 مارس/آذار 2021، https://www.guancha.cn/politics/2021_03_13_583945_5.shtml.

[16] مجموعة العمل مفتوحة النهاية المعنية بالتطورات في مجال المعلومات والاتصالات في سياق الأمن الدولي، الجلسة الرئيسية الثالثة، 8-12 مارس/آذار 2021، ملخص رئيس مجموعة العمل مفتوحة النهاية، ورقة غرفة المؤتمر، في 10 مارس/آذار 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.

[17] سفارة روسيا الاتحادية لدى المملكة المتحدة وإيرلندا الشمالية وبريطانيا العظمي، البيان المشترك لروسيا الاتحادية وجمهورية الصين الشعبية حول الذكرى العشرين لمعاهدة حسن الجوار والتعاون الودي بين روسيا الاتحادية وجمهورية الصين الشعبية، 28 يونيو/حزيران 2021، https://www.rusemb.org.uk/fnapr/7007.
تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.xinhuanet.com/2021-06/28/c_1127606620.htm.

بتاريخ 1 نوفمبر/تشرين الثاني 2021، قدمت روسيا الاتحادية عرضًا لمسودة نصها[18] حول اتفاقية مكافحة الجريمة الإلكترونية المقترحة من الأمم المتحدة وأعلن أن النص كان برعاية مشتركة من الصين.[19،20]

في 5 نوفمبر/تشرين الثاني 2021، طرحت الصين مقترحاتها على الجلسة الأولى للجنة المخصصة (AHC) بالأمم المتحدة.[21] وقد أكدت على سبيل المثال لا الحصر على ما يلي: "الدول الأعضاء مطالبون بتجريم التطفل وتدمير منشآت أو أنظمة أو بيانات تقنية المعلومات والاتصالات أو البنية التحتية الحيوية للمعلومات. وقد يشتمل ذلك على الوصول غير القانوني إلى أنظمة معلومات الكمبيوتر، والتدخل غير القانوني في أنظمة معلومات الكمبيوتر، والاستحواذ غير القانوني على بيانات الكمبيوتر، والتدخل غير القانوني في بيانات الكمبيوتر، وانتهاك البنية التحتية الحيوية للمعلومات، إلخ".

البيانات والتشريعات والقوانين المحلية

في 1 يوليو/تموز 2015، تم تمرير قانون الأمن القومي. ونصه كالتالي (بالمادة 59): "تؤسس الدولة أنظمة وآليات لإدارة مراجعة الأمن القومي والإشراف عليه، من خلال إجراء مراجعة للأمن القومي لكل من الاستثمار التجاري والبنود الخاصة والتقنيات، ومنتجات وخدمات الإنترنت وتكنولوجيا المعلومات، والمشروعات التي تنطوي على مسائل الأمن القومي، بالإضافة إلى المسائل والأنشطة الرئيسية الأخرى ذات الأثر أو التي قد يكون لها أثر على الأمن القومي".[22] وتنص المادة 25 من القانون على ما يلي: تؤسس الدولة شبكة قومية ونظامًا لحماية أمن المعلومات [...] بزيادة إدارة الشبكة والحفاظ على سيادة الفضاء الإلكترونين ومصالح الأمن والتنمية".

في 1 يونيو/حزيران 2017، تم تنفيذ قانون الأمن الإلكتروني (CSL). وهو ينص على أن الدولة مسئولة عن "تعزيز فضاء إلكتروني سلمي وآمن ومنفتح وتعاوني، مع تأسيس نظام حوكمة للإنترنت يتسم بالتعددية والديمقراطية والشفافية". كما ينص القانون أيضًا على حكم بتخزين بيانات الإنترنت محليًا في "الأراضي الصينية". وتحدد المادة 31 من القانون نطاق البنية التحتية للمعلومات الأساسية بأنها تشتمل على "نظام حماية متعدد الطبقات للأمن الإلكتروني مخصص لخدمات الاتصالات والمعلومات العامة والطاقة والمواصلات والموارد المائية والتمويل والخدمات العامة والحكومة الإلكترونية والبنية التحتية الأساسية الأخرى للمعلومات". وتشير المادة 37 من القانون إلى أنه، "في الحالات التي يكون من الضروري حقًا توفير ذلك [المعلومات الشخصية، البيانات الهامة] خارج البر الرئيسي بسبب متطلبات واشتراطات الأعمال، فيجب عليهم [مشغلي البنية التحتية للمعلومات الأساسية] اتباع التدابير التي تضامنت في صياغتها إدارة الأمن الإلكتروني والمعلوماتية في البلاد والإدارات المعنية في مجلس الدولة من أجل إجراء تقييم للأمن؛ وفي الحالات التي تنص فيها القوانين والأنظمة الإدارية على خلاف ذلك، فيجب اتباع تلك الأحكام".[23] (تم توفير الأحكام ذات الصلة في الملحق 1 بهذا البحث).

وفي 24 أغسطس/آب 2017، نشرت وزارة الصناعة وتكنولوجيا المعلومات الصينية (MIIT) التدابير المنقحة بخصوص إدارة أسماء نطاقات الإنترنت.[24] (تم توفير الأحكام ذات الصلة في الملحق 2 بهذا البحث).

---

[18] اتفاقية الأمم المتحدة بخصوص مكافحة استخدم تقنيات المعلومات والاتصالات للأغراض الإجرامية، 27 يوليو/تموز 2021، https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf.

[19] اتفاقية جديدة للأمم المتحدة ضد الجريمة الإلكترونية على وشك البدء، fm4.orf.at، https://fm4.orf.at/stories/3019118/.

[20] كونوستانتينيوس كومايتس، حساب تويتر، 1 نوفمبر/تشرين الثاني 2021 وفي 19 يناير/كانون الثاني 2022، https://twitter.com/i/web/status/1455217317504327683.

[21] مقترحات الصين حول النطاق والأهداف والهيكل (العناصر) في اتفاقية الأمم المتحدة بخصوص مكافحة استخدام تقنيات المعلومات والاتصالات لأغراض إجرامية: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf.

[22] ترجمة القانون الصيني، قانون الأمن القومي لجمهورية الصين الشعبية، 1 يوليو/تموز 2015، https://www.chinalawtranslate.com/en/2015nsl/. تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm

[23] دار New America، ترجمة: قانون الأمن الإلكتروني لجمهورية الصين الشعبية (يسري العمل به بتاريخ 1 يونيو/حزيران 2017)، 29 يونيو/حزيران 2018، https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

[24] وزارة الصناعة وتكنولوجيا المعلومات، تدابير إدارة أسماء نطاقات الإنترنت، 24 أغسطس/آب 2017 https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/.

وفي 29 يناير/كانون الثاني 2018، أعلنت وزارة الصناعة وتكنولوجيا المعلومات -وعلى أساس المادة 5 من تدابيرها الجديدة وفقًا لما ذكرنا أعلاه، نظام أسماء نطاقات الإنترنت الصينية.[25] (تم توفير الأحكام ذات الصلة في الملحق 3 بهذا البحث).

وفي 13 يونيو/حزيران 2019، فإن تدابير تقييم الأمن والنقل العابر للحدود للمعلومات الشخصية المقترح في المادة 2: "يلتزم مشغلو الشبكات الذين يوفرون معلومات شخصية يتم جمعها في مسيرة العمليات داخل منطقة البر الرئيسي لجمهورية الصين الشعبية (والمشار إليها فيما يلي هنا بلفظ نقل المعلومات الشخصية للخارج)، بإجراء عمليات تقييم للأمن بما يتفق مع هذه التدابير. وإذا ما تقرر من خلال تقييم الأمن أن عملية نقل المعلومات الشخصية للخارج قد تؤثر على الأمن القومي أو تضر بالمصلحة العامة، أو أن من الصعوبة توفير الحماية الفعالة لأمن المعلومات الشخصية، فلا يجوز أن تغادر هذه المعلومات البلاد. وفي الحالات التي يكون فيها للدولة أحكام أخرى فيما يخص عملية نقل المعلومات الشخصية للخارج، تسري تلك الأحكام".[26]

وفي 10 يونيو/حزيران 2021، اعتمد الاجتماع التاسع والعشرون للجنة الدائمة للائتلاف الشعبي القومي الثالث عشر قانون أمن البيانات (DSL).[27] (راجع النصوص ذات الصلة من القانون في الملحق 4 المرفق بهذا البحث).

في 30 يوليو/تموز 2021، تم إعلان النظام الجديد الخاص بحماية أمن البنية التحتية للمعلومات الحرجة (بعد اعتماد مجلس دولة الصين في 27 أبريل/نيسان 2021). وتحدد الأنظمة نطاق بنية المعلومات الحرجة، وتقدم أحكامًا "للصناعات والقطاعات" من أجل الاستفاضة في تفصيل النطاق، وتحديد متطلبات واشتراطات الإبلاغ الخاصة بهذه الوكالات إلى سلطات المعلومات المركزية في حالة "حوادث الأمن الإلكتروني شديدة الخطورة"، مثل التسرب "الكبير نسبيًا" للمعلومات الشخصية.[28] جرى العمل بالأنظمة في 1 سبتمبر/أيلول 2021. (المواد ذات الصلة في النظام موجودة بالملحق 6 بهذا البحث).

وفي 20 أغسطس/آب 2021، مررت اللجنة الدائمة بالمجلس الشعبي القومي التابع لجمهورية الصين الشعبية قانون حماية المعلومات الشخصية (PIPL). وقد دخل القانون حيز التنفيذ في 1 نوفمبر/تشرين الثاني 2021. وقد "تمت صياغة القانون [...] من أجل حماية حقوق ومصالح المعلومات الشخصية، ووضع معايير لأنشطة التعامل مع المعلومات الشخصية، وتعزيز الاستخدام الرشيد للمعلومات الشخصية". تحظى المعلومات الشخصية "للشخصيات الطبيعية بالحماية القانونية؛ حيث لا يجوز لأي مؤسسة أو فرد انتهاك حقوق ومصالح المعلومات الشخصية للشخصيات الطبيعية". علمًا بأن هذا القانون "ينطبق على المنظمات والأفراد الذي يتناولون أنشطة المعلومات الشخصية للأشخاص الطبيعيين ضمن حدود جمهورية الصين الشعبية". "وفي حالة وجود أي من الظروف التالية في أنشطة

تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.cac.gov.cn/2017-09/28/c_1121737753.htm.

[25] رابط URL الموصل إلى المصدر الصيني لا يعمل اعتبارًا من 19 أغسطس/آب 2021، باللغة الإنجليزية: https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/.
تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://xn--eqrt2g.xn--vuq861b/#.

[26] دار New America، ترجمة: مسودة قواعد جديدة حول نقل المعلومات الشخصية عبر الحدود خارج الصين، 13 يونيو/حزيران 2019، "تدابير تقييم أمن نقل المعلومات الشخصية خارج البلاد (مسودة للتعليق)"، 13 يونيو/حزيران 2019، https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/.
تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.cac.gov.cn/2019-06/13/c_1124613618.htm.

[27] القرصنة الداخلية، ترجمة كوفينغتون غير الرسمية: تدابير التقييم الأمني لنقل المعلومات الشخصية عبر الحدود (مسودة للتعليق)، 13 يونيو/حزيران 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، دار New America، ترجمة: مسودة قواعد جديدة حول نقل المعلومات الشخصية عبر الحدود خارج الصين، "تدابير تقييم أمن نقل المعلومات الشخصية خارج البلاد (مسودة للتعليق)"، يونيو/حزيران 2019 https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/.
تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.cac.gov.cn/2019-06/13/c_1124613618.htm.

[28] أمر مجلس الدولة بجمهورية الصين الشعبية رقم 745، بتاريخ 30 يوليو/تموز 2021، http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1، حسب ترجمة DigiChina: https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept.

التناول خارج حدود جمهورية الصين الشعبية للمعلومات الشخصية الخاصة بالأشخاص الطبيعيين ضمن حدود جمهورية الصين الشعبية، فإن هذا القانون يسري أيضًا" في حالات (1) "عندما يكون الغرض هو توفير منتجات أو خدمات إلى أشخاص طبيعيين داخل الحدود"، و(2) "عند تحليل أو تقييم أنشطة الأشخاص الطبيعيين داخل الحدود"، و(3) الظروف الأخرى المنصوص عليها في القوانين أو الأنظمة الإدارية". كما يحدد القانون كذلك المعلومات الشخصية وما هو مشمول في معالجتها: "المعلومات الشخصية هي جميع أنواع المعلومات التي يتم تسجيلها عن طريق الوسائل الإلكترونية أو غيرها ذات الصلة بالأشخاص الطبيعيين أصحاب الهويات المعروفة أو التي يمكن التعرف عليها، ولا تشمل المعلومات بعد التعامل مع تجهيل الهوية. ويشمل التعامل مع المعلومات الشخصية جمع المعلومات الشخصية وتخزينها واستخدامها ومعالجتها ونقلها وتوفيرها ونشرها وحذفها، إلخ".[29] (النص الكامل للقانون موجود في الملحق 5 بهذا البحث).

الخاتمة

تشارك الصين بنشاط في جميع المناقشات ذات الصلة بالمسائل السيبرانية في الأمم المتحدة. ولمساهمات الصين الدولية والقومية احتمالية التعرض لمهمة ورسالة ICANN. وسوف تواصل منظمة ICANN من خلال قسم المشاركة الحكومية توفير المعلومات إلى مجتمع ICANN عندما تكون تلك البيانات أو المقترحات ذات صلة بالحوكمة الفنية للإنترنت أو بمهمة ICANN.

[29] قانون حماية المعلومات الشخصية بجمهورية الصين الشعبية (تم تمريره في الاجتماع الثلاثين للجنة الدائمة التابعة للمؤتمر الشعبي القومي الثالث عشر في 20 أغسطس 2021)، http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

الملحق 1
قانون الأمن الإلكتروني لجمهورية الصين الشعبية[30]

تم تمريره في 6 نوفمبر/تشرين الثاني 2016. سري العمل به في 1 يونيو/حزيران 2017.

1. قائمة المحتويات

الفصل الأول: الأحكام العامة

المادة 1: تمت صياغة هذا القانون من أجل: ضمان الأمن الإلكتروني وضمان سيادة الفضاء الإلكتروني والأمن القومي، والمصالح الاجتماعية والعامة؛ وحماية الحقوق والمصالح القانونية للمواطنين والشخصيات الاعتبارية والمؤسسات الأخرى؛ وتعزيز التطور الصحي للتحول المعلوماتي لكل من الاقتصاد والمجتمع.

المادة 2: يسري العمل بهذا القانون على إنشاء وتشغيل وصيانة واستخدام الشبكات، بالإضافة إلى الإشراف على الأمن الإلكتروني وإدارته ضمن حدود دولة جمهورية الصين الشعبية.

المادة 3: تصر الدولة على التأكيد العادل على الأمن الإلكتروني وتطوير المعلوماتية، كما تلتزم بمبادئ الاستخدام النشط والتطور العلمي والإدارة بما يتفق مع القانون وضمان وحماية الأمن. تطوّر الدولة من إنشاء البنية التحتية للشبكات والاتصال البيني، كما تشجع على الابتكار وتطبيق تكنولوجيا الشبكات، وتدعم رعاية الأفراد المؤهلين في مجال الأمن الإلكتروني، وتؤسس نظامًا كاملاً لحماية الأمن الإلكتروني، كما ترفع من الطاقة الاستيعابية لحماية الأمن الإلكتروني.

المادة 4: تصيغ الدولة وتحسّن باستمرار من استراتيجية الأمن الإلكتروني، وتوضح المتطلبات الأساسية والأهداف الأولية لضمان الأمن الإلكتروني، كما تطرح سياسات للأمن الإلكتروني ومهام العمل والإجراءات الخاصة بالقطاعات الرئيسية.

المادة 5: تتخذ الدولة إجراءات من أجل مراقبة وحماية ومعالجة مخاطر الأمن الإلكتروني والتهديدات الناشئة عن داخل وخارج حدود البلاد بجمهورية الصين الشعبية. وتوفر الدولة الحماية للبنية التحتية للمعلومات الحرجة ضد الهجمات والتدخلات والتطفل والتدمير؛ وتفرض الدولة عقوبات على الأنشطة الإلكتروني غير المشروعة أو الإجرامية بما يتفق مع القانوني، مع حماية أمن ونظام الفضاء الإلكتروني.

المادة 6: تعزز الدولة وتدعم السلوك الصادق والأمين والصحي والمتحضر على الإنترنت؛ كما تعزز من بث ونشر القيم الاشتراكية الجوهرية، وتتبنى تدابير من أجل رفع الوعي لدى كامل المجتمع ومستوى الأمن الإلكتروني، كما تصيغ بيئة جيدة لكامل المجتمع من أجل المشاركة التضامنية في تطوير وتنمية الأمن الإلكتروني.

المادة 7: تسارع الدولة في إجراء حوارات دولية وتعاون في مجالات حوكمة الأمن الإلكتروني، وبحث وتطوير تقنيات الشبكات، وصياغة المعايير، ومهاجمة الجريمة الإلكترونية وعدم المشروعية وغيرها من الجوانب الأخرى؛ كما تعزز من إنشاء فضاء إلكتروني سلمي وآمن ومنفتح وتعاوني، مع تأسيس نظام حوكمة إنترنت يتميز بالتعددية والديمقراطية والشفافية.

المادة 8: إدارات أمن الفضاء الإلكتروني والمعلوماتية في الدولة هي المسئولة عن التخطيط الشامل وتنسيق جهود أمن الفضاء الإلكتروني وما يرتبط به من إشراف وجهود إدارية. إدارات مجلس الدولة لكل من الاتصالات السلكية واللاسلكية والأمن العام وغيرها من الإدارات الفرعية ذات الصلة هي المسئولة عن حماية أمن الفضاء الإلكتروني والإشراف عليه وجهود الإدارة ضمن نطاق مسئولياتها، وذلك بما يتفق مع الأحكام الواردة في هذا القانون والقوانين والأنظمة الإدارية ذات الصلة.

حماية أمن الفضاء الإلكتروني والإشراف عليه والجهود الإدارية للإدارات المعنية في الحكومات الشعبية سواء في مستوى المقاطعة أو أعلى من ذلك تقررها الأنظمة الوطنية ذات الصلة.

---

[30] NewAmerica، ترجمة: قانون الأمن الإلكتروني لجمهورية الصين الشعبية (يسري العمل به بتاريخ 1 يونيو/حزيران 2017)، 29 يونيو/حزيران 2018، https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

المادة 9: يجب على مشغلي الشبكات الذين ينفذون أنشطة أعمال وخدمات اتباع القوانين والأنظمة الإدارية، واحترام الأعراف الاجتماعية، والالتزام بالأخلاقيات التجارية والأمانة والمصداقية، وأداء الالتزامات من أجل حماية أمن الفضاء الإلكتروني، وقبل الإشراف من الحكومة والجمهور، مع تحمُّل المسئولية الاجتماعية.
المادة 10: يتم إنشاء وتشغيل الشبكات، أو توفير الخدمات من خلال الشبكات: بما يتفق مع أحكام القوانين والأنظمة الإدارية، ومع المتطلبات الإلزامية للمعايير الوطنية؛ واعتماد التدابير الفنية وغيرها من التدابير اللازمة لحماية أمن الفضاء الإلكتروني والاستقرار التشغيلي؛ والاستجابة الفعالة لحوادث أمن الفضاء الإلكتروني؛ ومنع الجريمة الإلكترونية والنشاط غير القانوني؛ وحفظ تكامل وسرية البيانات والقدرة على استخدامها.
المادة 11: تلتزم المؤسسات الصناعية المعنية في مجال الإنترنت، طبقًا للنظام الأساسي الخاص بها، بتعزيز الرقابة الذاتية في مجال الصناعة، وصياغة معايير سلوك أمن الفضاء الإلكتروني، وإرشاد أعضائها إلى تقوية ودعم حماية أمن الفضاء الإلكتروني طبقًا للقانون، ورفع مستوى حماية أمن الفضاء الإلكتروني، وبث التنمية الصحية للصناعة.
المادة 12: توفر الدولة الحماية لحقوق المواطنين والشخصيات الاعتبارية والمؤسسات الأخرى في استخدام الشبكات طبقًا لأحكام القانون؛ كما تعزز من الوصول واسع النطاق للشبكات، وترفع من مستوى خدمات الشبكة، وتوفر خدمات شبكات آمن وملائمة للمجتمع، وتضمن توزيعًا قانونيًا ومنظمًا وحرًا لمعلومات الشبكة.
يلتزم أي شخص ومؤسسة تستخدم الشبكات بالتقيد بالدستور والقوانين، ومراعاة النظام العام وحماية الأخلاقيات الاجتماعية؛ ويجب ألا يعرض أمن الفضاء الإلكتروني للخطر، ويجب ألا يستخدم الإنترنت للمشاركة في أنشطة تهدد الأمن القومي والسمعة الوطنية والمصالح الوطنية؛ ويجب ألا يحض على الإضرار بالسيادة القومية، أو الانقلاب على النظام الاشتراكي، أو الحض على النزعة الانفصالية، أو الإخلال بالوحدة الوطنية، أو الدفاع عن الإرهاب أو التطرف، أو الدفاع عن الكراهية العرقية والتمييز العرقي، ونشر معلومات الحض على العنف أو المعلومات الفاضحة أو الجنسية، أو إنشاء أو توزيع معلومات مزيفة لزعزعة النظام الاقتصادي أو الاجتماعي، أو معلومات تنتهك السمعة أو الخصوصية الملكية الفكرية أو غير ذلك من الحقوق والمصالح القانونية المشروعة للغير، وكل تلك الأفعال الأخرى.
المادة 13: تشجع الدولة أبحاث وتطوير منتجات وخدمات الشبكات المفضية إلى التنشئة الصحية للصغار؛ كما تلتزم الدولة بالمعاقبة القانونية لاستخدام الشبكة من أجل الانخراط في أنشطة تهدد الصحة النفسية والجسدية للقاصرين؛ وتلتزم الدولة بتوفير بيئة شبكة آمنة وصحية للقاصرين.
المادة 14: لكل الأفراد والمؤسسات الحق في الإبلاغ عن التصرفات المهددة لأمن الفضاء الإلكتروني لإدارة أمن الفضاء الإلكتروني والمعلوماتية والاتصالات والأمن العام وغيرها من الإدارات. وتلتزم الإدارات التي تتلقى البلاغات بالتعامل الفوري معها بما يتفق مع القانون؛ ومتى لم تكن المسائل تندرج ضمن مسئوليات تلك الإدارة، فتلتزم بإحالتها على الفور إلى الإدارة المخولة بالتعامل معها.
تحتفظ الإدارات المعنية بسرية معلومات المبلغين وتحمي الحقوق والمصالح المشروعة للمبلغين.

الفصل الثاني: دعم وتعزيز أمن الفضاء الإلكتروني

المادة 15: تقوم الدولة بتأسيس وتحسين نظام لمعايير أمن الفضاء الإلكتروني. تلتزم إدارات وضع المعايير الإدارية في مجلس الدولة وغيرها من إدارات مجلس الدولة المعنية، وعلى أساس مسئوليات كل منها على حدة، بتنظيم الصياغة والمراجعة الآنية للمعايير الوطنية ومعايير الصناعة ذات الصلة بالنسبة لإدارة أمن الفضاء الإلكتروني، بالإضافة إلى أمن منتجات الشبكة وخدماتها وعملياتها.
تدعم الدولة المشروعات الكبرى ومعاهد الأبحاث ومدارس التعلم العليا، والمؤسسات الصناعية ذات الصلة بالشبكات من أجل المشاركة في صياغة المعايير الوطنية ومعايير الصناعة الخاصة بأمن الفضاء الإلكتروني.
المادة 16: على مجلس الدولة والحكومات الشعبية في المقاطعات والمناطق المستقلة والبلديات ذات الحكم المباشر: إجراء تخطيط شامل؛ وتوسيع الاستثمار؛ ودعم صناعات والبرامج التكنولوجية الرئيسية في مجال أمن الفضاء الإلكتروني؛ ودعم أعمال البحث والتطوير والتطبيق والمعلوماتية لأمن الفضاء الإلكتروني؛ وتعزيز منتجات وخدمات الشبكات الآمنة والجديرة بالثقة؛ وحماية حقوق الملكية الفكرية لتقنيات الشبكات؛ ودعم معاهد الأبحاث والتطوير، ومدارس التعليم العالي، إلخ من أجل المشاركة في برامج ابتكار تكنولوجيا أمن الفضاء الإلكتروني للدولة.
المادة 17: تتطور الدولة في تأسيس أنظمة الخدمات الاشتراكية لأمن الفضاء الإلكتروني، من خلال تشجيع الشركات والمؤسسات المعنية على تنفيذ شهادات واختبارات أمن الفضاء الإلكتروني وتقييم المخاطر، بالإضافة إلى الأنشطة الأمنية الأخرى.
المادة 18: تشجع الدولة تطوير تقنيات حماية واستغلال أمن بيانات الشبكات، وذلك من خلال تطوير فتح موارد البيانات العامة، وتعزيز الابتكار الفني والتنمية الاقتصادية والاجتماعية.
وتدعم الدولة الطرق الابتكارية في إدارة أمن الفضاء الإلكتروني، من خلال استخدام تقنيات الشبكات الجديدة لتعزيز وتقوية مستوى حماية أمن الفضاء الإلكتروني.
المادة 19: تلتزم جميع مستويات الحكومات الشعبية والإدارات المعنية التابعة لها بتنظيم وتنفيذ تعميم وتعليم أمن الفضاء الإلكتروني الاعتيادي، وإرشاد وحث الوحدات المعنية على التنفيذ الصحيح لأعمال نشر أمن الفضاء الإلكتروني وتعليمه.
تجري وسائل الإعلام أعمال توعية وتعليم مستهدفة حول أمن الفضاء الإلكتروني موجهة إلى الجمهور.
المادة 20: تدعم الدولة المشروعات الكبرى والمؤسسات التعليمية أو التدريبية، مثل مدارس التعليم العالي والمدارس المهنية، على تنفيذ أعمال التوعية والتدريب المرتبطة بأمن الفضاء الإلكتروني، كما تستخدم العديد من الطرق من أجل تشجيع أفراد العمل المؤهلين في مجال أمن الفضاء الإلكتروني وتعزيز تفاعل المتخصصين والمحترفين في هذا المجال.

الفصل الثالث: أمن عمليات الشبكات

القسم 1: أحكام اعتيادية

المادة 21: تنفذ الدولة نظامًا لحماية أمن الفضاء الإلكتروني متعدد المستويات [MLPS]. يلتزم مشغلو الشبكات بأداء واجبات حماية الأمن التالية بما يتفق مع متطلبات نظام حماية أمن الفضاء الإلكتروني متعدد المستويات من أجل ضمان خلو الشبكة من التدخل أو الضرر أو الوصول غير المرخص، ولمنع حالات تسرب بيانات الشبكة أو السطو أو التزييف:

(1) صياغة نظام إدارة الأمن الداخلية والقواعد التشغيلية، وتحديد الأشخاص المسئولين عن أمن الفضاء الإلكتروني، وتنفيذ مسئولية حماية أمن الفضاء الإلكتروني.

(2) اعتماد التدابير الفنية من أجل منع فيروسات الكمبيوتر والهجمات الإلكترونية، وعمليات التطفل على الشبكة، وغير ذلك من الأفعال التي تهدد أمن الفضاء الإلكتروني.

(3) اعتماد التدابير الفنية من أجل مراقبة وتسجيل الحالات التشغيلية للشبكة وحوادث أمن الفضاء الإلكتروني، واتباع أحكام تخزين شعارات الشبكة لمدة ستة أشهر على أقل تقدير.

(4) اعتماد تدابير مثل تصنيف البيانات، والنسخ الاحتياطي للبيانات الهامة، والتشفير.

(5) الالتزامات الأخرى المنصوص عليها في القانون أو الأنظمة الإدارية.

المادة 22: يجب أن تتوافق منتجات وخدمات الشبكات مع المتطلبات الوطنية والإلزامية ذات الصلة. يجب ألا يقوم موفرو منتجات وخدمات الشبكات بتثبيت برامج ضارة؛ وفي حالة اكتشاف أن منتجاتهم وخدماتهم تحتوي على عيوب أمنية أو مواطن اختراق، يجب عليهم اعتماد تدابير تصحيحية على الفور، بالإضافة إلى اتباع الأحكام التي تقضي بإشعار المستخدمين على الفور وإبلاغ الإدارات المختصة.

يلتزم موفرو منتجات وخدمات الشبكة بتوفير الصيانة الأمنية لمنتجاتهم وخدماتهم، ويجب عليهم الامتناع عن إنهاء أحكام الصيانة الأمنية خلال القيود الزمنية أو الفترة المتفق عليها مع عملائهم.

إذا كان لمنتج أو خدمة شبكة وظيفة جمع معلومات المستخدمين، فيلتزم موفر تلك المنتجات أو الخدمات بتوضيح هذا الأمر جليًا والحصول على موافقة من المستخدم؛ وإذا انطوى ذلك على معلومات شخصية تخص المستخدمين، فيلتزم الموفر بالتقيد بالأحكام المنصوص عليها في هذا القانون والقوانين ذات الصلة بالإضافة إلى الأنظمة الإدارية الخاصة بحماية المعلومات الشخصية.

المادة 23: يجب أن تتبع معدات الشبكة ومنتجات أمن الفضاء الإلكتروني المخصصة المعايير الوطنية والمتطلبات الإلزامية، وأن تكون معتمدة من ناحية الأمن من جانب مؤسسة مؤهلة أو تستوفي متطلبات عملية فحص أمني قبل أن يتم بيعها أو توفيرها. تلتزم إدارات أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة وبالتعاون مع الإدارات المعنية في مجلس الدولة بصياغة وإصدار كتالوج بمعدات الشبكة الحرجة ومنتجات أمن الفضاء الإلكتروني المخصصة، وتعزيز الإقرار المتبادل للشهادات الأمنية ونتائج الفحص الأمني وذلك لتجنب تكرار الشهادات وعمليات الفحص.

المادة 24: يلتزم مشغلو الشبكات الذي يتعاملون مع الوصول إلى الشبكة وخدمات تسجيل أسماء النطاقات للمستخدمين والمتعاملين مع الوصول إلى الشبكات الثابتة أو شبكات المحمول أو الذين يوفرون للمستخدمين خدمة نشر المعلومات أو خدمات الرسائل الفورية بمطالبة المستخدمين بتوفير معلومات حول هوياتهم الحقيقية عند توقيع اتفاقيات مع المستخدمين أو تأكيد توفير الخدمات. وفي حالة عدم توفير المستخدمين لمعلومات حول الهوية الحقيقية، فيجب على مشغلي الشبكات عدم تزويدهم بالخدمات ذات الصلة.

تنفذ الدولة استراتيجية لمصادقة هوية الشبكة وتدعم أبحاث وتطوير تقنيات لمصادقة الهويات الإلكترونية الآمنة والملائمة، مع تعزيز القبول المتبادل فيما بين طرق المصادقة الإلكترونية المختلفة للهوية.

المادة 25: يلتزم مشغلو الشبكات بصياغة خطط للاستجابة للطوارئ من أجل حوادث أمن الفضاء الإلكتروني مع المعالجة الآنية لنقاط اختراق النظام، وفيروسات الكمبيوتر والهجمات الإلكترونية وحالات التطفل على الشبكة، وغير ذلك من مخاطر أمن الفضاء الإلكتروني. ويجب على مشغلي الشبكات عند وقوع حوادث تتعلق بأمن الفضاء الإلكتروني البدء على الفور في خطة للاستجابة للطوارئ، واعتماد تدابير تصحيحية مقابلة، وإبلاغ الإدارات المختصة بما يتفق مع الأحكام ذات الصلة.

المادة 26: على من يقومون بتنفيذ أعمال توثيق أو اختبار أمن الفضاء الإلكتروني أو تقييم المخاطر أو غير ذلك من الأنشطة—أو يقومون بنشر معلومات أمن الفضاء الإلكتروني مثل نواحي ضعف النظام أو فيروسات الكمبيوتر أو هجمات الشبكات أو غارات الشبكات—الالتزام بالأحكام الوطنية ذات الصلة.

المادة 27: يجب على الأفراد والمؤسسات عدم الانخراط في أعمال الهجوم غير القانوني على شبكات الغير، أو السبب في تعطل العمل الطبيعي لشبكات الغير، أو سرقة بيانات الشبكات أو الانخراط في أنشطة أخرى من شأنها تعريض أمن الفضاء الإلكتروني للخطر؛ ويجب عليهم عدم تقديم برامج أو أدوات تستخدم على وجه الخصوص في هجمات الشبكات التي تؤدي إلى تعطيل وظائف الشبكات الطبيعية وتدابير الحماية، أو سرقة بيانات الشبكة، أو الانخراط في الأعمال الأخرى التي تعرض أمن الفضاء الإلكتروني للخطر؛ ومتى ما كانوا على دراية واضحة بأن الآخرين سوف يشاركون في إجراءات من شأنه تعريض أمن الفضاء الإلكتروني للخطر فعليهم عدم تقديم أي عون مثل الدعم الفني أو الإعلان والترويج أو سداد المصروفات.

المادة 28: يلتزم مشغلو الشبكات بتوفير الدعم والمساعدة الفنية إلى جهات الأمن العامة وجهات الأمن القومي القائمة على حفظ وضمان الأمن القومي والتحري عن الأنشطة الإجرامية بما يتفق مع أحكام القانون.

المادة 29: تدعم الدولة التعاون بين مشغلي الشبكات في جوانب مثل جمع وتحليل وإعداد تقارير والتعامل في حالة الطوارئ مع معلومات أمن الفضاء الإلكتروني، من خلال زيادة سعة وكفاءة حفظ الأمن لدى مشغلي الشبكات.

من المفترض بالمؤسسات الصناعية المعنية تأسيس وإقرار آليات كاملة لوضع معايير وتنسيق أمن الفضاء الإلكتروني للصناعة الخاصة بهم، مع تقوية وتعزيز تحليلها وتقييمها لأمن الفضاء الإلكتروني، وإجراء تحذيرات دورية بالمخاطر، مع الدعم والتنسيق للأعضاء استجابةً لمخاطر أمن الفضاء الإلكتروني.

المادة 30: لا يجوز استخدام المعلومات التي تحصل عليها إدارات أمن الفضاء الإلكتروني والمعلوماتية والإدارات المعنية المنوط بها أداء واجبات حماية أمن الفضاء الإلكتروني إلا حسبما يكون ضروريًا لحماية أمن الفضاء الإلكتروني، ويجب ألا تستخدم بأية طرق أخرى.

القسم 2: أمن العمليات الخاصة بالبنية التحتية للمعلومات الحرجة

المادة 31: تنفذ الدولة حماية أساسية على أساس نظام حماية أمن الفضاء الإلكتروني متعدد المستويات لكل من خدمات الاتصالات العامة والإعلام والطاقة والمواصلات والموارد المائية والتمويل والخدمة العامة والحكومة الإلكترونية وغير ذلك من البنى التحتية الأساسية الأخرى للمعلومات والتي قد تعرّض الأمن القومي أو الرفاهة الوطنية أو حياة الشعب أو المصلحة العامة—في حالة التدمير أو فقد التشغيل الوظيفي أو التعرض لتسرب في البيانات—لخطر كبير. يلتزم مجلس الدولة بصياغة نطاق محدد بالإضافة إلى تدابير لحماية الأمن من أجل البنية التحتية للمعلومات الحيوية.

وتشجع الدولة مشغلي الشبكات خارج نظم البنية التحتية للمعلومات الحيوية [المخصصة] على المشاركة الطوعية في نظام حماية البنية التحتية للمعلومات الحيوية.

المادة 32: طبقًا للواجبات وقسمة العمل المقدمة من مجلس الدولة، فإن الإدارات المسئولة عن أعمال حماية الأمن للبنية التحتية للمعلومات الحيوية من المفترض أن تقوم وبشكل منفصل بتجميع وتنظيم خطط تنفيذ الأمن للبنية التحتية للمعلومات الحرجة الخاصة بصناعتها أو قطاعها، مع توجيه والإشراف على جهود الحماية الأمنية لعمليات البنية التحتية للمعلومات الحيوية.

المادة 33: يلتزم من يقومون بتأسيس بنية تحتية للمعلومات الحيوية بضمان تحلي تلك البنية بالقدرة دعم استقرار الأعمال والعمليات المستدامة، مع ضمان التخطيط المتزامن، والتأسيس المتزامن والتطبيق المتزامن للتدابير الفنية الخاصة بالأمن.

المادة 34: بالإضافة إلى الاحكام المنصوص عليها في المادة 21 من هذا القانون، يلتزم مشغلو البنية التحتية للمعلومات الحيوية بأداء واجبات حماية الأمن التالية:

(1) تأسيس وإقامة هيئات مخصصة لإدارة الأمن وأفراد مسئولين عن إدارة الأمن، مع إجراء فحوصات من حيث الخلفية الأمن على الأشخاص وأفراد العمل المسئولين في المراكز الحساسة.

(2) إجراء عمليات تعليمية في مجال أمن الفضاء الإلكتروني وتدريب فني وعمليات تقييم المهارات للموظفين دوريًا.

(3) إجراء عمليات نسخ احتياطي للاستعادة من الكوارث للنظم وقواعد البيانات الهامة.

(4) صياغة خطط للاستجابة للطوارئ بالنسبة لحوادث أمن الفضاء الإلكتروني، وتنظيم مناورات تدريبية دورية.

(5) الواجبات الأخرى المنصوص عليها في القانون أو الأنظمة الإدارية.

المادة 35: يلتزم مشغلو البنية التحتية للمعلومات الحيوية الذي يشترون منتجات وخدمات شبكات قد يكون لها تأثير على الأمن القومي بالخضوع لمراجعة الأمن القومي التي تنظمها إدارات أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة بالإضافة إلى الإدارات المختصة التابعة لمجلس الدولة.

المادة 36: يلتزم مشغلو البنية التحتية للمعلومات الحيوية الذي يشترون منتجات وخدمات شبكات باتباع الأحكام ذات الصلة والتوقيع على اتفاقية للأمن والحفاظ على السرية مع موفر الخدمة، مع توضيح الواجبات والمسئوليات الخاصة بالأمن والحفاظ على السرية.

المادة 37: على مشغلي البنية التحتية للمعلومات الحيوية الذين يجمعون أو يقدمون معلومات شخصية أو بيانات هامة خلال أعمالهم داخل حدود أراضي جمهورية الصين الشعبية تخزين تلك المعلومات والبيانات داخل الأراضي الصينية. في الحالات التي يكون من الضروري حقًا توفير ذلك خارج البر الرئيسي بسبب متطلبات واشتراطات الأعمال، فيجب عليهم اتباع التدابير التي تضامنت في صياغتها إدارة الأمن الإلكتروني والمعلوماتية في البلاد والإدارات المعنية في مجلس الدولة من أجل إجراء تقييم للأمن؛ وفي الحالات التي تنص فيها القوانين والأنظمة الإدارية على خلاف ذلك، فيجب اتباع تلك الأحكام.

المادة 38: يلتزم مشغلو البنية التحتية للمعلومات الحيوية مرة واحدة سنويًا على أقل تقدير بإجراء فحص وتقييم لأمن شبكاتهم والمخاطر التي قد تكون موجودة، سواء على الشبكات الخاصة بهم أو من خلال الاستعانة بمؤسسة لخدمات أمن الفضاء الإلكتروني؛ ويجب على مشغلي البنية التحتية للمعلومات الحيوية تقديم تقرير حول أمن الفضاء الإلكتروني بخصوص ظروف الفحص والتقييم بالإضافة إلى تدابير التحسين، على أن يتم إرسال ذلك إلى الإدارة المعنية المسئولة عن جهود حماية أمن البنية التحتية للمعلومات الحيوية.

المادة 39: تلتزم إدارات أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة بتنفيذ الإدارات المختصة في الاستعانة بالتدابير التالية من أجل حماية أمن البنية التحتية للمعلومات الحيوية:

(1) إجراء اختبارات موضعية وعشوائية لمخاطر أمن البنية التحتية للمعلومات الحيوية، مع طرح تدابير التحسين، ومتى ما كان ضروريًا فيمكنهم الاستعانة بمؤسسة لخدمات أمن الفضاء الإلكتروني من أجل إجراء الاختبارات وتقييم مخاطر أمن الفضاء الإلكتروني.

(2) إجراء تنظيم دوري لمشغلي البنية التحتية للمعلومات الحيوية من أجل إجراء مناورات الاستجابة لطوارئ أمن الفضاء الإلكتروني، وزيادة المستوى والتنسيق وسعة وقدرة الردود على حواد أمن الفضاء الإلكتروني.

(3) تعزيز مشاركة معلومات أمن الفضاء الإلكتروني فيما بين الإدارات المختصة ومشغلي البنية التحتية للمعلومات الحيوية، أيضًا المؤسسات البحثية المعنية ومنظمات خدمات أمن الفضاء الإلكتروني.

(4) توفير الدعم والمساعدة الفنية لإدارة طوارئ أمن الفضاء الإلكتروني والاستعادة، إلخ.

الفصل الرابع: أمن معلومات الشبكات

المادة 40: يلتزم مشغلو الشبكات بالحفاظ الصارم على سرية معلومات المستخدمين التي يقومون بجمعها، وتأسيس وإتمام نظم حماية معلومات المستخدمين.

المادة 41: يلتزم مشغلو الشبكات الذين يقومون بجمع واستخدام المعلومات الشخصية بالتقيد بمبادئ الشرعي والملكية والضرورة؛ مع الالتزام بنشر قواعد للجمع والاستخدام، مع البيان الواضح للأغراض والوسائل والنطاق الخاص بجمع أو استخدام المعلومات، والحصول على موافقة الأشخاص أصحاب البيانات التي يتم جمعها.

يجب على مشغلي الشبكات عدم جمع المعلومات الشخصية غير ذات الصلة بما يقدمونه من خدمات؛ ويجب ألا يخالفوا أحكام القوانين أو الأنظمة الإدارية أو الاتفاقيات المبرمة بين الأطراف لجمع أو استخدام المعلومات الشخصية؛ مع الالتزام باتباع أحكام القوانين والأنظمة الإدارة والاتفاقيات المبرمة من المستخدمين من أجل معالجة المعلومات الشخصية التي قاموا بتخزينها.

المادة 42: يجب على مشغلي الشبكات عدم الإفصاح ن المعلومات الشخصية التي يقومون بجمعها أو العبث بها أو تدميرها؛ وفي حالة عدم توافر موافقة الشخص الذي تم جمعها معلوماته، يجب عليهم عدم توفير المعلومات الشخصية للغير. وعلى الرغم من ذلك، تسري هذه الحالة باستثناء أنه يمكن توفير المعلومات إذا تبين أنه بعد المعالجة ليست هناك طريقة من أجل تحديد فرد بعينه، ولا يمكن استعادة الهوية.

يلتزم مشغلو الشبكات باعتماد التدابير الفنية وغيرها من التدابير اللازمة لضمان أمن المعلومات الشخصية التي يقومون بجمعها وحماية المعلومات الشخصية من التسرب أو التعرض للتدمير أو الفقد. وفي حالة حدوث تسرب أو تدمير أو فقد المعلومات الشخصية، أو في حالة احتمالية حدوث ذلك، يجب اتخاذ إجراءات تصحيحية على الفور، واتباع الأحكام من أجل إشعار المستخدمين على الفور وتقديم تقرير إلى الجهات المعنية بما يتفق مع الأنظمة السارية.

المادة 43: في حالة اكتشاف الأفراد أن مشغلي الشبكات قد خالفوا أحكام القوانين أو الأنظمة الإدارية أو الاتفاقيات المبرمة مع الأطراف لجمع أو استخدام معلوماتهم الشخصية، يكون لهم الحق في مطالبة مشغلي الشبكات بحذف معلوماتهم الشخصية؛ وفي حالة اكتشاف أن المعلومات الشخصية التي تم جمعها أو تخزينها بمعرفة مشغلي الشبكات بها أخطاء، يكون لهم الحق في مطالبة مشغلي الشبكات بإجراء التصحيحات. يلتزم مشغلو الشبكات بتنفيذ تدابير وإجراءات من أجل عمليات الحذف والتصحيح.

المادة 44: يجب على الأفراد أو المؤسسات عدم سرقة أو استخدام طرق أخرى غير قانونية من أجل الاستحواذ على المعلومات الشخصية، ويجب عليهم الامتناع عن البيع غير القانوني للمعلومات الشخصية أو تزويد الغير بها بشكل غير قانوني.

المادة 45: يجب على الإدارات المنوط بها واجبات الإشراف والإدارة القانونية على أمن الفضاء الإلكتروني ويجب على فرق العمل التابعة لها الحفاظ على السرية التامة للمعلومات الشخصية السرية والمعلومات الخاصة والأسرار التجارية التي يطلعون عليها عند أدائهم لواجباتهم، ويجب عليهم عدم تسريبها أو بيعها أو توفيرها للغير بشكل غير قانوني.

المادة 46: يتحمل جميع الأفراد والمؤسسات المسئولية عن استخدامهم لمواقع الويب ويجب عليهم عدم تأسيس مواقع على الويب أو مجموعات اتصالات لاستخدامها في ارتكاب أعمال الاحتيال أو نشر الطرق الإجرامية أو إنشاء أو بيع الأشياء المحظورة أو الخاضعة للرقابة، أو غير ذلك من الأنشطة المجرّمة، ويجب عدم استغلال مواقع الويب في نشر المعلومات ذات الصلة بارتكاب الاحتيال أو إنشاء أو بيع الأشخاص المحظورة أو الخاضعة للرقابة، او غير ذلك من الأنشطة غير المشروعة.

المادة 47: يلتزم مشغلو الشبكات بتقوية وتعزيز إدارة المعلومات التي ينشرها المستخدمون، وعند اكتشاف المعلومات التي يحظر القانون أو الأنظمة الإدارية نقلها، فيلتزمون بالتوقف فورًا عن نقل تلك المعلومات، والاستعانة بإجراءات معالجة مثل حذف المعلومات أو منع نشر المعلومات أو حذف السجلات ذات الصلة، وإبلاغ الإدارة المختصة بالمعنية بالأمر.

المادة 48: يجب ألا تقوم المعلومات الإلكترونية التي يتم إرسالها أو التطبيقات البرمجية التي يوفرها أي فرد أو مؤسسة بتثبيت برامج ضارة، ويجب ألا تحتوي على معلومات تحظر القوانين والأنظمة الإدارية نشرها أو نقلها.

يلتزم موفرو خدمة توزيع المعلومات الإلكترونية وموفرو خدمة تنزيل التطبيقات البرمجية بأداء واجبات إدارة الأمن؛ ومتى ما نما إلى علمهم أن مستخدميهم قد تورطوا في تصرف منصوص عليه في الفقرة السابقة، فيلتزمون: بتنفيذ تدابير مثل وقف توفير الخدمات وحذف المعلومات أو البرامج الضارة؛ وتخزين السجلات ذات الصلة؛ وإبلاغ الإدارات المختصة ذات الصلة.

المادة 49: يلتزم مشغلو الشبكات بتأسيس أنظمة لشكاوى وبلاغات أمن معلومات الشبكات، والإفصاح عن المعلومات للجمهور مثل طرق تقديم الشكاوى أو البلاغات، والقبول الفوري للشكاوى والبلاغات ذات الصلة بأمن معلومات الشبكات.

ويلتزم مشغلو الشبكات بالتعاون مع إدارات أمن الفضاء الإلكتروني والمعلوماتية والإدارات المعنية في إجراء تنفيذ أعمال الإشراف والفحص بما يتفق مع أحكام القانون.

المادة 50: تلتزم إدارات أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة والإدارات المعنية بأداء مسئوليات الإشراف على أمن معلومات الشبكات وإداراتها بما يتفق مع أحكام القانون؛ وفي حالة اكتشافهم لنشر أو نقل معلومات تحظرها القوانين أو الأنظمة الإدارية، فيلتزمون بمطالبة مشغلي الشبكات المعنيين بوقف عملية النقل واستخدام تدابير تصحيحية مثل الحذف وتخزين السجلات ذات الصلة؛ وبالنسبة للمعلومات المشار إليها أعلاه والتي تأتي من خارج البر الرئيسي لجمهورية الصين الشعبية، فيلتزمون بإشعار المؤسسة المعنية باعتماد تدابير فنية وغيرها من التدابير الضرورية من أجل حجب ومنع النقل.

الفصل الخامس: المراقبة والتحذير المبكر والاستجابة للطوارئ

المادة 51: تلتزم الدولة بتأسيس نظام لمراقبة أمن الفضاء الإلكتروني والإنذار المبكر ونقل المعلومات. تلتزم إدارات أمن الفضاء الإلكتروني والمعلوماتية بإجراء تنسيق كلي للإدارات المعنية من أجل تقوية جهود الجمع والتحليل والإبلاغ لمعلومات أمن الفضاء الإلكتروني، واتباع الأنظمة المخصصة للإصدار الموحد لمراقبة أمن الفضاء الإلكتروني ومعلومات الإنذار المبكر.

المادة 52: تلتزم الإدارات المسئولة عن جهود حماية أمن البنية التحتية للمعلومات الحيوية بتأسيس أنظمة كاملة لمراقبة أمن الفضاء الإلكتروني والإنذار المبكر والإبلاغ عن المعلومات من أجل الصناعة أو القطاع الذي يعملون فيه، والإبلاغ عن مراقبة أمن الفضاء الإلكتروني ومعلومات الإنذار المبكر بما يتفق مع الأنظمة.

المادة 53: تلتزم إدارات أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة بالتنسيق مع الإدارات المختصة من أجل تأسيس وإتمام آليات لتقييم مخاطر أمن الفضاء الإلكتروني وجهود الاستجابة للطوارئ، وصياغة خطط للاستجابة لطوارئ حوادث أمن الفضاء الإلكتروني وتنظيم مناورات دورية.

تلتزم الإدارات المسئولة عن جهود حماية أمن البنية التحتية للمعلومات الحيوية بصياغة خطط للاستجابة لطوارئ حوادث أمن الفضاء الإلكتروني للصناعة أو القطاع الذي يعملون فيه، مع تنظيم مناورات دورية.

وتقوم خطط الاستجابة لطوارئ حوادث أمن الفضاء الإلكتروني بتصنيف حوادث أمن الفضاء الإلكتروني على أساس عوامل مثل درجة الضرر بعد وقوع الحادث ونطاق التأثير، وتوفير التدابير المقابلة للتعامل مع استجابة الطوارئ.

المادة 54: وفي حالة زيادة خطر حوادث أمن الفضاء الإلكتروني، تلتزم الإدارات المعنية في الحكومات الشعبية وفي المستوى الإقليمي وما فوقه باتباع نطاق السلطة والإجراءات المقدمة، واستخدام التدابير التالية على أساس سمات وخصائص خطر أمن الفضاء الإلكتروني والضرر الذي قد تسببه:

(1) المطالبة بأن تقوم الإدارات والمؤسسات وفرق العمل المعنية بجمع المعلومات ذات الصلة والإبلاغ به، بالإضافة إلى تعزيز مراقبة حدوث مخاطر أمن الفضاء الإلكتروني.

(2) تنظيم الإدارات والمؤسسات وأفراد العمل المتخصصين المعنيين بإجراء تحليل وتقييم للمعلومات حول خطر أمن الفضاء الإلكتروني، والتنبؤ باحتمالية وقوع الحوادث، ونطاق التأثير، ومستوى الضرر.

(3) إصدار تحذيرات تخص أمن الفضاء الإلكتروني إلى الجمهور، ونشر تدابير لتجنب الضرر أو الحد منه.

المادة 55: عند وقوع حادثة من حوادث أمن الفضاء الإلكتروني، يجب إطلاق خطة الاستجابة للحوادث الطارئة على الفور، مع إجراء تقييم وتقدير لحادثة أمن الفضاء الإلكتروني، وتتم مطالبة مشغلي الشبكات باعتماد تدابير فنية وتدابير أخرى ضرورية، مع إزالة المخاطر الأمنية المحتملة، ويتم منع التهديد من التوسع، ويتم نشر وإعلان تحذيرات ذات صلة إلى الجمهور على الفور.

المادة 56: في الحالات التي تكتشف فيها هيئات الحكومات الشعبية في المستوى الإقليمي أو ما فوقه أثناء أداء أعمال وواجبات إدارة أمن الفضاء الإلكتروني والإشراف عليه أن الشبكات بها خطر كبير نسبيًا على الأمن أو وقوع حادثة تتعلق بالأمن، فيجوز لها الاتصال بالممثل القانوني أو الطرف المسئول لدى مشغل تلك الشبكة من أجل إجراء مراجعات بما يتفق مع نطاق الصلاحية والإجراءات المتاحة. يلتزم مشغلو الشبكات باتباع المتطلبات اللازمة لاستخدام الإجراءات والقيام بالتصحيحات والتخلص من المخاطر المخفية.

المادة 57: في حالة وقوع حالات طوارئ مفاجئة أو حوادث تتعلق بأمن الإنتاج نتيجة لحوادث أمن الفضاء الإلكتروني، فيتم التعامل معها بما يتفق مع الأحكام المنصوص عليها في "قانون الاستجابة للطوارئ بجمهورية الصين الشعبية" و"قانون سلامة الإنتاج بجمهورية الصين الشعبية" وغير ذلك من القوانين والأنظمة الإدارية ذات الصلة.

المادة 58: لتلبية الحاجة إلى حماية الأمن القومي والنظام الاجتماعي العام، وللاستجابة إلى متطلبات حوادث الأمن الكبيرة داخل المجتمع، من الممكن -وفقًا لما نص عليه أو اعتمده مجلس الدولة- اتخاذ تدابير مؤقتة فيما يخص اتصالات الشبكة في منطقة محددة على وجه الخصوص، مثل تقييد تلك الاتصالات.

الفصل السادس: المسئولية القانونية

المادة 59: في حالة عدم قيام مشغلي الشبكات بأداء واجبات حماية أمن الفضاء الإلكتروني المنصوص عليها في المادة 21 والمادة 25 من هذا القانون، تلتزم الإدارات المختصة بفرض تصحيحات وتقديم تحذيرات؛ وفي حالة رفض التصحيحات أو إذا أدت إلى الإضرار بأمن الفضاء الإلكتروني أو غيرها من العواقب، يتم فرض غرامة تتراوح ما بين 10,000 إلى 100,000 رنمينبي؛ كما يتم تغريم فريق الإدارة المسئول مسئولية مباشرة بمبلغ يتراوح بين 5,000 إلى 50,000 رنمينبي.

في حالة عدم قيام مشغلي البنية التحتية للمعلومات الحيوية بأداء واجبات حماية أمن الفضاء الإلكتروني المنصوص عليها في المادة 33 والمادة 34 والمادة 36 والمادة 38 من هذا القانون، تلتزم الإدارات المختصة بفرض تصحيحات وتقديم تحذيرات؛ وفي حالة رفض التصحيحات أو إذا أدت إلى الإضرار بأمن الفضاء الإلكتروني أو غيرها من العواقب، يتم فرض غرامة تتراوح ما بين 100,000 إلى 1,000,000 رنمينبي؛ كما يتم تغريم فريق الإدارة المسئول مسئولية مباشرة بمبلغ يتراوح بين 10,000 إلى 100,000 رنمينبي.

المادة 60: في حالة مخالفة المادة 22 الفقرة 1 أو المادة 48 الفقرة 1 من هذا القانون بأي من التصرفات التالية، تلتزم الإدارات المختصة ذات الصلة بفرض التصحيحات وتقديم تحذيرات؛ وفي حالة رفض التصحيحات أو إذا أدت إلى الإضرار بأمن الفضاء الإلكتروني أو غيرها من العواقب، يتم فرض غرامة تتراوح ما بين 50,000 إلى 500,000 رنمينبي؛ كما يتم تغريم الأشخاص المسئولين مسئولية مباشرة بمبلغ يتراوح بين 10,000 إلى 100,000 رنمينبي:

(1) تثبيت برامج ضارة.

(2) عدم اتخاذ إجراءات تصحيحية مباشرة للأعطاب أو الخروقات الأمنية الموجودة في المنتجات أو الخدمات، أو عدم إبلاغ المستخدمين وإبلاغ الإدارات المختصة بما يتفق مع الأنظمة المعمول بها.
(3) الإنهاء غير المرخص لتوفير الصيانة الأمنية للمنتجات أو الخدمات.

المادة 61: مشغلو الشبكات المخالفين للمادة 24 الفقرة 1 من هذا القانون بعدم مطالبة المستخدمين بتوفير معلومات هوية حقيقية أو توفير الخدمات ذات الصلة إلى مستخدمين لا يوفرون معلومات هوية حقيقية، مطالبون بإجراء تصحيحات بمعرفة الإدارة المختصة ذات الصلة؛ وفي حالة رفض التصحيحات أو إذا كانت الظروف خطيرة، يتم فرض غرامة قدرها 50,000 إلى 500,000 رنمينبي، ويجوز للإدارة المختصة ذات الصلة إصدار أمر بتعليق العمل مؤقتًا أو تعليق العمل من أجل إجراء التصحيحات أو إغلاق مواقع الويب أو إلغاء تراخيص العمل ذات الصلة أو إلغاء تراخيص الأعمال؛ ويتم تغريم الأشخاص المسئولين مسئولية مباشرة وفريق العمل المسئول مسئولية مباشرة بمبلغ يتراوح ما بين 10,000 إلى 100,000 رنمينبي.

المادة 62: في حالة مخالفة المادة 26 من هذا القانون بتنفيذ شهادات أمن الفضاء الإلكتروني أو الاختبار أو عمليات تقييم المخاطر أو نشر معلومات أمن الفضاء الإلكتروني مثل نقاط ضعف واختراق النظام أو فيروسات الكمبيوتر أو الهجمات الإلكترونية أو التدخل في عمل الشبكات، يتم فرض تصحيحات وتقديم إنذار بذلك؛ وفي حالة رفض التصحيحات أو إذا كانت الظروف خطيرة، يتم فرض غرامة قدرها 10,000 إلى 100,000 رنمينبي، ويجوز للإدارة المختصة ذات الصلة إصدار أمر بتعليق العمل مؤقتًا أو تعليق العمل من أجل إجراء التصحيحات أو إغلاق مواقع الويب أو إلغاء تراخيص العمل ذات الصلة أو إلغاء تراخيص الأعمال؛ ويتم تغريم الأشخاص المسئولين مسئولية مباشرة وفريق العمل المسئول مسئولية مباشرة بمبلغ يتراوح ما بين 5,000 إلى 50,000 رنمينبي.

المادة 63: في حالة مخالفة المادة 27 من هذا القانون بالمشاركة في أنشطة تضر أمن الفضاء الإلكتروني أو بتوفير برمجيات أو أدوات مخصصة تستخدم في الانخراط في أنشطة تضر بأمن الفضاء الإلكتروني أو بتزويد آخرين مشاركين في أنشطة تضر بأمن الفضاء الإلكتروني بالمساندة مثل الدعم الفني أو الإعلانات أو عمليات الترويج أو سداد الرسوم، ومتى لم يمثل ذلك جريمة، تصادر هيئات الأمن العام المكتسبات غير القانونية وتفرض حظرًا لمدة 5 أيام بحد أقصى، ويجوز لها فرض غرامة تتراوح ما بين 50,000 ومبلغ 500,000 رنمينبي؛ وفي حال كانت الظروف خطيرة، فيجوز لها فرض حظر لمدة 5 إلى 15 يومًا ويجوز لها فرض غرامة بمبلغ يتراوح ما بين 100,000 ومبلغ 1,000,000 رنمينبي.

وفي حالة تورط وحدات في التصرفات المنصوص عليها في الفقرة السابقة، تصادر هيئات الأمن العام المكتسبات غير القانونية وتفرض غرامة تتراوح ما بين 100,000 ومبلغ 1,000,000 رنمينبي؛ ويتم تغريم الأشخاص المسئولين مسئولية مباشرة وغيرهم من فريق العمل المسئول مسئولية مباشرة بما يتفق مع الفقرة السابقة.

في حالة مخالفة المادة 27 من هذا القانون، يجب على الأشخاص الذين يتلقون عقوبات إدارية من الأمن العام عدم المشاركة في إدارة أمن الفضاء الإلكتروني أو شغل المناصب الرئيسية في تشغيل الشبكات لمدة 5 سنوات؛ ويخضع من يتعرضون لعقوبات جنائية لحظر مدى الحياة على المشاركة في أعمال إدارة أمن الفضاء الإلكتروني وشغل المناصب الرئيسية في تشغيل الشبكات.

المادة 64: تُصدر الإدارة المختصة ذات الشأن أمرًا إلى مشغلي الشبكات وموفري منتجات أو خدمات الشبكات المخالفين للمادة 22 الفقرة 3 أو المادة 42 إلى المادة 43 من هذا القانون بانتهاك المعلومات الشخصية المحمية بموجب القانون بإجراء تصحيحات، ويجوز أن يتلقوا سواء بشكل مستقل أو متزامن إنذارات أو يخضعوا لمصادرة المكتسبات غير القانونية، و/أو تغريمهم بمبلغ يتراوح ما بين 1 إلى 10 أضعاف مبلغ المكتسبات غير القانونية؛ ويكون الحد الأقصى لمبلغ الغرامة 1,000,000 رنمينبي، ويتم فرض غرامة قدرها ما بين 10,000 إلى 100,000 رنمينبي على الأشخاص وفريق العمل المسئول مسئولية مباشرة؛ وفي حال كانت الظروف خطيرة، فيجوز للإدارة المختصة المعنية بالأمر فرض تعليق مؤقت للعمل، أو تعليق للأعمال من أجل التصحيحات، أو إغلاق مواقع الويب، أو إلغاء تراخيص العمل ذات الصلة، أو إلغاء رخص الأعمال.

في حالة مخالفة المادة 44 من هذا القانون بسرقة أو استخدام وسائل غير مشروعة من أجل الحصول على معلومات شخصية أو بيعها أو توفيرها بشكل غير قانوني للغير، ولم يمثل ذلك جريمة، تصادر هيئات الأمن العام المكتسبات غير القانونية وتفرض غرامة تتراوح قيمتها ما بين 1 إلى 10 أضعاف مبلغ المكتسبات غير القانونية، وفي حالة عدم وجود مكتسبات غير قانونية فسوف تفرض غرامة قدرها 1,000,000 رنمينبي بحد أقصى.

المادة 65: في حالة مخالفة مشغلي البنية التحتية للمعلومات الحيوية للمادة 35 من هذا القانون من خلال استخدام منتجات وخدمات الشبكات التي لم تخضع لعمليات فحص أمني أو لم تجتاز الاختبارات الأمنية، توجه الإدارة المعنية والمختصة أمرًا بوقف الاستخدام وتفرض غرامة بمبلغ يتراوح ما بين 1 إلى 10 أضعاف سعر الشراء؛ كما يتم تغريم الأشخاص وفريق العمل المسئول مسئولية مباشرة بمبلغ يتراوح بين 10,000 إلى 100,000 رنمينبي

المادة 66: في حالة مخالفة مشغلي البنية التحتية للمعلومات الحيوية للمادة 37 من هذا القانون من خلال تخزين بيانات الشبكة خارج حدود البلاد، أو توفير بيانات الشبكة لمن هم خارج حدود البلاد، تفرض الإدارة المختصة والمعنية أمرًا باتخاذ إجراءات تصحيحية، وتقدم إنذارًا، وتصادر المكتسبات غير المشروع، وتفرض غرامات ما بين 50,000 إلى 500,000 رنمينبي؛ ويجوز لها فرض تعليق مؤقت على التشغيل، أو تعليق الأعمال من أجل الإجراءات التصحيحية، أو إغلاق مواقع الويب، أو إلغاء تراخيص العمل ذات الصلة، أو إلغاء تصاريح العمل. ويتم تغريم الأشخاص المسئولين مسئولية مباشرة أو فريق العمل المسئول مسئولية مباشرة بمبلغ يتراوح ما بين 10,000 ومبلغ 100,000 رنمينبي.

المادة 67: في حالة مخالفة المادة 46 من هذا القانون من خلال تأسيس موقع على الويب أو مجموعة اتصالات تستخدم من أجل ارتكاب أنشطة غير قانونية أو إجرامية، أو في حالة استخدام الشبكة من أجل نشر معلومات مرتبطة بارتكاب أنشطة غير قانونية أو إجرامية، لكن لم يتم ارتكاب جريمة، تفرض مؤسسات الأمن العام حظرًا لمدة 5 أيام ويجوز لها فرض غرامة قدرها يتراوح ما بين 10,000 إلى 15,000 رنمينبي؛ ومتى ما كان الظروف خطيرة، فيجوز لها فرض حظر لمدة ما بين 5 ومدة 15 يومًا، ويجوز لها فرض غرامة ما بين 50,000 ومبلغ 500,000 رنمينبي. ويجوز لها أيضًا إغلاق مواقع الويب ومجموعات الاتصالات المستخدمة في الأنشطة الإجرامية أو غير القانونية.

وفي حالة تورط وحدات في التصرفات المشمولة في الفقرة السابقة، تفرض مؤسسات الأمن العام غرامة تتراوح ما بين 100,000 ومبلغ 500,000 رنمينبي؛ ويتم تغريم المدير الرئيسي وفريق العمل المسئول مسئولية مباشرة بما يتفق مع أحكام الفقرة السابقة.

المادة 68: في حالة مخالفة مشغلو الشبكات للمادة 47 من هذا القانون بعدم وقف نقل المعلومات التي تم فرض حظر على نقلها ونشرها من خلال القوانين أو الأنظمة الإدارية، أو عدم اتخاذ إجراءات تصحيحية مثل الحذف أو عدم حفظ السجلات ذات الصلة، تفرض الإدارة المختصة والمعنية أمرًا بالتصحيح وتقدم إنذارًا وتصادر المكاسب غير المشروعة؛ وفي حالة رفض التصحيح أو إذا كانت الظروف خطيرة، يتم فرض غرامة ما بين 100,000 وبين 500,000 رنمينبي، ويجوز فرض تعليق مؤقت للعمليات أو تعليق الأعمال من أجل إجراء التصحيح أو غلق مواقع الويب أو إلغاء تراخيص العمل ذات الصلة أو إلغاء تصاريح العمل؛ ويتم تغريم الأشخاص المسئولين مسئولية مباشرة وغيرهم من فريق العمل المسئول مسئولية مباشرة ما بين 10,000 إلى 100,000 رنمينبي.

وفي حالة عدم أداء موفرو خدمة المعلومات الإلكترونية وخدمة تنزيل التطبيقات البرمجية لواجبات الإدارة الأمنية المنوطة بهم والمنصوص عليها في الفقرة 2 بالمادة 48 من هذا القانون، تكون العقوبة وفقًا للأحكام المنصوص عليها في الفقرة السابقة.

المادة 69: توجه الإدارات المختصة والمعنية أمرًا إلى مشغلي الشبكات الذين يخالفون أحكام هذا القانون، ويرتكبون أي من التصرفات التالية، بإجراء تصحيحات؛ وفي حالة رفض التصحيحات أو إذا كانت الظروف خطيرة، يتم فرض غرامة تتراوح ما بين 50,000 إلى 500,000 رنمينبي، ويتم تغريم فريق الإدارة المسئول مسئولية مباشرة وغيرهم من أفراد العمل المسئولين مسئولية مباشرة بمبلغ يتراوح ما بين 10,000 ومبلغ 100,000 رنمينبي:

(1) عدم اتباع متطلبات واشتراطات الإدارات المختصة باعتماد تدابير تصحيحية مثل وقف نشر أو حذف المعلومات التي تحظر القوانين أو الأنظمة الإدارية نشرها أو توزيعها.

(2) رفض أو إعاقة الإدارات المعنية في أدائها للإشراف أو الفحص القانوني.

(3) رفض توفير الدعم والمساعدة الفنية لهيئات الأمن العام وهيئات الأمن التابعة للدولة.

المادة 70: تتم معاقبة نشر أو توزيع المعلومات المحظورة بموجب المادة 12 الفقرة 2 من هذا القانون أو غيرها من القوانين أو الأنظمة الإدارية بما يتفق مع الأحكام المنصوص عليها في القوانين والأنظمة الإدارية ذات الصلة.

المادة 71: إذا كان هناك تصرف يخالف الأحكام المنصوص عليها في هذا القانون، يتم تسجيلها في ملفات قيد ونشرها أمام الجماهير بما يتفق مع الأحكام والأنظمة الإدارية ذات الصلة.

المادة 72: في حالة عدم قيام مشغلي شبكات الشؤون الحكومية المؤسسية في الدولة بأداء واجبات حماية أمن الفضاء الإلكتروني وفقًا لما ينص عليه هذا القانون، توجه المؤسسة في المستوى الأعلى أو المؤسسات المعنية أمرًا بإجراء تصحيحات؛ ويتم فرض عقوبات على المديرين المسئولين مسئولية مباشرة وعلى فريق العمل الآخر المسئول مسئولية مباشرة.

المادة 73: في حالة مخالفة هيئات أمن الفضاء الإلكتروني والمعلوماتية وغيرها من الإدارات المعنية للأحكام المنصوص عليها في المادة 30 من هذا القانون باستخدام المعلومات الشخصية المستحصل عليها خلال أداء واجبات حماية أمن الفضاء الإلكتروني لأغراض أخرى، يتم فرض عقوبات على الأشخاص المسئولين مسئولية مباشرة وفريق العمل الآخر المسئول مسئولية مباشرة عن ذلك.

وفي حالة إغفال إدارات أمن الفضاء الإلكتروني والمعلومات وغيرهم من فرق العمل في الإدارات المختصة لواجباتهم، أو في حالة استغلال سلطتهم أو ممارسة المحسوبية، ولم يمثل ذلك جريمة، يتم فرض عقوبات بما يتفق مع أحكام القانون.

المادة 74: في حال ألحقت مخالفات الأحكام المنصوص عليها في هذا القانون أضرارًا بالغير، يتم تحمُّل المسئولية المدنية بما يتفق مع أحكام القانون.

أما في حالة مخالفة هذا القانون، بما يمثل مخالفة لإدارة النظام العام، يتم فرض عقوبات حسب النظام العام بما يتفق مع القانون؛ ومتى ما تقرر ارتكاب جريمة، يتم تتبع المسئولية الجنائية بما يتفق مع أحكام القانون.

المادة 75: في حالة تورط مؤسسات أو منظمات أو أفراد أجانب في أنشطة الهجمات أو التدخلات أو العبث أو الإضرار أو غير ذلك من الأنشطة التي تهدد البنية التحتية للمعلومات الحيوية في جمهورية الصين الشعبية، وتتسبب في عواقب خطيرة، يتم تتبع المسئولية القانونية بما يتق مع أحكام القانون؛ ويجوز لهيئات الأمن العام العاملة في ظل مجلس الدولة والإدارات المعنية أيضًا اتخاذ قرار بتجميد أصول المؤسسة أو المنظمة أو الأفراد واتخاذ ما يلزم من تدابير عقابية أخرى.

الفصل السابع: أحكام تكميلية

المادة 76: تحمل الكلمات التالية المعاني التالية الوارد في هذا القانون:

(1) "الشبكة" [网络]، وأيضًا "إلكتروني"] وتشير إلى نظام مؤلف من أجهزة كمبيوتر وغير ذلك من محطات المعلومات والمعدات ذات الصلة والتي تتبع قواعد وإجراءات محددة في جمع المعلومات وتخزينها ونقل وتبادلها ومعالجتها.

(2) "أمن الفضاء الإلكتروني" [网络安全، أيضًا "أمن الشبكة"] وتشير إلى اتخاذ التدابير اللازمة من أجل منع الهجمات الإلكترونية والتدخلات والتطفل والتمدير والاستخدام غير القانوني، بالإضافة إلى الحوادث غير المتوقعة، ووضع الشبكات في حالة تشغيل مستقرة ومعتمدة، إضافة إلى ضمان اكتمال وسرية السعة المتاحة لبيانات الشبكة والقدرة على استخدامها.

(3) "مشغلو الشبكات" [网络运营者] ويشير إلى أصحاب الشبكات ومديروها وموفري خدمة الشبكات.

(4) "بيانات الشبكة" [网络数据] وتشير إلى جميع أنواع البيانات الإلكترونية التي يتم جمعها وتجزينها ونقله ومعالجتها وتقديمها من خلال الشبكات.

(5) "المعلومات الشخصية" [个人信息] وتشير إلى جميع أنواع المعلومات المسجلة إلكترونيًا أو بوسيلة أخرى والتي تكون -عندم معاملتها وحدها أو مع معلومات أخرى- كافية لتحديد هوية شخصية طبيعية، بما في ذلك على سبيل المثال لا الحصر الأسماء الكاملة للأشخاص الطبيعيين وتواريخ ميلادهم وأرقام بطاقاتهم القومية ومعلوماتهم الإحصائية البيولوجية الشخصية، وأرقام هواتهم، وما إلى ذلك.

المادة 77: يجب أن تتبع حماية الأمن التشغيلي للشبكات التي تخزن أو تعالج معلومات تخص الأسرار القومية هذا القانون كما يجب أن تراعي الأحكام المنصوص عليها في القوانين والأنظمة الإدارية ذات الصلة بحماية السرية.

المادة 78: تتم صياغة قواعد حماية الأمن للشبكات العسكرية بمعرفة الهيئة العسكرية المركزية.

المادة 79: يسري العمل بهذا القانون اعتبارًا من 1 يونيو/حزيران 2017.

الملحق 2
تدابير إدارة أسماء نطاقات الإنترنت لوزارة الصناعة وتكنولوجيا المعلومات الصينية[31] (مقتطفات).

المادة 3 من التدابير التي حددتها وزارة الصناعة وتكنولوجيا المعلومات لتنفيذ "أعمال الإدارة والإشراف على خدمات أسماء النطاقات على مستوى البلاد، ومهامها الرئيسية هي: (1) صياغة قواعد وسياسات لإدارة أسماء نطاقات الإنترنت؛ و(2) صياغة نظام لأسماء نطاقات الإنترنت، والتخطيط لتطوير موارد أسماء النطاقات؛ و(3) تسيير أعمال إدارات تشغيل خادم ملف الجذر لأسماء النطاقات المحلية؛ و(4) تحمُّل المسئولية عن إدارة الشبكات وأمن المعلومات الخاص بنظام أسماء النطاقات؛ و(5) حماية المعلومات الشخصية للمستخدمين وحقوقهم ومصالحهم المشروعة طبقًا لأحكام القانون؛ و(6) تحمُّل المسئولية عن التنسيق الدولة فيما يخص أسماء النطاقات؛ و(7) إدارة خدمات حل أسماء النطاقات المحلية؛ و(8) إدارة الأنشطة الأخرى ذات الصلة بخدمات أسماء النطاقات".

نصت **المادة 10** من التدابير على أن "من يتقدم من أجل تأسيس خادم ملف جذر لأسماء النطاقات أو هيئة لإدارة خادم ملف جذر أسماء النطاقات يجب أن يفي بالشروط التالية: (1) أن يتم تأسيس خادم جذر أسماء النطاقات داخل حدود البلاد، وأن يتوافق مع الخطط المقابلة لتطوير الإنترنت ومتطلبات التشغيل الآمن والمستقر لنظام أسماء النطاقات".

المادة 11: على من يتقدم بطلب لتأسيس هيئة لإدارة خادم ملف جذر أسماء النطاقات استيفاء الشروط التالية:

(1) أن يتم تأسيس نظام إدارة أسماء النطاقات داخل حدود البلاد، وأن تتوافق أسماء نطاقات المستوى الأعلى التي يديرونها مع القوانين والأنظمة ومع الخطط المقابلة لتطوير الإنترنت ومتطلبات التشغيل الآمن والمستقر لنظام أسماء النطاقات؛

(2) [أن] يكونوا شخصيات اعتبارية مؤسسة وقائمة داخل حدود البلاد، وأن تتمتع الشخصية الاعتبارية والمستثمرين الرئيسيين فيها وفريق التشغيل والإدارة بالسمعة الطيبة؛

(3) أن تكون لديهم خطط تنمية وخطط تكنولوجية احترافية، بالإضافة إلى المنشآت والتمويل وفريق عمل من المتخصصين المناسبين للمشاركة في عمليات وإدارة أسماء نطاقات المستوى الأعلى، بالإضافة إلى توافق نظم إدارة المعلومات مع متطلبات هيئة إدارة الاتصالات السلكية واللاسلكية؛

(4) أن تكون لديهم إجراءات كاملة لإدارة أمن الشبكات والمعلومات، بما في ذلك فريق عمل الإدارة، والهياكل الإدارية لأمن الشبكات والمعلومات، وخطط معالجة الاستجابة للطوارئ وما يقابل ذلك من الإجراءات التكنولوجية والإدارية؛

(5) أن تكون لديهم القدرة على المشاركة في توثيق معلومات الهوية الحقيقية وحماية المعلومات الشخصية للمستخدمين، والقدرة على توفير خدمات طويلة المدى بالإضافة إلى آليات كاملة لمعالجة سحب الخدمات؛

(6) أن تكون لديهم هياكل لإدارة خدمة تسجيل أسماء النطاقات وآليات إشراف كاملة لهيئات خدمات تسجيل أسماء النطاقات؛

(7) المتطلبات الأخرى المنصوص عليها في القوانين والأنظمة الإدارية.

المادة 12: على من يتقدم بطلب لتأسيس هيئة لخدمات تسجيل أسماء النطاقات استيفاء الشروط التالية:

(1) أن يتم تأسيس نظام خدمة تسجيل أسماء النطاقات وقاعدة بيانات التسجيل وأنظمة حل المصادقة داخل حدود البلاد؛

(2) [أن] يكونوا شخصيات اعتبارية مؤسسة وقائمة داخل حدود البلاد، وأن تتمتع الشخصية الاعتبارية والمستثمرين الرئيسيين فيها وفريق التشغيل والإدارة بالسمعة الطيبة؛

(3) أن تكون لديهم المنشآت والتمويل وفريق عمل من المتخصصين المناسبين للمشاركة في خدمات تسجيل أسماء النطاقات، بالإضافة إلى توافق نظم إدارة المعلومات مع متطلبات هيئة إدارة الاتصالات السلكية واللاسلكية؛

(4) أن تكون لديهم القدرة على المشاركة في توثيق معلومات الهوية الحقيقية وحماية المعلومات الشخصية للمستخدمين، والقدرة على توفير خدمات طويلة المدى وآلية كاملة لمعالجة سحب الخدمات؛

(5) أن تكون لديهم هياكل لإدارة خدمة تسجيل أسماء النطاقات وآليات إشراف كاملة لهيئات خدمات تسجيل أسماء النطاقات؛

(6) أن تكون لديهم إجراءات كاملة لحماية أمن الشبكات والمعلومات، بما في ذلك فريق عمل الإدارة، والهياكل الإدارية لأمن الشبكات والمعلومات، وخطط معالجة الاستجابة للطوارئ وما يقابل ذلك من الإجراءات التكنولوجية والإدارية؛

و(7) المتطلبات الأخرى المنصوص عليها في القوانين والأنظمة الإدارية.

المادة 13: على من يتقدمون بطلب لتأسيس خادم جذر أسماء النطاقات وهيئة لإدارة خادم ملف الجذر، أو هيئة لإدارة تسجيل أسماء النطاقات تقديم مواد الطلب إلى وزارة الصناعة وتكنولوجيا المعلومات. وعلى من يتقدمون بطلب من أجل تأسيس هيئة لخدمة تسجيل أسماء النطاقات تقديم مواد الطلب إلى إدارة الاتصالات السلكية واللاسلكية المحلية الإقليمية أو الموجودة في المنطقة المستقلة أو التابعة للبلدية.

تشمل مواد الطلب ما يلي:

---

[31] وزارة الصناعة وتكنولوجيا المعلومات، تدابير إدارة أسماء نطاقات الإنترنت، 24 أغسطس/آب 2017 (ترجمة غير رسمية) https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/. تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.cac.gov.cn/2017-09/28/c_1121737753.htm.

(1) الظروف والأحوال الأساسية لوحدة العمل المتقدمة بالطلب
(2) مواد التوثيق والشهادات للإدارة الفعالة لخدمات أسماء النطاقات، بما في ذلك مواد التوثيق للنظم والمنشآت ذات الصلة، بالإضافة إلى قدرات الخدمات وهياكل الإدارة إضافة إلى الاتفاقيات المبرمة مع الهيئات الأخرى؛
(3) هياكل وتدابير حماية أمن الشبكات والمعلومات؛
(4) المواد التي تثبت سمعة وحدة الأعمال المتقدمة بالطلب؛
(5) خطاب التزام مُوقَّع من ممثل معيّن قانونًا ومؤهل لأداء الأعمال بإخلاص وطبقًا لأحكام القانون".
المادة 37: "عند توفير خدمات حل مصادقة أسماء النطاقات، لا يجوز التلاعب بمعلومات حل المصادقة دون ترخيص. ويجب ألا يتم إعادة توجيه حل مصادقة أسماء النطاقات توجيهًا ضارًا تجاه عناوين IP لأشخاص آخرين من جانب أي مؤسسة أو فرد".
تنص **المادة 41** في التدابير على أنه "عند الضرورة وبسبب يعود لدواعي الأمن القومي أو للتعامل مع الحوادث الطارئة، تلتزم هيئات إدارة خادم جذر أسماء النطاقات وهيئات إدارة التسجيل وهيئات خدمة تسجيل أسماء النطاقات باتباع تعليمات الهيئات الموحدة لتوجيه وتنسيق إدارة الاتصالات السلكية واللاسلكية، واحترام المتطلبات الإدارية لهيئات إدارة الاتصالات السلكية واللاسلكية.
المادة 46: "تلتزم هيئات إدارة الاتصالات السلكية واللاسلكية بإنشاء هياكل سجلات ائتمانية لهيئات إدارة خادم جذر أسماء النطاقات وهيئات إدارة تسجيل أسماء النطاقات وهيئات خدمة تسجيل أسماء النطاقات، مع الالتزام بقيد مخالفاتها لهذه التدابير -بالإضافة إلى العقوبة الإدارية التي تتلقاها- في ملف الائتمان".

الملحق 3
نظام أسماء النطاقات الصيني[32] (مقتطفات)

أولاً. يجوز أن تتألف جميع مستويات أسماء نطاقات الإنترنت في أمتنا من الحروف (a-z، A-Z، على أن تكون الحروف الكبيرة والصغيرة مترادفة)، والأرقام (0-9)، مع استخدام الشرطة (-)، أو الحروف الصينية؛ ويجب أن تستخدم جميع النطاقات النقطة (.) والروابط، ويجب أن تستخدم جميع مستويات أسماء النطاقات باللغة الصينية إما النقاط أو النقطة الصينية (。) والروابط.

ثانيًا: بالإضافة إلى نطاق ".CN" ونطاق ".中国" من المستوى الأعلى، يؤسس نظام أسماء نطاقات الإنترنت القومي العديد من نطاقات المستوى الأعلى باللغة الإنجليزية والصينية، على أن يكون من بينها نطاق "政务" [.gov] ونطاق ".公益" [.org - للمصلحة العامة حرفيًا] في المستوى الأعلى نطاقين من المستوى الأعلى مخصصين باللغة الصينية للمجموعات والهيئات الخاصة بالحزب والحكومة الوطنية وجميع مستويات إدارات الشؤون الحكومية الأخرى وللمؤسسات غير الربحية. يمكن مطالعة المخطط التوضيحي لنظام أسماء نطاقات الإنترنت الوطني على الرابط http://中国互联网域名体系.中国 أو "http://中国互联网域名体系.政务" أو "中国互联网域名体系.信息" **Error! Hyperlink reference not valid.**".

ثالثًا. يندرج تحت نطاق المستوى الأعلى الوطني ".CN" نوعان من نطاقات المستوى الأعلى، "نطاقات الفئات" و"نطاقات المنطقة الإدارية". وتم تأسيس تسعة "نطاقات للفئات"، وهي على وجه التحديد: "政务" ويستخدم لمجموعات وهيئات الحزب والحكومة في جميع مستويات إدارات الحزب والشؤون الحكومية الأخرى؛ و"公益" ويستخدم للمؤسسات غير الربحية؛ و"GOV" ويستخدم للهيئات الحكومية؛ و"ORG" ويستخدم للمؤسسات غير الربحية؛ و"AC" ويستخدم لمعاهد الأبحاث العلمية؛ و"COM" ويستخدم للمؤسسات الصناعية والتجارية والمالية وغيرها من المؤسسات؛ و"EDU" ويستخدم للهيئات التعليمية؛ و"MIL" ويستخدم لمؤسسات الدفاع الوطني؛ و"NET" ويستخدم للمؤسسات التي توفر خدمات الإنترنت.
وتم تأسيس أربعة وثلاثين "نطاق منطقة إدارية"، من المقرر استخدامها لكل مقاطعات الدولة والمناطق ذات الحكم الذاتي، والبلديات ذات الحكم المباشر، والمنظمات الخاصة للمنطقة الإدارية [...].

رابعًا. يجوز تقديم الطلبات من أجل تسجيل أسماء نطاقات المستوى الثاني مباشرة ضمن نطاق ".CN" ونطاق ".中国" الوطنيين من المستوى الأعلى.

[32] ترجمة القانون الصيني، نظام أسماء النطاقات الصيني، 5 مارس/آذار 2018 https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/ (ترجمة غير رسمية). تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://xn--eqrt2g.xn--vuq861b/#.

الملحق 4
قانون أمن البيانات لجمهورية الصين الشعبية (DSL)[33] (مقتطفات)

المادة 3: يشير لفظ "البيانات" المستخدمة في هذا القانون إلى أي سجل للمعلومات في شكل إلكتروني أو أي أشكال أخرى.
- تشمل معالجة البيانات جمع البيانات وتخزينها واستخدامها ومعالجتها ونقلها وتوفيرها والإفصاح عنها وما إلى ذلك.
- يشير أمان البيانات إلى استخدام التدابير اللازمة لضمان حماية البيانات بشكل فعال واستخدامها قانونيًا، فضلاً عن امتلاك القدرة على ضمان حالة أمنية مستدامة.

المادة 7: تحمي الدولة حقوق ومصالح الأفراد والمنظمات فيما يتعلق بالبيانات، كما تشجع على الاستخدام القانوني والمعقول والفعال للبيانات؛ وتضمن التدفق الحر والقانوني والمنظم للبيانات؛ وتعزز تنمية اقتصاد رقمي على أن تكون البيانات أحد العوامل الرئيسية.

المادة 11: تنفذ الدولة بخطى حثيثة حوارات وتعاون دولي في قطاعات حوكمة أمن البيانات وتطوير البيانات واستخدامها، كما تشارك في صياغة القواعد والمعايير الدولية المتعلقة بأمن البيانات، وتعزز التدفق الآمن والحر للبيانات عبر الحدود.

المادة 14: تنفذ الدولة استراتيجية بيانات كبيرة، مع المضي قدمًا في تأسيس البنية التحتية للبيانات، وتشجيع ودعم التطبيقات الابتكارية للبيانات في كل صناعة ومجال.

المادة 17: يتعين على الدولة المضي قدمًا في إنشاء نظام معايير لتطوير البيانات وتقنيات استغلالها وأمن البيانات. وفي نطاق مهام كل إدارة من إدارات مجلس الدولة المسؤولة عن التقييس وغيرها من الإدارات ذات الصلة في مجلس الدولة، يتعين على كل منها تنظيم الصياغة والمراجعة المناسبة للمعايير المتعلقة بالتكنولوجيا والمنتجات الخاصة بتطوير واستخدام البيانات وأمن البيانات. تدعم الدولة المؤسسات والمجموعات الاجتماعية والهيئات التعليمية أو البحثية وغيرها في المشاركة في صياغة المعايير.

المادة 21: البيانات ذات الصلة بالأمن القومي وشريان حياة الاقتصاد الوطني وأسباب الرزق الهامة للشعب والمصالح العامة الرئيسية وغيرها مما يرتبط بالبيانات الجوهرية الوطنية تنطبق على نظام إدارة أكثر صرامة.

المادة 25: على الدولة تنفيذ ضوابط التصدير وفقًا للقانون بالنسبة للبيانات التي تخضع للرقابة والمتعلقة بالحفاظ على الأمن القومي والوفاء بالالتزامات الدولية.

المادة 26: في حالة استخدام أي دولة أو منطقة تدابير تمييزية أو تقييدية أو غيرها من الإجراءات المماثلة ضد جمهورية الصين الشعبية في مجالات مثل الاستثمار أو التجارة في البيانات والتكنولوجيا لاستغلال البيانات وتطويرها، يجوز لجمهورية الصين الشعبية استخدام تدابير مماثلة ضد تلك الدولة أو المنطقة بناءً على الظروف الفعلية.

المادة 27: يجب أن يحقق تنفيذ أنشطة معالجة البيانات عبر شبكات المعلومات واجبات حماية أمن البيانات على أساس نظام حماية أمن متعدد المستويات لأمن الفضاء الإلكتروني.

المادة 31: تسري أحكام قانون أمن الفضاء الإلكتروني لجمهورية الصين الشعبية على الإدارة الأمنية لتصدير البيانات من المنطقة [البر الرئيسي] التي تم جمعها أو إنتاجها بمعرفة مشغلي البنية التحتية للمعلومات الحيوية داخل المنطقة [البر الرئيسي] لجمهورية الصين الشعبية؛ على أن تتم صياغة إجراءات الإدارة الأمنية لتصدير البيانات الهامة من منطقة البر الرئيسي التي تم جمعها أو إنتاجها من قبل معالجي البيانات الآخرين داخل أراضي [البر الرئيسي] لجمهورية الصين الشعبية بمعرفة إدارة معلومات الإنترنت بالدولة بالتعاون مع الإدارات ذات الصلة في مجلس الدولة.

المادة 32: يجب على أي منظمة أو فرد يقوم بجمع البيانات أن يستخدم طرقًا قانونية ومناسبة ولا يجوز له سرقة البيانات أو الحصول عليها بطرق أخرى غير قانونية. وإذا احتوت القوانين واللوائح الإدارية على أحكام بشأن غرض أو نطاق جمع البيانات واستخدامها، فيجب جمع البيانات أو استخدامها ضمن الغرض والنطاق المنصوص عليهما في تلك القوانين واللوائح الإدارية.

المادة 33: تلتزم المؤسسات العاملة في خدمات وساطة معاملات البيانات عند توفر خدمات بمطالبة الطرف الذي يقدم البيانات بتوضيح مصادر البيانات، والتحقق من هويات طرفي المعاملة، وتخزين سجل للمراجعة والمعاملة.

المادة 36: تلتزم الهيئات المختصة في دولة جمهورية الصين الشعبية -وبموجب الأحكام المنصوص عليها في القوانين والمعاهدات أو الاتفاقيات المبرمة مع جمهورية الصين الشعبية أو التي تكون الصين طرفًا فيها، أو بموجب مبدأ المساواة والمنافع المشتركة- بمعالجة طلب توفير البيانات من هيئة قضائية أو هيئة إنفاذ قانون أجنبية. ولا يجوز للمؤسسات أو الأفراد داخل منطقة [البر الرئيسي] لجمهورية الصين الشعبية توفير بيانات داخل [البر الرئيسي] لجمهورية الصينة الشعبية إلى هيئة قضائية أو جهة إنفاذ قانون أجنبية دون الحصول على موافقة هيئات الدولة المختصة في جمهورية الصين الشعبية.

المادة 38: يجب أن يكون أداء هيئات الدولة للواجبات المحددة قانونًا وتتطلب جمعًا واستخدامًا للبيانات في حدود نطاق الواجبات المحددة قانونًا ومزاولتها بما يتفق مع المتطلبات والإجراءات المنصوص عليها في القوانين والأنظمة الإدارية؛ وبأداء واجبات معرفة الخصوصية

---

[33] قانون أمن البيانات في جمهورية الصين الشعبية، 11 يونيو/حزيران 2021، حسب الترجمة هنا: https://www.secrss.com/articles/31844 (ترجمة غير رسمية، ويوجد المنشور الأصلي هنا: http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm).
تمت ترجمة هذه الوثيقة إلى لغات متعددة للعلم بها فقط. ويمكن الحصول على النص الأصلي والموثوق (باللغة الصينية) في: http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm.

الشخصية والمعلومات الشخصية والأسرار التجارية ومعلومات الأعمال السرية وغيرها من البيانات فيجب الحفاظ على سريتها بما يتفق مع أحكام القانون، ولا يجوز الإفصاح عنها أو تقديمها بشكل غير قانوني للغير.

المادة 40: تلتزم هيئات الدولة التي تعهد للغير بمهمة تأسيس أو حفظ أنظمة إلكترونية للشئون الحكومية أو بتخزين أو معالجة بيانات الشؤون الحكومية باتباع إجراءات الموافقة الصارمة مع الالتزام بالإشراف على أداء التزامات حماية أمن البيانات المقابلة بمعرفة الأطراف الموكل إليها تلك المهام. يلتزم الطرف المعهود إليه بالمهام بأن يؤدي التزامات حماية أمن البيانات بما يتفق مع الأحكام المنصوص عليها في القوانين والأنظمة والاتفاقيات التعاقدية، ولا يجوز له حفظ أو استخدام أو كشف بيانات الشؤون الحكومية أو توفيرها للغير دون ترخيص.

المادة 44: في حالة اكتشاف الإدارات التنظيمية المعنية التي تجري واجبات الإشراف على أمن البيانات وإداراتها أن أنشطة معالجة البيانات تنطوي على مخاطر أمنية أكبر، فيجوز أن تقدم توبيخًا إلى تلك المؤسسات والأفراد ومطالبتها بتفعيل إجراءات واتخاذ تصحيحات وإزالة المخاطر الخفية بما يتفق مع الصلاحيات والإجراءات المقدمة.

المادة 49: في حالة عدم إجراء هيئات الدولة لالتزامات حماية أمن البيانات وفقًا لما ينص عليه هذا القانون، يتم فرض عقوبات على المديرين المسئولين مسئولية مباشرة وعلى أفراد العمل المسئولين مسئولية مباشرة وذلك بما يتفق مع أحكام القانون.

المادة 52: في حال ألحقت مخالفات الأحكام المنصوص عليها في هذا القانون أضرارًا بالغير، يتم تحمُّل المسئولية المدنية بما يتفق مع أحكام القانون.

الملحق 5

قانون حماية المعلومات الشخصية لجمهورية الصين الشعبية[34]

(تم تمريره في الاجتماع الثلاثين للجنة الدائمة التابعة للمؤتمر الشعبي القومي الثالث عشر في 20 أغسطس 2021)

الفصل الأول: الأحكام العامة
الفصل الثاني: قواعد معالجة المعلومات الشخصية
القسم 1: أحكام اعتيادية
القسم 2: قوانين للتعامل مع المعلومات الشخصية الحساسة
القسم 3: أحكام خاصة حول التعامل مع المعلومات الشخصية من جانب هيئات الدولة
الفصل الثالث: قواعد لتوفيري المعلومات الشخصية عبر الحدود
الفصل الرابع: حقوق الأفراد في أنشطة معالجة المعلومات الشخصية
الفصل الخامس: واجبات معالجي المعلومات الشخصية
الفصل السادس: الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية
الفصل السابع: المسئولية القانونية
الفصل الثامن: أحكام تكميلية

الفصل الأول: الأحكام العامة

المادة 1: تمت صياغة هذا القانون على أساس الدستور من أجل حماية حقوق ومصالح المعلومات الشخصية، ووضع معايير لأنشطة التعامل مع المعلومات الشخصية، وتعزيز الاستخدام الرشيد للمعلومات الشخصية.

المادة 2: تحظى المعلومات الشخصية للشخصيات الطبيعية بالحماية القانونية؛ حيث لا يجوز لأي مؤسسة أو فرد انتهاك حقوق ومصالح المعلومات الشخصية للشخصيات الطبيعية.

المادة 3: ينطبق هذا القانون على أنشطة معالجة المعلومات الشخصية للأشخاص الطبيعيين ضمن حدود جمهورية الصين الشعبية.
وفي حالة وجود أي من الظروف التالية في أنشطة التناول خارج حدود جمهورية الصين الشعبية للمعلومات الشخصية الخاصة بالأشخاص الطبيعيين ضمن حدود جمهورية الصين الشعبية، فإن هذا القانون يسري أيضًا"

1. عندما يكون الغرض هو توفير منتجات أو خدمات إلى أشخاص طبيعيين داخل الحدود.
2. عند تحليل أو تقييم أنشطة الأشخاص الطبيعيين داخل الحدود.
3. الظروف الأخرى المنصوص عليها في القوانين أو الأنظمة الإدارية.

المادة 4: المعلومات الشخصية هي جميع أنواع المعلومات التي يتم تسجيلها عن طريق الوسائل الإلكترونية أو غيرها ذات , الصلة بالأشخاص الطبيعيين أصحاب الهويات المعروفة أو القابلة للتعرف عليها، ولا تشمل المعلومات بعد التعامل مع تجهيل الهوية.
ويشمل التعامل مع المعلومات الشخصية جمع المعلومات الشخصية وتخزينها واستخدامها ومعالجتها ونقلها وتوفيرها والإفصاح عنها وحذفها، إلخ.

المادة 5: تُراعى مبادئ الشرعية والملكية والضرورة والمصداقية في معالجة المعلومات الشخصية. ويُحظر معالجة المعلومات الشخصية بطريقة مضللة أو خادعة أو بطريق الإكراه أو غير ذلك من الطرق.

المادة 6: يكون لمعالجة المعلومات الشخصية هدف واضح ومعقول، ويكون مرتبط ارتباطًا مباشرًا بغرض المعالجة، من خلال استخدام الطريقة ذات التأثير الأقل على حقوق ومصالح الأفراد.
يكون جمع المعلومات الشخصية مقتصرًا على أضيق نطاق لتحقيق الغرض من المعالجة، ويحظر القيام بجمع موسع للمعلومات الشخصية.

المادة 7: تُراعى مبادئ الانفتاح والشافية في التعامل مع المعلومات الشخصية، من خلال الإفصاح عن قواعد معالجة المعلومات الشخصية مع الإشارة بوضوح لغرض وطريقة ونطاق المعالجة.

المادة 8: تضمن معالجة المعلومات الشخصية جودة المعلومات الشخصية، وتتجنب التأثيرات الضارة على حقوق ومصالح الأفراد من المعلومات الشخصية غير الدقيقة أو غير المكتملة.

المادة 9: يتحمل معالجو المعلومات الشخصية المسئولية عن أنشطتهم في معالجة المعلومات الشخصية، واعتماد التدابير اللازمة من أجل حفظ أمن المعلومات الشخصية التي يعالجونها.

[34] قانون حماية المعلومات الشخصية بجمهورية الصين الشعبية (تم تمريره في الاجتماع الثلاثين للجنة الدائمة التابعة للمؤتمر الشعبي القومي الثالث عشر في 20 أغسطس 2021)، http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml، حسب ترجمة DigiChina هنا: https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021

المادة 10: لا يجوز لأي مؤسسة أو فرد القيام بجمع أو استخدام أو معالجة أو نقل المعلومات الشخصية للغير بطريقة غير قانونية، أو بيع أو شراء أو توفير أو الإفصاح غير القانوني عن المعلومات الشخصية للغير، أو المشاركة في أنشطة معالجة المعلومات الشخصية بما يضر الأمن القومي أو المصلحة العامة.
المادة 11: تؤسس الدولة هيكلاً لحماية المعلومات الشخصية بهدف منع ومعاقبة التصرفات التي تلحق الضرر بحقوق ومصالح المعلومات ولتقوية نشر حماية المعلومات الشخصية والتوعية بها، ولتعزيز إيجاد بيئة جيدة لحماية المعلومات الشخصية، مع المشاركة التضامنية من جانب الحكومة والشركات والمؤسسات الاجتماعية المعنية وعامة الجماهير.
المادة 12: تشارك الدولة بقوة في صياغة القوانين [أو الأعراف] الدولية لحماية المعلومات الشخصية، والتعاون على الحوار والتعاون الدوليين في مجال حماية المعلومات الشخصية، وتعزيز الاعتراف المتبادل بقواعد [أعراف] حماية المعلومات الشخصية ومعاييرها إلخ، مع الدول والمناطق والمؤسسات الدولية.

الفصل الثاني: قواعد معالجة المعلومات الشخصية

القسم 1: أحكام اعتيادية

المادة 13: لا يجوز لمعالجي المعلومات الشخصية معالجة المعلومات الشخصية متى ما توافقت مع واحدة من الظروف التالية:
1. الحصول على موافقة الأفراد.
2. متى ما كان ضروريًا لإبرام أو إنجاز عقد يكون فيه الشخص طرفًا معنيًا، أو متى ما كان ضروريًا لإجراء إدارة للموارد البشرية طبقًا لقواعد وهياكل العمل المصاغة صياغة قانونية والعقود الجماعية المبرمة قانونًا.
3. عندما يكون من الضروري إنجاز الواجبات والمسئوليات النظامية أو الالتزامات النظامية.
4. عندما يكون من الضروري الاستجابة لحوادث الصحة العامة المفاجئة أو حماية حياة وصحة الشخصيات الطبيعية، أو أمن ممتلكاتهم، بموجب الظروف الطارئة.
5. معالجة المعلومات الشخصية ضمن النطاق المعقول لتنفيذ تقارير إخبارية ومراقبة الرأي العام، وغير ذلك من الأنشطة التي تحقق المصلحة العامة.
6. عند معالجة المعلومات الشخصية التي يفصح عنها الأشخاص أنفسهم أو التي تم الإفصاح عنها بالفعل بشكل قانوني، ضمن نطاق معقول بما يتفق مع أحكام هذا القانون.
7. الظروف الأخرى المنصوص عليها في القوانين والأنظمة الإدارية.

طبقًا للأحكام الأخرى ذات الصلة في هذا القانون، يجب الحصول على موافقة الشخص عند معالجة المعلومات الشخصية. وعلى الرغم من ذلك، لا يلزم الحصول على موافقة الأفراد في الظروف المقررة في البند 2 إلى البند 7 أعلاه.
المادة 14: في حالة معالجة المعلومات الشخصية استنادًا إلى موافقة الأفراد، يتم تقديم الموافقة المذكورة بموجب شرط المعرفة الكاملة، وفي بيان طوعي وواضح. إذا نصت القوانين والأنظمة الإدارية على ضرورة الحصول على موافقة منفصلة أو موافقة خطية لمعالجة المعلومات الشخصية، فيجب اتباع تلك الأحكام.
في حالة حدوث تغيير غرض معالجة المعلومات الشخصية، أو طريقة المعالجة أو فئات المعلومات الشخصية المعالجة، يجب الحصول على موافقة الشخص مرة أخرى.
المادة 15: في حالة معالجة المعلومات الشخصية استنادًا إلى موافقة الأفراد، يكون للأفراد الحق في إلغاء موافقتهم. يلتزم معالجو المعلومات الشخصية بتوفير طريقة ملائمة لسحب الموافقة.
في حالة إلغاء أي فرد موافقته، فلا يؤثر ذلك على فاعلية أنشطة معالجة المعلومات الشخصية المنفذة على أساس موافقة الفرد قبل إلغاء الموافقة.
المادة 16: لا يجوز لمعالجي المعلومات الشخصية رفض توفير المنتجات أو الخدمات على أساس عدم موافقة الفرد على معالجة معلوماته الشخصية أو إلغاء موافقته، باستثناء إذا كانت معالجة المعلومات الشخصية ضرورية من أجل توفير المنتجات والخدمات.
المادة 17: يلتزم معالجو المعلومات الشخصية -وقبل معالجة المعلومات الشخصية- بإشعار الأفراد بوضوح وبأمانة ودقة وبالكامل عن البنود التالية من خلال استخدام صياغة واضحة وسهلة الفهم:
1. الاسم أو الاسم الشخصي وطريقة الاتصال بمعالج المعلومات الشخصية.
2. الغرض من معالجة المعلومات الشخصية وطرق المعالجة، وفئات المعلومات الشخصية الخاضعة للمعالجة، بالإضافة إلى فترة الاحتجاز.
3. الطرق والإجراءات المتاحة للأفراد من أجل ممارسة الحقوق المنصوص عليها في هذا القانون.
4. ويجب تقديم إشعار بالبنود التي تنص عليها القوانين والأنظمة الإدارية الأخرى.

في حالة وقوع تغيير في المسائل المنصوص عليها في الفقرة السابقة، يتم إشعار الأفراد بذلك التغيير.
في حالة قيام معالجو المعلومات الشخصية بتقديم إشعار بالأمور المنصوص عليها في الفقرة 1 من خلال طريقة صياغة قواعد التعامل مع المعلومات الشخصية، يتم الإعلان [الإفصاح] عن قواعد المعالجة وتسهيل قراءتها وتخزينها.
المادة 18: يجوز لمعالجي المعلومات الشخصية القائمين على معالجة المعلومات الشخصية عدم تقديم إشعار للأفراد حول البنود المنصوص عليها في الفقرة 1 من المادة السابقة في الظروف التي تنص فيها القوانين والأنظمة الإدارية على الحفاظ على السرية أو عدم ضرورة تقديم إشعارات.

في ظل الظروف الطارئة، ومتى كان من المستحيل إشعار الأفراد في الوقت المناسب من أجل حماية حياة وصحة الشخصيات الطبيعية وأمن ممتلكاتهم، يلتزم معالجو المعلومات الشخصية بإشعارهم بعد زوال الظروف الطارئة.

المادة 19: تكون فترات احتجاز المعلومات الشخصية هي أقصر فترة لازمة لتحقيق الغرض من معالجة المعلومات الشخصية، إلا إذا نصت القوانين والأنظمة الإدارية على خلاف ذلك.

المادة 20: في حالة قرر اثنان أو أكثر من معالجي المعلومات الشخصية بالتضامن فيما بينهم غرضًا لمعالجة المعلومات الشخصية وطريقة المعالجة، فيلتزمون بالاتفاق على حقوق والتزامات كل منهم. وعلى الرغم من ذلك، لا تؤثر هذه الاتفاقية على حقوق الأفراد في مطالبة أي معالج واحد للبيانات الشخصية بالعمل وفقًا لأحكام هذا القانون.

في حال تسبب معالجو المعلومات الشخصية المتضامنين في معالجة المعلومات الشخصية في الإضرار بحقوق ومصالح المعلومات الشخصية، بما يؤدي إلى أضرار تعويضية، فإنهم يتحملون المسئولية التضامنية طبقًا لأحكام القانون.

المادة 21: إذا قام معالجو المعلومات الشخصية بتعهيد وإسناد معالجة المعلومات الشخصية للغير، فيلتزمون بإبرام اتفاقية مع الشخص المسند إليه حول أعمال المعالجة الموكلة إليه والمدة الزمنية وطريقة المعالجة وفئات المعلومات الشخصية وتدابير الحماية، إضافة إلى حقوق وواجبات كل الطرفين، إلخ، وإجراء مراقبة على أنشطة معالجة المعلومات الشخصية للشخص الموكل إليه.

يلتزم الأشخاص الموكل إليهم مهمة المعالجة بمعالجة المعلومات الشخصية طبقًا لأحكام الاتفاقية؛ ولا يجوز لهم معالجة المعلومات الشخصية لأغراض معالجة أو بطرق معالجة وغيره تتجاوز حدود المتفق عليه. إذا لم يدخل عقد الإسناد حيز التنفيذ أو إذا كان باطلاً أو تم إلغاؤه أو إنهاؤه، يلتزم الشخص المعهود إليه بإعادة المعلومات الشخصية إلى معالج المعلومات الشخصية أو حذفها، ولا يجوز له الاحتفاظ بها.

لا يجوز للشخص المعهود إليه أن يعهد بمعالجة المعلومات الشخصية للغير من الباطن دون الحصول على موافقة معالج المعلومات الشخصية.

المادة 22: يلتزم معالجو المعلومات الشخصية -متى ما كان من الضروري نقل المعلومات الشخصية بسبب أعمال الاندماج أو الفصل أو الحل أو إعلان الإفلاس وغير ذلك من الأسباب- بإشعار الأفراد باسم الطرف المتلقي للمعلومات أو الاسم الشخص وطريقة الاتصال. يواصل الطرف المتلقي للمعلومات أداء الواجبات المفروضة على معالج المعلومات الشخصية. وفي حالة قيام الطرف المتلقي للمعلومات بتغيير الغرض الأصلي للمعالجة أو طريقة المعالجة، فيلتزم بإشعار الفرد مرة أخرى وفقًا لأحكام هذا القانون.

المادة 23: في حالة قيام معالجو المعلومات الشخصية بتزويد معالجين آخرين للمعلومات الشخصية بالمعلومات الشخصية التي يعالجونها، فيجب عليهم إشعار الأفراد بالاسم والاسم الشخصي للمتلقي، وطريقة الاتصال به، والغرض من المعالجة وطريقتها، بالإضافة إلى فئات المعلومات الشخصية، مع الحصول على موافقة منفصلة من الفرد. يعالج المتلقون المعلومات الشخصية في حدود النطاق المذكور أعلاه لأغراض المعالجة، وطرق المعالجة، وفئات المعلومات الشخصية، إلخ. وفي حالة قيام المتلقين لغرض المعالجة الأصلي أو طرق المعالجة، فيجب عليهم الحصول مرة أخرى على موافقة الفرد.

المادة 24: إذا استخدم معالجو المعلومات الشخصية معلومات شخصية لإجراء اتخاذ تلقائي للقرارات، يجب ضمان شفافية اتخاذ القرارات وإنصاف وعدالة نتيجة المعالجة، ولا يجوز لهم المشاركة في أي معالجة تفضيلية غير معقولة للأفراد في الظروف التجارية مثل السعر التجاري، إلخ.

على من يجرون تسليمًا للمعلومات من قبل المرسل أو مبيعات تجارية إلى الأفراد من خلال طرق اتخاذ قرارات تلقائية أن يوفروا على الفور خيار عدم استهداف خصائص الأفراد، أو تزويد الأفراد بطريقة مناسبة للرفض.

عندما يثمر استخدام اتخاذ القرارات التلقائية إلى قرارات ذات تأثير كبير على حقوق ومصالح الفرد، يكون له الحق في مطالبة معالجي المعلومات الشخصية بتفسير وشرح الأمر، ويكون لهم الحق في رفض قيام معالجي المعلومات الشخصية اتخاذ القرارات وحدهم من خلال طرق اتخاذ القرارات التلقائية.

المادة 25: لا يجوز لمعالجي المعلومات الشخصية الإفصاح عن المعلومات التي يعالجونها إلا في حالة الحصول على موافقة منفصلة.

المادة 26: يتم تثبيت معدات جمع الصور والتعرف على الهويات الشخصية في الأماكن العامة حسب المطلوب لحماية الأمن العام ومراعاة أنظمة الدولة ذات الصلة، مع تثبيت وتركيب لافتات توضيحية واضحة. لا يجوز استخدام ما يتم جمعه من صور شخصية ومعلومات محددة ومميزة للهوية الشخصية إلا لأغراض حماية الأمن العام؛ ولا يجوز استخدامها لأغراض أخرى، باستثناء الحصول على موافقة منفصلة من الأفراد.

المادة 27: يجوز لمعالجي المعلومات الشخصية -في حدود نطاق معقول- معالجة المعلومات الشخصية التي كشف عنها بالفعل الشخص المعنيّ أو غيره بطريقة مشروعة، عدا حالات الرفض الواضح من الشخص المعنيّ. يلتزم معالجو المعلومات الشخصية الذين يعالجون معلومات شخصية معلنة بالفعل وعندما يكون هناك تأثير كبير على حقوق ومصالح الأفراد بالحصول على الموافقة الشخصية وفقًا للأحكام المنصوص عليها في هذا القانون.

القسم الثاني: قواعد للتعامل مع المعلومات الشخصية الحساسة

المادة 28: يقصد بالمعلومات الشخصية الحساسة المعلومات الشخصية التي قد يسهل أن تتسبب عند تسربها أو استخدامها استخدامًا غير قانوني في ضرر لكرامة الشخصيات الطبيعية أو ضرر جسيم للأمن الشخصي أو للممتلكات، بما في ذلك المعلومات المتعلقة بالسمات البيولوجية والمعتقدات الدينية والحالة المحددة تحديدًا خاصًا والصحة الطبية والحسابات المالية وتعقب مواقع الأفراد إلخ، بالإضافة إلى المعلومات الشخصية للقاصرين تحت سن 14 سنة.

ولا يجوز لمعالجي المعلومات الشخصية معالجة المعلومات الشخصية الحساسة إلا إذا كان هناك غرض محدد وظروف تفرض ضرورة تنفيذ تدابير حماية صارمة.
المادة 29: لمعالجة المعلومات الشخصية الحساسة، يجب الحصول على الموافقة المنفصلة للفرد. إذا نصت القوانين والأنظمة الإدارية على ضرورة الحصول على موافقة خطية لمعالجة المعلومات الشخصية الحساسة، فيجب اتباع تلك الأحكام.
المادة 30: يلتزم معالجو المعلومات الشخصية الذين يعالجون معلومات شخصية حساسة، بالإضافة إلى الأحكام المنصوص عليها في المادة 17، الفقرة 1 من هذا القانون أيضًا بإشعار الأفراد بالضرورة والتأثير على حقوق ومصالح الفرد في معالجة المعلومات الشخصية الحساسة، عدا الحالات التي ينص فيها هذا القانون على جواز عدم إشعار الأفراد.
المادة 31: في حالة قيام معالجو المعلومات الشخصية بمعالجة معلومات شخصية لقاصرين تحت سن 14 عامًا، فيلتزمون بالحصول على موافقة الأبوين أو ولي أمر آخر للقاصر.
في حالة قيام معالجو المعلومات الشخصية بمعالجة معلومات شخصية لقاصرين تحت سن 14 عامًا، فيلتزمون بصياغة قواعد مخصصة لمعالجة المعلومات الشخصية.
المادة 32: إذا نصت القوانين والأنظمة الإدارية على ضرورة الحصول على تراخيص إدارية ذات صلة أو سريان قيود أخرى على معالجة معلومات شخصية حساسة، فيجب اتباع تلك الأحكام.

القسم الثالث: أحكام خاصة بخصوص هيئات الدولة التي تعالج معلومات شخصية

المادة 33: يسري هذا القانون على أنشطة هيئات الدولة التي تعالج معلومات حساسة؛ وفي حالة احتواء هذا القسم على أحكام خاصة، تسري أحكام هذا القسم.
المادة 34: تلتزم هيئات الدولة التي تعالج معلومات شخصية للوفاء بواجباتها والتزاماتها التعاقدية بإجرائها وفقًا للصلاحيات والإجراءات المنصوص عليها في القوانين أو الأنظمة الإدارية؛ ولا يجوز لهم تجاوز النطاق والمدى اللازم لإنجاز مهامهم والتزاماتهم النظامية.
المادة 35: تلتزم هيئات الدولة التي تعالج معلومات شخصية لغرض الوفاء بواجباتها والتزاماتها التعاقدية بإجراء واجبات الإشعار، باستثناء الحالات التي توجد بها الظروف الموضحة في المادة 18، الفقرة الأولى من هذا القانون، أو إذا كان الإشعار من شأنه إعاقة تنفيذ هيئات الدولة لواجباتها والتزاماتها التعاقدية.
المادة 36: يتم تخزين المعلومات الشخصية التي تقوم هيئات الدولة بمعالجتها داخل حدود البلاد بجمهورية الصين الشعبية. إذا كان من الضروري فعليًا توفيرها خارج البلاد، يتم إجراء تقييم للأمن. يجوز مطالبة الهيئات المعنية بالدعم والمساندة في التقييم الأمني.
المادة 37: تسري الأحكام المنصوص عليها في هذا القانون فيما يخص معالجة هيئات الدولة للمعلومات الشخصية على معالجة المعلومات الشخصية للوفاء بالواجبات النظامية للمنظمات المخولة بموجب القانون والأنظمة لإدارة وظائف الشئون العامة.

الفصل الثالث: قواعد لتوفيري المعلومات الشخصية عبر الحدود

المادة 38: في حال تعيّن بالفعل على معالجي المعلومات الشخصية تقديم المعلومات الشخصية خارج حدود جمهورية الصين الشعبية تلبية لمتطلبات الأعمال أو غيرها من المتطلبات، يجب عليهم استيفاء واحد من الشروط التالية:

1. اجتياز تقييم أمني تنظمه إدارة أمن الفضاء الإلكتروني والمعلوماتية في الدولة طبقًا لأحكام المادة 40 من هذا القانون.
2. الخضوع لتوثيق حماية المعلومات الشخصية تجريه هيئة مخصصة طبقًا للأحكام التي تفرضها إدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة.
3. إبرام عقد مع الجانب الأجنبي المتلقي للمعلومات طبقًا لعقد قياسي تصيغه إدارة أمن الفضاء الإلكتروني والمعلوماتية في الدولة، بالاتفاق على حقوق ومسئوليات كلا الطرفين.
4. الشروط الأخرى المنصوص عليها في القوانين أو الأنظمة الإدارية أو إدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة.

إذا كان من المقرر أن تحتوي المعاهدات والاتفاقية الدولية التي أبرمتها جمهورية الصين الشعبية أو انضمت إليها على أحكام ذات صلة مثل شروط توفير البيانات الشخصية خارج حدود جمهورية الصين الشعبية، فيجوز تنفيذ تلك الأحكام.
يعتمد معالجو المعلومات الشخصية التدابير اللازمة لضمان وصول أنشطة معالجة المعلومات الشخصية للأطراف الأجنبية المتلقية لها لمعيار حماية المعلومات الشخصية المنصوص عليه في هذا القانون.
المادة 39: إذا قدم معالجو المعلومات الشخصية معلومات شخصية خارج حدود جمهورية الصين الشعبية، فيلتزمون بإشعار الفرد باسم الجانب المتلقي للمعلومات أو الاسم الشخصي وطريقة الاتصال والغرض من المعالجة وطرق المعالجة وفئات المعلومات الشخصية، بالإضافة إلى الطرق أو الإجراءات اللازمة لممارسة الأفراد للحقوق المنصوص عليها في هذا القانون مع الطرف الأجنبي المتلقي للمعلومات، وغير ذلك من الأمور، والحصول على موافقة منفصلة من الأفراد.
المادة 40: يلتزم مشغلو البنية التحية للمعلومات الحيوية ومعالجو المعلومات الشخصية الذي يعالجون معلومات شخصية تصل إلى الكميات التي تقررها إدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة بتخزين المعلومات الشخصية التي يتم جمعها وتقديمها داخل حدود جمع المعلومات الشخصية على المستوى المحلي. وإذا تعيّن عليهم توفير تلك المعلومات خارج البلاد، فيجب أن يجتازوا التقييم الأمن الذي تنظمه إدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة؛ وإذا سمحت القوانين والأنظمة الإدارية وأحكام إدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة بدعم إجراء تقييم أمني، فيجب اتباع تلك الأحكام.

المادة 41: يجب على السلطات المختصة في جمهورية الصين الشعبية، وطبقًا للقوانين والمعاهدات ذات الصلة أو الاتفاقية الطوية التي أبرمتها جهات إنفاذ القانون أو انضمت إليها، أو طبقًا لمبدأ المساواة والمنفعة المتبادلة، معالجة طلبات الهيئات القضائية الأجنبية أو هيئات إنفاذ القانون فيما يخص توفير معلومات شخصية مخزنة محليًا. لا يجوز لمعالجي المعلومات الشخصية توفير المعلومات الشخصية المخزنة داخل أراضي جمهورية الصين الشعبية إلى هيئات قضائية أو وكالات إنفاذ قانون أجنبية دون الحصول على موافقة السلطات المختصة في جمهورية الصين الشعبية.

المادة 42: في حالة تورط مؤسسات أو أفراد أجانب في أعمال معالجة معلومات شخصية بما يخالف حقوق مواطني جمهورية الصين الشعبية ومصالحهم في المعلومات الشخصية، أو بما يلحق الضرر بالأمن القومي أو المصلحة العامة لجمهورية الصين الشعبية، يجوز لإدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة إدراجهم على قائمة تقيّد أو تحظر توفير المعلومات الشخصية، وإصدار إنذار واعتماد تدابير مثل تقييد أو حظر توفير المعلومات الشخصية إليهم، وما إلى ذلك.

المادة 43: في حالة تبنّي أي دولة أو منطقة حظرًا تمييزيًا أو قيود أو غير ذلك من التدابير المماثلة ضد جمهورية الصين الشعبية في مجال حماية المعلومات الشخصية، يجوز لجمهورية الصين الشعبية تبنّي تدابير مقابلة ضد تلك الدولة أو المنطقة بناءً على الظروف الفعلية.

الفصل الرابع: حقوق الأفراد في أنشطة معالجة المعلومات الشخصية

المادة 44: للأفراد الحق في المعرفة والحق في التقرير فيما يخص معلوماتهم الشخصية، ولهم الحق في تقييد أو رفض معالجة الغير لمعلوماتهم الشخصية، ما لم تنص القوانين أو الأنظمة الإدارية على خلاف ذلك.

المادة 45: للأفراد الحق في مشاورة معالجي معلوماتهم الشخصية والحصول منهم على نسخة منها، باستثناء الظروف المنصوص عليها في المادة 18، الفقرة 1 أو المادة 35 من هذا القانون.

إذا طلب الأفراد مراجعة أو نسخ معلوماتهم الشخصية، فيلتزم معالجو المعلومات الشخصية بتوفيرها دون تأخير.

إذا طلب الأفراد نقل معلوماتهم الشخصية إلى معالج معلومات شخصية من اختيارهم ويستوفي شروط إدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة، فيلتزم معالجو المعلومات الشخصية بتوفير قناة لنقلها.

المادة 46: إذا اكتشف الأفراد أن معلوماتهم الشخصية غير صحيحة أو غير مكتملة، فلهم الحق في مطالبة معالجي المعلومات الشخصية بتصحيح أو إكمال معلوماتهم الشخصية. إذا طلب الأفراد تصحيح أو إكمال معلوماتهم الشخصية، فيلتزم معالجو المعلومات الشخصية بالتحقق من المعلومات الشخصية وتصحيحها أو إكمالها دون تأخير.

إذا طلب الأفراد تصحيح معلوماتهم الشخصية أو الإضافة إليها، فيلتزم معالجو المعلومات الشخصية بالتحقق من المعلومات الشخصية وتصحيحها أو الإضافة إليها دون تأخير.

المادة 47: يبادر معالجو المعلومات الشخصية إلى حذف المعلومات الشخصية متى ما وقع أي من الظروف التالية؛ وإذا لم يسارع معالج المعلومات الشخصية إلى حذفها، يكون للأفراد الحق في طلب الحذف:

1. إذا تم تحقيق الهدف من المعالجة، أو كان من المستحيل تحقيقيه أو أن تحقيق هدف معالجة [المعلومات الشخصية] لم يعد ضروريًا.
2. توقف معالجو المعلومات الشخصية عن توفير المنتجات أو الخدمات أو انتهاء فترة الاحتفاظ.
3. إلغاء الفرد لموافقته.
4. قيام معالجو المعلومات الشخصية بمعالجة المعلومات الشخصية بالمخالفة للقوانين أو الأنظمة الإدارية أو الاتفاقيات.
5. الظروف الأخرى المنصوص عليها في القوانين أو الأنظمة الإدارية.

في حالة انتهاء فترة الاحتجاز التي نصت عليها القوانين أو الأنظمة الإدارية، أو كان من الصعب إجراء حذف المعلومات الشخصية، يلتزم معالجو المعلومات الشخصية بالتوقف عن معالجة المعلومات الشخصية باستثناء ما يكون للتخزين واتخاذ تدابير الأمن الوقائية اللازمة.

المادة 48: للأفراد الحق في مطالبة معالجي المعلومات الشخصية بشرح وتوضيح قواعد معالجة المعلومات الشخصية.

المادة 49: في حالة وفاة شخص طبيعي، يجوز لقرابته من الدرجة الأولى ولمصلحتهم المشروعة والقانونية ممارسة الحقوق المنصوص عليها في هذا الباب في الاطلاع على المعلومات الشخصية للمتوفى ونسخها وتصحيحها وحذفها وما إلى ذلك، إلا إذا كان المتوفى قد رتب خلاف ذلك قبل انقضاء أجله.

المادة 50: يقر معالجو المعلومات الشخصية آليات ملائمة لقبول ومعالجة الطلبات المقدمة من الأفراد لممارسة حقوقهم. وفي حالة رفضهم لطلبات الأفراد ممارسة حقوقها، فيلتزمون بتقديم سبب الفرض.

في حالة رفض معالجو المعلومات الشخصية لطلبات الأفراد بممارسة حقوقهم، يجوز للأفراد رفع قضية أمام إحدى المحاكم الشعبية طبقًا للقانون.

الفصل الخامس: واجبات معالجي المعلومات الشخصية

المادة 51: يلتزم معالجو المعلومات الشخصية -وعلى أساس الغرض من معالجة المعلومات الشخصية وطرق المعالجة وفئات المعلومات الشخصية إضافة إلى التأثير على حقوق ومصالح الأفراد وربما المخاطر الأمنية الحالية، إلخ- باعتماد الإجراءات التالية لضمان توافق معالجة المعلومات الشخصية مع الأحكام المنصوص عليها في القوانين والأنظمة الإدارية، ومنع الوصول غير المرخص إضافة إلى تسرب المعلومات الشخصية أو التشويه أو الفقد:

2. صياغة هياكل إدارية وقواعد تشغيلية داخلية.
3. تنفيذ إدارة مصنفة للمعلومات الشخصية.

4. اعتماد تدابير أمنية فنية مكافئة مثل التشفير ومنع اكتشاف الهوية، إلخ.
5. تقرير القيود التشغيلية المعقولة لمعالجة المعلومات الشخصية، وإجراء توعية بالأمن وتدريب للموظفين دوريًا.
6. صياغة وتنظيم تنفيذ خطط الاستجابة لحوادث الأمن المتعلقة بالمعلومات الشخصية.
7. التدابير الأخرى المنصوص عليها في القوانين أو الأنظمة الإدارية.

المادة 52: يلتزم معالجو المعلومات الشخصية الذي يعالجون معلومات شخصية تصل إلى الكميات التي تقررها إدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة بتعيين مسئولين عن حماية المعلومات الشخصية، كي يتحملوا المسئولية عن الإشراف على أنشطة معالجة المعلومات الشخصية بالإضافة إلى تدابير الحماية المعتمدة، إلخ.

يلتزم معالجو المعلومات الشخصية بالإفصاح عن طرق الاتصال بمسئولي حماية المعلومات الشخصية، إبلاغ الإدارات المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية بالأسماء الشخصية للمسئولية وطرق الاتصال بهم.

المادة 53: يلتزم معالجو المعلومات الشخصية خارج حدود جمهورية الصين الشعبية ووفقًا للأحكام المنصوص عليها في المادة 3، الفقرة 2 من هذا القانون بتأسيس هيئة مخصصة أو تعيين وكيل داخل حدود جمهورية الصين الشعبية لكي يكون مسئولاً عن المسائل ذات الصلة بالمعلومات الشخصية التي يعالجونها، وعليه الإبلاغ باسم الكيان المعني أو الاسم الشخصي للوكيل وطريقة الاتصال به، إلخ إلى الإدارات المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية.

المادة 54: يلتزم معالجو المعلومات الشخصية بالمشاركة الدورية في عمليات تدقيق لمعالجة المعلومات الشخصية والامتثال للقوانين والأنظمة الإدارية.

المادة 55: عند وقوع أي من الظروف التالية، يلتزم معالجو المعلومات الشخصية بإجراء تقييم لتأثير حماية المعلومات الشخصية مقدمًا، وتسجيل حالة المعالجة:

1. معالجة معلومات شخصية حساسة.
2. استخدام المعلومات الشخصية في إجراء اتخاذ قرارات تلقائية.
3. تعهيد معالجة المعلومات الشخصية للغير، من خلال تقديم المعلومات الشخصية إلى معالجين آخرين للمعلومات الشخصية، أو الإفصاح عن المعلومات الشخصية.
4. توفير معلومات شخصية خارج البلاد.
5. أنشطة معالجة المعلومات الشخصية الآخر ذات التأثير الكبير على الأفراد.

المادة 56: يشتمل محتوى تقييم تأثير حماية المعلومات الشخصية على ما يلي:

1. هل الغرض من معالجة المعلومات الشخصية وطريقة المعالجة قانونية ومشروعة وضرورية أم لا.
2. التأثير على حقوق ومصالح الأفراد والمخاطر الأمنية.
3. هل ما يتخذ من تدابير وقائية قانوني وفعال ومناسب لدرجة المخاطر أم لا.

يتم الاحتفاظ بتقارير تقييم أثر حماية المعلومات الشخصية وسجلات حالة المعالجة لمدة ثلاث سنوات على أقل تقدير.

المادة 57: في حالة وقوع أو إمكانية وقوع تسريب للمعلومات الشخصية أو العبث بها أو فقدانها، يلتزم معالجو المعلومات الشخصية على الفور باعتماد تدابير تصحيحية، وإشعار الدوائر المعنية بتنفيذ واجبات ومسئوليات حماية المعلومات الشخصية والأفراد. يشتمل الإشعار على البنود التالية:

1. فئات المعلومات والأسباب والأضرار المحتملة بسبب التسرب أو العبث أو الفقد الذي حدث أو ربما يكون قد حدث.
2. الإجراءات التصحيحية التي اتخذها معالج المعلومات الشخصية والتدابير التي يمكن للأفراد اعتمادها من أجل الحد من الضرر.
3. طريقة الاتصال بمعالج المعلومات الشخصية.

في حالة اعتماد معالجو المعلومات الشخصية تدابير لها القدرة على التجنب الفعال للأضرار الحادثة بسبب حالات تسرب المعلومات أو العبث بها أو فقدها، يجوز لمعالجي المعلومات الشخصية عدم إشعار الأفراد؛ وعلى الرغم من ذلك، إذا رأت الإدارات المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية إمكانية حدوث ضرر، فلهم مطالبة معالجي المعلومات الشخصية بإشعار الأفراد.

المادة 58: يلتزم معالجو المعلومات الشخصية الذين يقدمون خدمات هامة على منصات الإنترنت ولديهم عدد كبير من المستخدمين ونماذج الأعمال الخاصة بهم معقدة بتلبية الالتزامات التالية:

1. تأسيس وإكمال نظم وهياكل الامتثال لحماية المعلومات الشخصية طبقًا لقوانين الدولة، وإنشاء هيئة مستقلة مؤلفة بالأساس من أعضاء خارجيين للإشراف على ظروف حماية المعلومات الشخصية.
2. الالتزام بمبادئ الانفتاح والإنصاف والعدل؛ وصياغة قواعد للمنصات؛ وتوضيح معايير معالجة موفري المنتجات أو الخدمات داخل المنصات للمعلومات الشخصية وواجبات حماية المعلومات الشخصية المنوطة بهم.
3. وقف توفير الخدمات إلى موفري المنتجات والخدمات على المنصة التي تخالف صراحة القوانين أو الأنظمة الإدارية في معالجة المعلومات الشخصية.
4. إصدار تقارير دورية حول المسئولية الاجتماعية لحماية المعلومات الشخصية، وقبول إشراف المجتمع.

المادة 59: يلتزم الأشخاص الموكل إليهم قبول معالجة المعلومات الشخصية وطبقًا لأحكام هذا القانون والقوانين ذات الصلة والأنظمة الإدارية باتخاذ التدابير اللازمة لضمان أمن المعلومات الشخصية التي يعالجونها، ومساعدة معالجي المعلومات الشخصية على إنجاز التزاماتهم المنصوص عليها في هذا القانون.

8. **الفصل السادس: الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية**

المادة 60: تتحمل إدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة المسئولية عن التخطيط الشامل وتنسيق أعمال حماية المعلومات الشخصية وما يرتبط به من إشراف وجهود إدارية. الدوائر المختصة في مجلس الدولة هي المسئولة عن حماية المعلومات الشخصية وأعمال الإشراف والإدارة في حدود نطاق واجبات ومسئوليات كل منها، طبقًا لأحكام هذا القانون والقوانين أو الأنظمة الإدارية ذات الصلة.
تتقرر واجبات ومسئوليات حماية المعلومات الشخصية وإدارتها والإشراف عليها في الدوائر الحكومية الشعبية في مستوى المقاطعة والمستويات الأعلى طبقًا لأحكام وقوانين الدولة ذات الصلة.
يشار إلى الدوائر المنصوص عليها في الفقرتين السابقين جميعًا بلفظ الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية.
المادة 61: تتولى الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية إنجاز واجبات ومسئوليات حماية المعلومات الشخصية التالية:

1. تنفيذ الدعاية والتوعية بحماية المعلومات الشخصية وتوجيه ومراقبة تنفيذ معالجو المعلومات الشخصية لأعمال حماية المعلومات الشخصية.
2. قبول ومعالجة الشكاوى والبلاغات ذات الصلة بحماية المعلومات الشخصية.
3. تنظيم تقييم حالة حماية المعلومات الشخصية مثل الإجراءات المستخدمة ونشر نتائج التقييم.
4. التحري والتعامل مع أنشطة معالجة المعلومات الشخصية غير القانونية.
5. الواجبات والمسؤوليات الأخرى المنصوص عليها في القوانين أو الأنظمة الإدارية.

المادة 62: تنسق إدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة جميع أعمال حماية المعلومات الشخصية التالية التي تقوم بها الدوائر المعنية:

1. صياغة قواعد ومعايير قوية لحماية المعلومات الشخصية.
2. صياغة قواعد ومعايير مخصصة لحماية المعلومات الشخصية لصغار معالجي المعلومات الشخصية وتقنيات وتطبيقات جديدة لمعالجة المعلومات الشخصية الحساسة والتعرف على الوجوه والذكاء الاصطناعي، إلخ.
3. دعم التطوير والتنمية والاعتماد الواسع لتقنيات توثيق الهوية الإلكترونية الآمنة والملائمة، بالإضافة إلى تعزيز إنشاء خدمات توثيق الهوية عبر الإنترنت للجماهير.
4. تطوير إنشاء نظم الخدمات من أجل تعميم حماية المعلومات الشخصية، ودعم المؤسسات المعنية على إطلاق خدمات تقييم وتوثيق حماية المعلومات الشخصية.
5. تحسين آليات عمل شكاوى وبلاغات حماية المعلومات الشخصية.

المادة 63: عندما تنجز الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية واجبات ومسئوليات حماية المعلومات الشخصية، يجوز لها اعتماد التدابير التالية:

1. إجراء مقابلات مع الأطراف المعنية ذات اصلة، والتحري عن الظروف ذات الصلة بأنشطة معالجة المعلومات الشخصية.
2. مراجعة ونسخ عقود وتقارير وإيصالات الأطراف المعنية بالإضافة إلى المواد الأخرى ذات الصلة والمرتبطة بأنشطة معالجة المعلومات الشخصية.
3. إجراء عمليات فحص وتفتيش ميدانية وإجراء تحريات على أنشطة معالجة المعلومات الشخصية المشبوهة.
4. فحص المعدات والأدوات ذات الصلة بأنشطة معالجة المعلومات الشخصية؛ وعند وجود دليل على استخدام المعدات أو الأدوات للمشاركات في أنشطة غير قانونية لمعالجة المعلومات الشخصية، وبعد إبلاغ الشخص الرئيسي المسئول في دائرته خطيًا والحصول على الموافقة فيجوز له غلقها ومصادرتها.

في حالة قيام الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية بإنجاز واجباتها ومسئولياتها طبقًا للقانون، تلتزم الأطراف المعنية بتوفيري المساعدة والتعاون، ولا يجوز لهم تعطيلهم أو إعاقتهم.
المادة 64: في حال اكتشفت الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية وجود مخاطر كبيرة نسبيًا في أنشطة معالجة المعلومات الشخصية أو وقوع حوادث تتعلق بأمن المعلومات الشخصية، فيجوز لهم إجراء حوار مع الوكيل القانون لمعالج المعلومات الشخصية أو الشخص الرئيسي المسئول طبقًا للصلاحيات والإجراءات النظامية أو مطالبة معالجي المعلومات الشخصية بإسناد إجراء عملية تدقيق للامتثال إلى مؤسسات متخصصة فيما يتعلق بأنشطة معالجة المعلومات الشخصية. يعتمد معالجو المعلومات الشخصية تدابير طبقًا لمتطلبات تصحيح الأمور والتخلص من الأخطاء والثغرات.
إذا اكتشفت الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية خلال مسيرة واجباتها معالجة غير قانونية للمعلومات الشخصية ويشتبه في أنها تمثل جريمة، فيلتزمون على الفور بإحالة الأمر إلى سلطات الأمن العام من أجل المعالجة طبقًا لأحكام القانون.
المادة 65: لأي مؤسسة أو فرد الحق في تقديم شكوى أو بلاغ حول أنشطة معالجة المعلومات الشخصية غير القانونية إلى الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية. وتلتزم الدوائر التي تتلقى الشكاوى والبلاغات بمعالجتها على الفور وطبقًا لأحكام القانون، وإشعار صاحب الشكوى أو البلاغ بنتيجة المعالجة.
تلتزم الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية بنشر طرق الاتصال وقبول الشكاوى والتقارير.

الفصل السابع: المسئولية القانونية

المادة 66: في حالة معالجة المعلومات الشخصية بما يخالف أحكام هذا القانون أو معالجة المعلومات الشخصية دون القيام بواجبات حماية المعلومات الشخصية طبقًا للأحكام المنصوص عليها في هذا القانون، فعلى الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية إصدار أمر بالتصحيح ومصادرة الدخل غير المشروع، وإصدار أمر بتعليق شرطي للعمل أو إنهاء توفير الخدمة للتطبيقات البرمجية التي تتعامل بشكل غير قانوني مع المعلومات الشخصية؛ وفي حالة رفض التصحيح، يتم فرض غرامة إضافية لا تزيد عن مليون يوان واحد؛ كما يتم تغريم الشخص المسئول مسئولية مباشرة وفريق العمل المسئول مسئولية مباشرة بمبلغ يتراوح بين 10,000 ومبلغ 100,000 يوان.

في حال كانت ظروف التصرفات غير القانونية المذكورة في الفقرة السابقة خطيرة، فتلتزم الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية في مستوى الإقليم أو مستوى أعلى منه بتوجيه أمر بالتصحيح ومصادرة الدخل غير القانوني، وفرض غرامة لا تزيد عن 50 مليون يوان، أو نسبة 5% من الدخل السنوي. كما يجوز لهم إصدار أمر بتعليق أنشطة الأعمال المرتبطة بذلك أو وقف الأعمال من أجل التصحيح، وإبلاغ الإدارة المختصة بإلغاء التراخيص الإدارية المقابلة أو إلغاء تراخيص الأعمال. يتم تغريم الشخص المسئول مسئولية مباشرة وفريق العمل الآخر المسئول مسئولية مباشرة بمبلغ يتراوح بين 100,000 ومليون يوان واحد، ويمكن أن يتقرر أيضًا منعهم من شغل مناصب المديرين أو المشرفين أو مديرين من المستوى الرفيع، أو مسئولين عن حماية المعلومات الشخصية لفترة محددة.

المادة 67: في حالة وقوع التصرفات غير القانونية المنصوص عليها في هذا القانون، يتم تسجيلها في ملفات قيد حسبما تنص عليه القوانين أو الأنظمة الإدارية، ونشرها.

المادة 68: في حالة تقاعس هيئات الدولة عن إنجاز واجبات حماية المعلومات الشخصية وفقًا لما ينص عليه هذا القانون، تلتزم الهيئات الأعلى منها أو الدوائر المنوطة بواجبات ومسئوليات حماية المعلومات الشخصية بتوجيه أمر بالتصحيح؛ على أن تتم معاقبة الشخص المسئول مسئولية مباشرة وغير من الأشخاص المسئولين مسئولية مباشرة طبقًا للقانون.

وفي حالة ارتكاب فريق العمل بالدوائر المنوطة بواجبات حماية المعلومات الشخصية تقصيرًا في الواجبات، أو إساءة استخدام الصلاحيات، أو التورط في المحسوبية، لكنها لا تمثل رغم ذلك جريمة، فتتم معاقبتهم طبقًا لأحكام القانون.

المادة 69: في حال أدت مخالفات معالجة المعلومات الشخصية لحقوق ومصالح المعلومات الشخصية إلى ضرر، وتعذر إثبات خطأ ومخالفة معالجي المعلومات الشخصية، فإنهم يتحمل التعويض ويتولون المسئولية عن الانتهاك.

في الفقرة السابقة، تتقرر مسئولية التعويض عن الانتهاكات طبقًا لما ينتج عنها من خسارة للفرد أو المزايا الناجمة لمعالج المعلومات الشخصية. وإذا تعذر تقرير الخسارة التي لحقت بالفرد أو مزايا معالج المعلومات الشخصية، يتقرر التعويض وفقًا للظروف العملية.

المادة 70: في حالة قيام معالجو المعلومات الشخصية بمعالجة المعلومات الشخصية بالمخالفة لأحكام هذا القانون، وبما يخالف حقوق ومزايا العديد من الأفراد، فيجوز لمؤسسات العملاء المخصصين بشكل نظامي من جانب نواب العموم في جمهورية الصين الشعبية والمنظمات المعينة بمعرفة إدارة أمن الفضاء الإلكتروني والمعلوماتية التابعة للدولة رفع قضية أمام إحدى المحاكم الشعبية طبقًا للقانون.

المادة 71: إذا مثلت مخالفة لأحكام هذا القانون انتهاكاً لإدارة الأمن العام، يتم فرض عقوبة من إدارة الأمن العام طبقًا لأحكام القانون؛ ومتى ما اعتبرت جريمة، يتم التحري عن المسئولية الجنائية طبقًا لأحكام القانون.

الفصل الثامن: أحكام تكميلية

المادة 72: لا يسري هذا القانون على الشخصيات الطبيعية التي تعالج المعلومات الشخصية لأغراض شخصية أو شؤون تخص الأسرة.

إذا احتوى القانون على أحكام تخص معالجة المعلومات الشخصية بمعرفة الحكومات الشعبية في جميع المستويات ودوائرها المعنية والمؤسسات التي تنفذ أنشطة إدارة إحصائية وأرشيفية، يسري العمل بتلك الأحكام.

المادة 73: فيما يلي تعريف بالمصطلحات التالية المستخدمة في هذا القانون:

1. "معالج المعلومات الشخصية" ويقصد بهذا اللفظ المؤسسات والأفراد الذين يقررون بشكل مستقل أغراض وطرق المعالجة في أنشطة معالجة المعلومات الشخصية.
2. "اتخاذ القرارات التلقائي" ويشير إلى نشاط استخدام برامج الكمبيوتر في إجراء تحليل وتقييم تلقائي لأنماط السلوك الشخصي أو العادات أو الاهتمامات أو الهويات أو الحالة المالية أو الصحية أو الائتمانية أو أي حالة أخرى، واتخاذ قرارات [بناءً عليها].
3. "حجب تحديد الهوية" ويشير إلى عملية خضوع المعلومات الشخصية للمعالجة لضمان استحالة تحديد أشخاص طبيعيين محددين دون الحصول على دعم المعلومات الإضافية.
4. "تجهيل الهوية" ويشير إلى عملية خضوع المعلومات الشخصية للمعالجة ليكون من المستحيل تمييز الأشخاص الطبيعيين المحددين واستحالة الاستعادة.

المادة 74: يسري العمل بهذا القانون اعتبارًا من 1 نوفمبر/تشرين الثاني 2021.

الملحق 6
أنظمة حماية أمن البنية التحتية للمعلومات الحيوية.[35] (مقتطفات)

المادة 2. تشير البنية التحتية للمعلومات الحيوية كما هو مذكور في هذا النظام إلى البنية التحتية للشبكات الهامة ونظم المعلومات وغيرها، في الصناعات والقطاعات الهامة مثل خدمات الاتصالات السلكية واللاسلكية العامة وخدمات المعلومات والطاقة والمواصلات والمياه والتمويل والخدمات العامة والحكومة الإلكترونية وعلوم الدفاع القومي والتكنولوجيا والصناعة، إلخ، بالإضافة إلى أنه في حالة تلف تلك المعلومات أو فقد وظائفها التشغيلية أو تسرب البيانات فقد يؤدي ذلك إلى إضرار كبير بالأمن القومي أو الاقتصاد الوطني أو معيشة الشعب أو المصلحة العامة.

المادة 8: الإدارات المختصة ودوائر المراقبة والإدارة في الصناعات والقطاعات الهامة المذكورة في المادة 2 من هذا النظام هي الدوائر المسئولة عن أعمال حماية البنية التحتية للمعلومات الحيوية (والمشار إليها فيما يلي هنا اختصارًا بلفظ "دوائر أعمال الحماية").

المادة 9: يناط بدوائر عمل الحماية صياغة قواعد تحديد البنية التحتية للمعلومات الحيوية بالتكامل مع الوضع الفعلي في الصناعات والقطاعات التابعة لها، وإبلاغ إدارة الأمن العام بمجلس الدولة بها من أجل قيدها وتسجيلها.

عند صياغة قواعد تحديد الهوية، يجب مراعاة العوامل التالية بشكل أساسي:

1. درجة أهمية البنية التحتية للشبكات ونظام المعلومات إلخ، بالنبة للأنشطة الحيوية والجوهرية داخل الصناعة أو القطاع.
2. درجة الضرر الذي قد ينجم عن البنية التحتية للشبكات ونظام المعلومات إلخ، في حالة تلفها أو فقد وظائفها التشغيلية أو تعرض بياناتها للتسرب.
3. التأثير المرتبط على الصناعات والقطاعات الأخرى.

المادة 18: في حالة وقوع حوادث كبيرة تخص أمن الفضاء الإلكتروني أو اكتشاف تهديدات كبيرة تتعلق بأمن الفضاء الإلكتروني في البنية التحتية للمعلومات الحيوية، يلتزم المشغلون بإبلاغ الأمر لإدارة أعمال الحماية وسلطات الأمن العام طبقًا لأحكام القوانين ذات الصلة.

إذا حدث أن توقفت البنية التحتية للمعلومات الحيوية بالكامل عن العمل أو تم إعاقة وظائفها الرئيسية، أو في حالة تسرب معلومات قومية أساسية أو غيرها من المعلومات الهامة، أو تسرب معلومات شخصية على نطاق كبير نسبيًا، أو حدوث ضرر اقتصادي كبير نسبيًا، أو في حالة نشر معلومات غير قانونية على نطاق واسع نسبيًا، أو غير ذلك من الحوادث الخطيرة ذات الصلة خصيصًا بأمن الفضاء الإلكتروني، أو في حالة اكتشاف تهديدات مرتبطة على وجه الخصوص بأمن الفضاء الإلكتروني، فتلتزم دائرة أعمال الحماية وبعد تلقيها بلاغًا بإبلاغ الأمر إلى الإدارة الوطنية لأمن الفضاء الإلكتروني والمعلوماتية وإدارة الأمن العام في مجلس الدولة.

[35] أمر مجلس الدولة بجمهورية الصين الشعبية رقم 745، بتاريخ 30 يوليو/تموز 2021، http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1، حسب ترجمة DigiChina: https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept