Rapport national : initiatives politiques et lois relatives à Internet en Chine

Veni Markovski et Alexey Trepykhalin
31 janvier 2022
GE-010 (mise à jour)

ICANN

TABLE DES MATIERES

Introduction

Le présent rapport porte sur les initiatives politiques et les lois/réglementations mises en place par la Chine entre le 16 septembre 2015 et le 5 novembre 2021. Il vise à fournir à la communauté de l'ICANN les informations nécessaires afin de mieux comprendre les délibérations qui ont lieu au sein des Nations Unies, de l'UIT et autres agences des Nations Unies.

Il s'inscrit dans le cadre d'une série périodique de rapports nationaux qui donnent un aperçu des activités liées à l'écosystème de l'Internet et à la mission de l'ICANN. Le suivi de ces initiatives relève d'une responsabilité fondamentale de l'équipe de l'organisation ICANN en charge de la relation avec les gouvernements et les organisations intergouvernementales (GE), à savoir tenir l'ensemble de la communauté de l'ICANN informée des questions importantes relatives à l'Internet mondial, unique et interopérable et à ses systèmes d'identificateurs uniques[1].

Comme dans les précédents rapports de l'équipe GE, le présent rapport se fonde sur des textes de sources primaires liés aux politiques et technologies Internet telles que le système des noms de domaine (DNS), les adresses de protocole Internet (IP) et les paramètres de protocole, entre autres. De plus, ce rapport se base sur des textes, déclarations et dispositions légales/réglementaires d'intérêt concernant les positions de la Chine sur ces questions au sein des Nations Unies, de l'Union internationale des télécommunications (UIT) et à l'échelle nationale.

Déclarations et initiatives de la Chine en matière de politique étrangère

Le 16 décembre 2015, lors d'un discours de la cérémonie d'ouverture de la deuxième Conférence mondiale de l'Internet à Wuzhen[2], le président de la République populaire de Chine, Xi Jinping, déclare ce qui suit : « ..la communauté internationale doit renforcer le dialogue et la coopération sur la base d'un respect et d'une confiance mutuels, promouvoir la transformation du système de gouvernance mondiale de l'Internet, travailler ensemble au développement d'un cyberespace pacifique, sécurisé, ouvert et coopératif, et mettre en place un système de gouvernance mondiale de l'Internet multilatéral, démocratique et transparent. »[3].

À cette fin, le président Xi Jinping affirme que « le respect de la cybersouveraineté » de chacun des pays, accompagné de la participation à une « gouvernance mondiale du cyberespace sur

[1] « Plans opérationnels et financiers de l'ICANN », p. 47, organisation ICANN, décembre 2020, https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf.
[2] La Conférence mondiale de l'Internet, qui se tient chaque année à Wuzhen, dans la province du Zhejiang, est organisée par l'Administration du cyberespace de Chine et le gouvernement populaire de la province du Zhejiang http://www.wuzhenwic.org/2020-10/15/c_547699.htm. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : https://www.wicwuzhen.cn/.
[3] Remarques de H.E. Xi Jinping, président de la République populaire de Chine, lors de la cérémonie d'ouverture de la deuxième Conférence mondiale de l'Internet, Wuzhen, 16 décembre 2015 https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.

un pied d'égalité », est indispensable et constitue l'un des quatre principes directeurs[4]. Le président Xi Jinping ajoute également que « la gouvernance mondiale du cyberespace doit prendre la forme d'une approche multilatérale caractérisée par une participation multipartite. Elle doit se fonder sur une consultation entre toutes les parties de sorte à optimiser le rôle des différents acteurs, dont les gouvernements, les organisations internationales, les sociétés Internet, les communautés technologiques, les institutions non gouvernementales et les citoyens. Il ne doit pas y avoir d'unilatéralisme. Les décisions ne doivent pas être prises par une seule partie qui dicte les règles ou par quelques parties qui discutent entre elles. L'ensemble des pays doivent intensifier la communication et les échanges, renforcer le dialogue et les mécanismes de consultation dans le cyberespace, et examiner et formuler des règles de gouvernance pour l'Internet mondial, afin que le système de gouvernance mondiale de l'Internet devienne plus juste et raisonnable et reflète de manière plus équilibrée les aspirations et les intérêts de la majorité des pays. »[5].

Le 7 mars 2016, lors de la séance du Comité consultatif gouvernemental (GAC) de l'ICANN, les représentants chinois soulignent que « les quatre principes et les cinq propositions » avancés par le président Xi Jinping lors de la deuxième Conférence mondiale de l'Internet de 2016 à Wuzhen « nous fournissent (inaudible) de la pensée et des positions de la Chine eu égard à la gouvernance de l'Internet ».[6]

Le 27 avril 2016, la Chine rend publique sa stratégie nationale en matière de cybersécurité[7], expliquant qu'il est important pour le pays de « renforcer la coopération internationale dans le cyberespace ». À cette fin, la stratégie indique que cette coopération doit « promouvoir la réforme du système de gouvernance mondiale de l'Internet » et « l'internationalisation de la gestion des adresses Internet, des serveurs de noms de domaine et autres ressources de base ». La stratégie fait également part de sa volonté que « les Nations Unies jouent un rôle de premier plan, favorisent l'élaboration de normes internationales pour le cyberespace qui soient reconnues, au niveau international, par l'ensemble des parties concernées et d'un traité international relatif à la lutte contre le terrorisme dans le cyberespace, mettent en place des mécanismes d'aide judiciaire pour combattre la cybercriminalité, renforcent la coopération internationale dans des domaines tels que les politiques et les lois, l'innovation technologique, les règles et normes, les interventions d'urgence, la protection des infrastructures critiques en matière d'information, etc. ». Elle appelle aussi à « mettre en place un système de gouvernance mondiale de l'Internet multilatéral, démocratique et transparent ».

Le 2 mars 2017, la Chine publie la stratégie internationale de coopération dans le cyberespace[8]. Elle prévoit que « la Chine œuvrera à la réforme institutionnelle du Forum des

[4] Remarques de H.E. Xi Jinping.
[5] Remarques de H.E. Xi Jinping.
[6] MARRAKECH – Réunion gouvernementale de haut niveau du GAC, lundi 7 mars 2016, ICANN55 | Marrakech, Maroc, page 86 https://gac.icann.org/transcripts/public/transcript-icann55-gac-hl-governmental-meeting-2016-03-07.pdf.
[7] China Copyright and Media, stratégie nationale en matière de sécurité du cyberespace, mise à jour le 27 décembre 2016, https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.cac.gov.cn/2016-12/27/c_1120195926.htm.
[8] Stratégie internationale de coopération dans le cyberespace, China Daily, 2 mars 201, https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm. Ce document a été traduit dans

Nations Unies sur la gouvernance de l'Internet afin de permettre aux Nations Unies de jouer un rôle plus important dans la gouvernance de l'Internet, de renforcer leurs capacités décisionnelles, de garantir un financement stable et de mettre en place des procédures ouvertes et transparentes pour l'élection des membres et la présentation de rapports ». La stratégie internationale de coopération dans le cyberespace indique également que la Chine « participera à des discussions internationales sur la répartition et la gestion équitables des ressources critiques d'Internet », et qu'elle « promouvra ardemment la réforme de l'ICANN de sorte à en faire une institution internationale réellement indépendante, à renforcer sa représentation et à garantir une plus grande ouverture et transparence de son processus décisionnelle et de ses opérations »[9].

Le 20 avril 2018, lors de la Conférence nationale sur les travaux liés à la cybersécurité et à l'informatisation tenue à Beijing, le président Xi Jinping déclare que « dorénavant, la réforme du système de gouvernance mondiale de l'Internet s'inscrit dans un mouvement général et constitue une aspiration commune ». Il ajoute que « la gouvernance mondiale du cyberespace doit continuer à faire la part belle à une participation multilatérale et de toutes les parties prenantes, permettant à tous types d'acteurs de jouer leur rôle, dont les gouvernements, les organisations internationales, les sociétés Internet, la communauté technique, les organisations de la société civile et les citoyens. Nous devons à la fois promouvoir la gouvernance du cyberespace dans le cadre des Nations Unies et s'efforcer de permettre à tous types d'acteurs non étatiques de jouer le rôle constructif qui leur revient. »[10].

Le 9 juillet 2019, dans ses conclusions rendues au Groupe de travail à composition limitée sur les évolutions dans le domaine des informations et télécommunications dans le contexte de la sécurité internationale (OEWG), la Chine fait les remarques suivantes : « Les États doivent collaborer afin de créer un système de gouvernance mondiale de l'Internet multilatéral, démocratique et transparent. L'organisation chargée d'assurer la gestion des ressources critiques telles que les serveurs racine doit être réellement indépendante de tout contrôle étatique de sorte à garantir une large participation et une prise de décision commune entre tous les États. »[11].

En avril 2020, la Chine rend l'avant-projet de rapport suivant à l'OEWG des Nations Unies, dans lequel elle déclare ce qui suit : « Compte tenu du peu de temps dont nous disposons, il convient d'éviter introduire dans le rapport des concepts qui n'ont pas encore fait l'objet d'un consensus mondial (par exemple le « bien public ») ». Elle ajoute également que : « Lors des deux précédentes séances, les parties, Chine comprise, ont présenté des dizaines de propositions constructives sur des questions telles que la cybersouveraineté, la sécurité des chaînes

---

plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.china.org.cn/chinese/2017-03/07/content_40424606.htm.

[9] Stratégie internationale de coopération dans le cyberespace, China Daily, 2 mars 2017.

[10] New America, traduction : discours de Xi Jinping du 20 avril lors de la Conférence nationale sur les travaux liés à la cybersécurité et à l'informatisation, 30 avril 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/ . Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.xinhuanet.com/politics/2018-04/21/c_1122719810.htm.

[11] Conclusions rendues par la Chine au Groupe de travail à composition limitée sur les évolutions dans le domaine des informations et télécommunications dans le contexte de la sécurité internationale, 7 juillet 2019. https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf.

d'approvisionnement, la protection des infrastructures critiques, le fait de s'abstenir de prononcer des sanctions unilatérales et la lutte contre le cyberterrorisme. Il faut espérer que ces propositions soient intégrées au rapport. »[12].

Le 8 septembre 2020, le ministère chinois des Affaires étrangères publie un document intitulé « Initiative mondiale sur la sécurité des données », via lequel il répond aux besoins des États de mieux coopérer dans les domaines de la sécurité des données, de la cybercriminalité, etc. Le document suggère que les « gouvernements, organisations internationales, sociétés TIC[13], communautés technologiques, organisations de la société civile, individus et tous autres acteurs mènent des efforts concertés visant à promouvoir la sécurité des données en vertu des principes de vaste consultation, de contribution commune et de partage des bénéfices ». Le document invite les États, entre autres, à « assurer la gestion de la sécurité des données de manière exhaustive, objective et en se fondant sur des données probantes, et à maintenir une chaîne d'approvisionnement ouverte, sécurisée et stable des produits et services TIC au niveau mondial »[14].

En mars 2021, la conférence législative annuelle « Deux sessions » adopte le 14e plan quinquennal et la vision 2035, dans lesquels la section 4 (Promouvoir la construction d'une communauté avec un futur partagé dans le cyberespace) du chapitre 18 (Créer un écosystème numérique de qualité) prévoit ce qui suit : « Renforcer les échanges internationaux et la coopération dans le cyberespace, et promouvoir l'élaboration de règles numériques et liées au cyberespace à l'échelle internationale au sein des Nations Unies en tant que principal canal et dans le cadre de la Charte des Nations Unies en tant que principes de base. Promouvoir l'établissement d'un système de gouvernance mondiale de l'Internet multilatéral, démocratique et transparent, et la mise en place d'un mécanisme de gouvernance des infrastructures et ressources de réseau plus équitable et raisonnable. »[15].

Le 10 mars 2021, lors des délibérations de l'OEWG au sein des Nations Unies, la Chine déclare ce qui suit : « Les États doivent participer à la gestion et à la répartition des ressources Internet internationales sur un pied d'égalité. »[16].

---

[12] Contribution de la Chine à l'avant-projet de rapport de l'OEWG, 16 avril 2020 (date selon les propriétés du PDF), https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf .

[13] TIC – Technologies de l'information et des communications, UNTERM – Base de données terminologique des Nations Unies, https://unterm.un.org/unterm/display/record/imo/na?OriginalId=551772be82184a22adaeb86841e335e6.

[14] Initiative mondiale sur la sécurité des données, site web du ministère chinois des Affaires étrangères, 8 septembre 2020, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjfywj_665252/202009/t20200908_599773.html et « La Chine lance une Initiative mondiale sur la sécurité des données pour s'opposer à la politisation des enjeux liés à la sécurité des données », Reuters, 7 septembre 2020, https://www.reuters.com/article/wangyi-global-digital-security-0908-idCNKBS25Z0AJ. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : https://www.fmprc.gov.cn/chn/pds/ziliao/tytj/t1827469.htm.

[15] Guancha, « 14e plan quinquennal » et exposé des objectifs à long terme pour 2035 (texte intégral), 13 mars 2021, https://www.guancha.cn/politics/2021_03_13_583945_5.shtml.

[16] Groupe de travail à composition limitée sur les évolutions dans le domaine des informations et télécommunications dans le contexte de la sécurité internationale, troisième séance de fond, 8-12 mars 2021, résumé du président de l'OEWG, document de séance, 10 mars 2021, A/AC.290/2021/CRP.3*,

Le 29 juin 2021, la Chine et la fédération de Russie publient une déclaration commune annonçant leur décision de prolonger le « Traité de bon voisinage et de coopération amicale ». Dans cette déclaration commune, ils prévoient de « réaffirmer leur engagement à renforcer la sécurité des informations internationales au niveau bilatéral et multilatéral » et mettent en avant « leur unité sur les questions liées à la gouvernance de l'Internet, notamment en garantissant que tous les États bénéficient des mêmes droits à participer à la gouvernance du réseau mondial, en renforçant leur rôle dans ce processus et en préservant le droit souverain des États de réguler leur segment national de l'Internet. La Russie et la Chine soulignent la nécessité de rehausser le rôle de l'Union internationale des télécommunications et la représentation des deux pays dans ses instances dirigeantes. »[17].

Le 1er novembre 2021, la fédération de Russie présente son avant-projet de texte[18] pour une proposition de convention sur la cybercriminalité des Nations Unies et annonce que le texte est coparrainé par la Chine.[19,20]

Le 5 novembre 2021, la Chine présente ses propositions lors de la première séance du Comité ad hoc (AHC) des Nations Unies[21]. Entre autres, elle déclare ce qui suit : « Les États sont tenus de pénaliser l'intrusion et la destruction des installations TIC, des systèmes, des données ou des infrastructures critiques en matière d'information. Cela peut comprendre l'accès illégal à des systèmes d'information informatiques, l'interférence illégale avec des systèmes d'information informatiques, l'acquisition illégale de données informatiques, l'interférence illégale avec des données informatiques, l'utilisation abusive d'infrastructures critiques en matière d'information, etc. »

Déclarations, législation et réglementations à l'échelle nationale

https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

[17] Ambassade de la fédération de Russie auprès du Royaume-Uni de Grande-Bretagne et d'Irlande, déclaration commune de la fédération de Russie et de la République populaire de Chine à l'occasion du vingtième anniversaire du Traité de bon voisinage et de coopération amicale entre la fédération de Russie et la République populaire de Chine, 28 juin 2021, https://www.rusemb.org.uk/fnapr/7007. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.xinhuanet.com/2021-06/28/c_1127606620.htm.

[18] Convention des Nations Unies sur la lutte contre l'utilisation des technologies de l'information et des communications à des fins criminelles, 27 juillet 2021, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf .

[19] Prochaine entrée en vigueur de la nouvelle Convention des Nations Unies sur la lutte contre la cybercriminalité, fm4.orf.at, https://fm4.orf.at/stories/3019118/ .

[20] Konstantinos Komaitis, compte Twitter, 1er novembre 2021 et 19 janvier 2022, https://twitter.com/i/web/status/1455217317504327683.

[21] Suggestions de la Chine concernant la portée, les objectifs et la structure (les éléments) de la Convention des Nations Unies sur la lutte contre l'utilisation des TIC à des fins criminelles : https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf.

Le 1er juillet 2015, la loi sur la sécurité nationale est adoptée. Voilà ce qu'elle prévoit (dans son article 59) : « L'État met en place des systèmes et mécanismes d'examen, de supervision et de gestion de la sécurité nationale, qui prennent la forme d'évaluation de la sécurité nationale d'investissements commerciaux étrangers, d'articles et technologies spécifiques, de produits et services liés aux technologies de l'information sur Internet, de projets touchant à des questions de sécurité nationale, ainsi que d'autres affaires et activités d'importance qui ont un impact ou pourraient avoir un impact sur la sécurité nationale. »[22]. Article 25 : « L'État met en place un système national de protection de la sécurité des réseaux et des informations, [...] qui renforce la gestion du réseau, garantit la souveraineté du cyberespace, la sécurité et les intérêts liés au développement. »

Le 1er juin 2017, la loi sur la cybersécurité (la CSL) entre en vigueur. Elle prévoit que l'État est chargé « de promouvoir un cyberespace pacifique, sécurisé, ouvert et coopératif et de mettre en place un système de gouvernance de l'Internet multilatéral, démocratique et transparent. » Cette loi contient également une disposition visant à stocker les données Internet sur le territoire national de la « Chine continentale ». L'article 31 de la loi précise que le cadre des infrastructures critiques en matière d'information doit comprendre « un système de protection de la cybersécurité à plusieurs niveaux pour les services de communication et d'information publiques, l'énergie, le trafic, les ressources hydriques, la finance, les services publics, l'e-gouvernement et autres infrastructures critiques en matière d'information. » L'article 37 de la loi prévoit ce qui suit : « lorsqu'en raison d'impératifs commerciaux il est vraiment nécessaire de les fournir [des données personnelles, des données importantes] en dehors des frontières de la Chine continentale, ils [les opérateurs des infrastructures critiques en matière d'information] doivent respecter les mesures élaborées conjointement par le département de la cybersécurité et de l'informatisation de l'État et les départements concernés du Conseil des affaires de l'État afin de procéder à une évaluation de la sécurité ; en cas de dispositions contraires des lois et règlements administratifs, il convient de respecter ces dispositions. »[23]. (Les dispositions en question sont fournies à l'Annexe 1 du présent rapport.)

Le 24 août 2017, le ministère chinois de l'Industrie et des Technologies de l'information (le MIIT) publie la mise à jour des mesures relatives à la gestion des noms de domaine Internet. [24] (Les dispositions en question sont fournies à l'Annexe 2 du présent rapport.)

[22]China Law Translate, loi sur la sécurité nationale de la République populaire de Chine, 1er juillet 2015, https://www.chinalawtranslate.com/en/2015nsl/. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm.

[23] New America, traduction : loi sur la cybersécurité de la République populaire de Chine (entrée en vigueur le 1er juin 2017), 29 juin 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

[24] Ministère chinois de l'Industrie et des Technologies de l'information, mesures relatives à la gestion des noms de domaine Internet, 24 août 2017 https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.cac.gov.cn/2017-09/28/c_1121737753.htm.

Le 29 janvier 2018, le MIIT annonce, sur le fondement de l'article 5 de ses nouvelles mesures susmentionnées, le système des noms de domaine Internet chinois ajusté.[25] (Les dispositions en question sont fournies à l'Annexe 3 du présent rapport.)

Le 13 juin 2019, les mesures relatives à l'évaluation de la sécurité des transferts transfrontaliers de données personnelles proposaient, dans leurs articles 2, ce qui suit : « Les opérateurs de réseau qui fournissent des données personnelles collectées dans le cadre d'opérations menées sur le territoire continental de la République populaire de Chine (ci-après les « transferts sortants de données personnelles ») doivent mener des évaluations de la sécurité conformément aux présentes mesures. Si l'évaluation de la sécurité révèle que le transfert sortant de données personnelles pourrait avoir un impact sur la sécurité nationale ou porter atteinte à l'intérêt public, ou que la protection de la sécurité des données personnelles n'est pas facile à garantir, ces données ne doivent pas sortir du pays. Si l'État prévoit d'autres dispositions concernant les transferts sortants de données personnelles, ces dispositions s'appliqueront. »[26].

Le 10 juin 2021, la loi sur la sécurité des données (DSL) est adoptée à l'occasion de la 29e réunion du Comité permanent de la 13e Assemblée nationale populaire.[27] (Voir les textes de la loi y afférents à l'Annexe 4 du présent rapport.)

Le 30 juillet 2021, les nouveaux règlements relatifs à la protection de la sécurité des infrastructures critiques en matière d'information sont publiés (après avoir été adoptés par le Conseil des affaires de l'État chinois le 27 avril 2021). Ces règlements précisent le cadre des infrastructures critiques en matière d'information, prennent des dispositions spécifiques pour certains « secteurs et industries » détaillant ledit cadre, et posent à leurs égards des exigences de déclaration auprès des autorités centrales en charge de la cybersécurité en cas « d'incidents de cybersécurité particulièrement graves » tels que la fuite « à relativement grande échelle » de

[25] Au 19 août 2021, l'URL vers la source chinoise ne fonctionnait pas. Voici la version anglaise : https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://xn--eqrt2g.xn--vuq861b/#.

[26] New America, traduction : avant-projet de nouvelles règles concernant les transferts sortants de données personnelles en dehors de Chine, 13 juin 2019, « Mesures relatives à l'évaluation de la sécurité des transferts sortants de données personnelles (avant-projet à des fins de commentaire) », 13 juin 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.cac.gov.cn/2019-06/13/c_1124613618.htm.

[27] Inside Privacy, traduction non officielle de Covington : mesures relatives à l'évaluation de la sécurité des transferts transfrontaliers de données personnelles (avant-projet à des fins de commentaire), 13 juin 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, et New America, traduction : avant-projet de nouvelles règles concernant les transferts sortants de données personnelles en dehors de Chine, « Mesures relatives à l'évaluation de la sécurité des transferts sortants de données personnelles (avant-projet à des fins de commentaire) », juin 2019 https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-new-draft-rules-cross-border-transfer-personal-information-out-china/. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.cac.gov.cn/2019-06/13/c_1124613618.htm.

données personnelles.[28] Ces règlements entrent en vigueur le 1er septembre 2021. (Les articles des règlements nous intéressant sont disponibles à l'Annexe 6 du présent rapport.)

Le 20 août 2021, le Comité permanent de l'Assemblée nationale populaire de la République populaire de Chine adopte la loi sur la protection des données personnelles (PIPL). Elle entre en vigueur le 1er novembre 2021. La loi « est formulée [...] de sorte à protéger les droits et intérêts relatifs aux données personnelles, à normaliser les activités de traitement de données personnelles, et à promouvoir l'utilisation rationnelle des données personnelles ». Les données personnelles « de personnes physiques bénéficient d'une protection juridique : aucune organisation ou aucun individu ne peut enfreindre les droits et intérêts relatifs aux données personnelles de personnes physiques. » La présente loi « s'applique aux activités de traitement des données personnelles d'organisations et d'individus de personnes physiques situées dans les frontières de la République populaire de Chine ». « En cas de survenue d'une des circonstances suivantes dans le cadre des activités de traitement, menées hors des frontières de la République populaire de Chine, de données personnelles de personnes physiques situées dans les frontières de la République populaire de Chine, la présente loi s'applique également » : (1) « Si l'objectif consiste à fournir des produits ou services à des personnes physiques à l'intérieur des frontières » ; (2) « En cas d'analyse ou d'évaluation d'activités menées par des personnes physiques à l'intérieur des frontières » ; (3) « En cas d'autres circonstances prévues par les lois ou règlements administratifs ». La loi définit également les données personnelles et précise les éléments inclus dans leur traitement : « Les données personnelles constituent toutes sortes de données enregistrées par voie électronique ou autre liées à des personnes physiques identifiées ou identifiables ; les données anonymisées ne sont pas comprises dans cette définition. Le traitement des données personnelles comprend la collecte, le stockage, l'utilisation, la gestion, la transmission, la fourniture, la publication, la suppression, etc. de données personnelles.[29] (Le texte intégral de la loi est disponible à l'Annexe 5 du présent rapport.)

Conclusion

La Chine participe activement à l'ensemble des discussions liées à Internet au sein des Nations Unies. Les contributions internationales et nationales de la Chine pourraient potentiellement concerner la mission de l'ICANN. L'organisation ICANN, via son équipe en charge de la relation avec les gouvernements, continuera à fournir des informations à la communauté de l'ICANN en cas de déclarations ou propositions portant sur la gouvernance technique de l'Internet ou la mission de l'ICANN.

[28] Décision n° 745 du Conseil des affaires de l'État de la République populaire de Chine, 30 juillet 2021, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1, traduite par DigiChina : https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept.

[29] Loi sur la protection des données personnelles de la République populaire de Chine, (adoptée à l'occasion de la 30e réunion du Comité permanent de la 13e Assemblée nationale populaire du 20 août 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

Annexe 1
Loi sur la cybersécurité de la République populaire de Chine[30]

Adoptée le 6 novembre 2016. Entrée en vigueur le 1er juin 2017.

1. Table des matières

Chapitre I : Dispositions générales

Article 1 : La présente loi est élaborée afin : de garantir la cybersécurité ; de sauvegarder la souveraineté du cyberespace, la sécurité nationale ainsi que les intérêts sociaux et publics ; de protéger les droits et intérêts légitimes des citoyens, des personnes morales et autres organisations ; et de promouvoir le développement harmonieux de l'informatisation de l'économie et de la société.

Article 2 : La présente loi s'applique à la construction, au fonctionnement, à la maintenance et à l'utilisation de réseaux, ainsi qu'à la supervision et la gestion de la cybersécurité sur le territoire continental de la République populaire de Chine.

Article 3 : L'État continue à promouvoir, sur le même plan, la cybersécurité et le développement de l'informatisation, se conforme aux principes d'utilisation active, de développement scientifique, de gestion dans le respect de la loi, et de garantie de la sécurité. L'État fait progresser la construction d'infrastructures de réseau et la connectivité, encourage l'innovation et l'application de technologies de réseau, soutient la formation d'experts en cybersécurité, met en place un système complet de sauvegarde de la cybersécurité, et renforce les capacités liées à la protection de la cybersécurité.

Article 4 : L'État élabore et améliore en permanence la stratégie en matière de cybersécurité, clarifie les exigences fondamentales et les objectifs prioritaires liés à la protection de la cybersécurité, et propose des politiques, des missions de travail et des procédures relatives à la cybersécurité pour les principaux secteurs concernés.

Article 5 : L'État prend des mesures visant à suivre, prévenir et traiter les risques et menaces à la cybersécurité à la fois dans les frontières et hors des frontières du territoire continental de la République populaire de Chine. L'État protège les infrastructures critiques en matière d'information contre les attaques, les intrusions, les interférences et les destructions ; l'État

[30] NewAmerica, traduction : loi sur la cybersécurité de la République populaire de Chine (entrée en vigueur le 1er juin 2017), 29 juin 2018, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/. Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

sanctionne les cyberactivités illégitimes et criminelles conformément à la loi, en préservant la sécurité et l'ordre du cyberespace.
Article 6 : L'État préconise d'adopter une conduite en ligne sincère, honnête, saine et civilisée ; il promeut la diffusion des valeurs socialistes fondamentales, adopte des mesures visant à renforcer la sensibilisation de l'ensemble de la société et le niveau de cybersécurité, et crée un environnement propice à la participation par l'ensemble de la société à la promotion de la cybersécurité.

Article 7 : L'État mène activement des échanges et des activités de coopération, à l'échelle internationale, dans les domaines de la gouvernance du cyberespace, de la recherche et du développement de technologies de réseau, de l'élaboration de normes, de la lutte contre la cybercriminalité et l'illégalité, et autres domaines ; il assure la promotion de la construction d'un cyberespace pacifique, sécurisé, ouvert et coopératif et de la mise en place d'un système de gouvernance de l'Internet multilatéral, démocratique et transparent.
Article 8 : Le département de la cybersécurité et de l'informatisation de l'État est chargé de planifier et de coordonner l'ensemble des activités en matière de cybersécurité et activités connexes de supervision et gestion. Les départements des télécommunications, de la sécurité publique et autres entités concernées du Conseil des affaires de l'État sont chargés des activités de protection, de supervision et de gestion de la cybersécurité dans le cadre de leurs responsabilités, conformément aux dispositions de la présente loi et des lois et règlements administratifs applicables.
Les missions de protection, supervision et gestion de la cybersécurité des départements concernés des gouvernements populaires au niveau national ou supranational seront déterminées par des règlements nationaux.
Article 9 : Les opérateurs de réseau qui mènent des activités commerciales et de service doivent se conformer aux lois et règlements administratifs, respecter la moralité sociale, faire preuve d'une éthique commerciale, être honnêtes et crédibles, s'acquitter d'obligations visant à protéger la cybersécurité, accepter la supervision du gouvernement et du public, et assumer leur responsabilité sociale.
Article 10 : La construction et le fonctionnement de réseaux, ou la fourniture de services via des réseaux, doivent être assurés conformément aux dispositions des lois et règlements administratifs, et conformément aux exigences obligatoires posées par les normes nationales. Dans le cadre de cette construction et de ce fonctionnement de réseaux, il convient d'adopter des mesures techniques et autres mesures requises afin de garantir la cybersécurité et la stabilité opérationnelle, d'apporter des réponses efficaces en cas d'incidents de cybersécurité, de prévenir tout cybercrime et toute activité illégitime, et de préserver l'intégrité, la confidentialité et l'exploitabilité des données en ligne.
Article 11 : Les organisations de l'industrie d'Internet, selon leurs statuts,
doivent renforcer l'autodiscipline du secteur, élaborer des normes de comportement en matière de cybersécurité, orienter leurs membres pour le renforcement de la protection de la cybersécurité dans le respect de la loi, augmenter le niveau de protection de la cybersécurité, et favoriser le développement harmonieux du secteur.
Article 12 : L'État protège les droits des citoyens, des personnes morales et autres organisations à utiliser les réseaux conformément à la loi ; il assure la promotion d'un accès généralisé aux réseaux, augmente le niveau des services de réseau, fournit des services de réseau sécurisés et adaptés, et garantit la circulation légale, ordonnée et libre des informations de réseau.
Toute personne ou organisation qui utilise des réseaux doit se conformer à la Constitution et aux lois, ne pas perturber l'ordre public et respecter la moralité sociale ; elle ne doit pas compromettre la cybersécurité et ne doit pas utiliser Internet afin de se livrer à des activités

compromettant la sécurité nationale, l'honneur nationale et les intérêts nationaux ; elle ne doit pas inciter à la subversion de la souveraineté nationale, bouleverser le système socialiste, pousser au séparatisme, rompre l'unité nationale, faire l'apologie du terrorisme ou de l'extrémisme, inciter à la haine et la discrimination ethniques, diffuser des informations violentes, obscènes ou sexuelles, produire ou diffuser de fausses informations afin de perturber l'ordre économique ou social, ou des informations portant atteinte à la réputation, à la vie privée, à la propriété intellectuelle ou autres droits et intérêts d'autrui, et commettre des actes similaires.

Article 13 : L'État encourage la recherche et le développement de produits et services de réseau favorisant la qualité de l'éducation proposée aux mineurs ; l'État, en toute légitimité, sanctionnera l'utilisation de réseaux visant à mener des activités compromettant le bien-être psychologique et physique des mineurs ; et l'État fournira aux mineurs un environnement de réseau sain et sécurisé.

Article 14 : L'ensemble des individus et organisations ont le droit de signaler tout agissement compromettant la cybersécurité aux départements en charge de la cybersécurité, de l'informatisation, des télécommunications, de la sécurité publique et autres. Les départements recevant ces signalements doivent les traiter dans de brefs délais conformément à la loi ; en cas d'affaires ne relevant pas des responsabilités du département qui a reçu le signalement, ce département doit transférer dans de brefs délais le signalement au département compétent. Les départements compétents préserveront la confidentialité des informations des auteurs des signalements et protégeront leurs droits et intérêts.

Chapitre II : Soutien à et promotion de la cybersécurité

Article 15 : L'État met en place et améliore un système de normes relatives à la cybersécurité. Les départements administratifs en charge de la normalisation du Conseil des affaires de l'État et autres départements compétents du Conseil des affaires de l'État, selon leurs responsabilités respectives, organiseront l'élaboration et la révision en temps opportun des normes nationales et de l'industrie en matière de gestion de la cybersécurité et de sécurité des produits, services et opérations de réseau.

L'État encourage les entreprises, les instituts de recherche, les établissements d'enseignement supérieur et les organisations du secteur intervenant dans les réseaux à participer à l'élaboration de normes nationales et de l'industrie en matière de cybersécurité.

Article 16 : Le Conseil des affaires de l'État et les gouvernements populaires des provinces, régions autonomes et municipalités sous contrôle direct devront : procéder à une planification exhaustive ; développer les investissements ; apporter un soutien aux principaux programmes et secteurs des technologies en matière de cybersécurité ; apporter un soutien à la recherche et au développement, à l'application et à la vulgarisation des technologies en matière de cybersécurité ; promouvoir des produits et services de réseau sécurisés et fiables ; protéger les droits de propriété intellectuelle des technologies de réseau ; et encourager les instituts de recherche et développement, établissements d'enseignement supérieur, etc., à participer à des programmes d'innovation technologique en matière de cybersécurité mis en place par l'État.

Article 17 : L'État renforce la mise en place de systèmes de services socialisés pour la cybersécurité, en encourageant les entreprises et instituts concernés à procéder à des certifications, des tests et des évaluations des risques en matière de cybersécurité, et à fournir d'autres services de sécurité connexes.

Article 18 : L'État encourage le développement de technologies d'utilisation et de protection de la sécurité de données de réseau, en facilitant l'ouverture de ressources de données publiques et en promouvant l'innovation technique et le développement économique et social.

L'État apporte son soutien aux méthodes innovantes de gestion de la cybersécurité en utilisant de nouvelles technologies de réseau pour renforcer le niveau de protection de la cybersécurité.

Article 19 : Tous les échelons des gouvernements populaires et leurs départements respectifs doivent régulièrement organiser et mener des campagnes publicitaires et d'éducation en matière de cybersécurité, et orienter et encourager les unités concernées à mener des activités adéquates de publicité et d'éducation en matière de cybersécurité.
Les médias de masse doivent mener des campagnes publicitaires et d'éducation ciblées en matière de cybersécurité destinées au grand public.
Article 20 : L'État encourage les entreprises et les établissements d'enseignement ou de formation, tels que les établissements d'enseignement supérieur et les écoles professionnelles, à éduquer et former à la cybersécurité, et a recours à différentes méthodes pour former un personnel qualifié à la cybersécurité et promouvoir l'interaction des professionnels de la cybersécurité.

Chapitre III : Sécurité des opérations de réseau

Section 1. Dispositions générales

Article 21 : L'État met en place un système de protection de la cybersécurité à plusieurs niveaux (MLPS). Les opérateurs de réseau exécuteront les missions suivantes liées à la protection de la sécurité conformément aux exigences du système de protection de la cybersécurité à plusieurs niveaux afin de veiller à ce que les réseaux ne fassent pas l'objet d'interférences, de dommages ou d'accès non autorisés, et afin de prévenir toute fuite, tout vol ou toute falsification de données de réseau :

(1) Concevoir des systèmes de gestion internes de la sécurité et élaborer des règles de fonctionnement, déterminer quelles sont les personnes responsables de la cybersécurité, et instaurer des responsabilités quant à la protection de la cybersécurité ;

(2) Adopter des mesures techniques visant à prévenir les virus informatiques, les cyberattaques, les intrusions de réseau et autres actions compromettant la cybersécurité ;

(3) Adopter des mesures techniques visant à suivre et enregistrer les statuts opérationnels des réseaux et les incidents de cybersécurité, et respecter les dispositions relatives au stockage de journaux de réseau pendant au moins six mois ;

(4) Adopter des mesures telles que la classification de données, la sauvegarde de données importantes et le chiffrement ;

(5) D'autres obligations prévues par les lois ou règlements administratifs.

Article 22 : Les produits et services de réseau doivent respecter les exigences nationales et impératives applicables. Les fournisseurs de produits et services de réseau ne doivent pas installer de programmes malveillants ; s'ils constatent que leurs produits et services présentent des défauts de sécurité ou des vulnérabilités, ils doivent immédiatement adopter des mesures correctives et respecter les dispositions imposant d'en informer les utilisateurs et de rapporter de tels faits aux départements concernés dans de brefs délais.
Les fournisseurs de produits et services de réseau doivent assurer le maintien de la sécurité de leurs produits et services, sans interruption, pendant toute la durée convenue avec les clients.
Si une des fonctionnalités du produit ou service de réseau permet de collecter des données d'utilisateur, son fournisseur indiquera clairement cette fonctionnalité et devra obtenir le consentement de l'utilisateur ; et si cette collecte implique d'obtenir des données personnelles d'utilisateur, le fournisseur devra également respecter les dispositions de la présente loi ainsi que les lois et règlements administratifs relatifs à la protection des données personnelles.
Article 23 : Les équipements de réseau critiques et les produits de cybersécurité spécialisés doivent respecter les normes nationales et les exigences impératives, et leur sécurité doit être certifiée par un établissement agréé ou ils doivent faire l'objet d'un contrôle de sécurité avant d'être vendus ou fournis. Le département de la cybersécurité et de l'informatisation de l'État ainsi que les départements concernés du Conseil des affaires de l'État concevront et publieront

un catalogue répertoriant les équipements de réseau critiques et les produits de cybersécurité spécialisés, et promouvront la reconnaissance mutuelle des certifications de sécurité et des résultats des contrôles de sécurité afin d'éviter les doublons de certifications et de contrôles.
Article 24 : Les opérateurs de réseau qui gèrent l'accès aux réseaux et les services d'enregistrement des noms de domaine pour les utilisateurs, qui gèrent l'accès à des réseaux de téléphonie fixe ou mobile, ou qui fournissent aux utilisateurs des services de publication d'informations ou de messagerie instantanée, imposeront aux utilisateurs de fournir des informations exactes concernant leur identité lors de la conclusion de contrats avec les utilisateurs ou de la confirmation de la fourniture de services. Dans l'hypothèse où des utilisateurs ne fourniraient pas d'informations exactes concernant leur identité, les opérateurs de réseau ne devront pas leur fournir les services requis.
L'État met en place une stratégie relative à la crédibilité de l'identité des réseaux et soutient la recherche et le développement de technologies d'authentification d'identité numérique sécurisées et pratiques, en promouvant l'acceptation réciproque entre les différentes méthodes d'authentification d'identité numérique.
Article 25 : Les opérateurs de réseau formuleront des plans d'intervention d'urgence pour les incidents de cybersécurité et apporteront dans de brefs délais une réponse aux vulnérabilités du système, aux virus informatiques, aux cyberattaques, aux intrusions de réseau et autres risques menaçant la cybersécurité. En cas d'incidents de cybersécurité, les opérateurs de réseau doivent immédiatement lancer un plan d'intervention d'urgence, adopter les mesures correctives s'imposant et signaler les incidents aux départements compétents conformément aux dispositions applicables.
Article 26 : Les personnes procédant à des certifications, des tests, des évaluations des risques ou autres activités connexes en matière de cybersécurité, ou qui sont chargées de publier des informations liées à la cybersécurité telles que des vulnérabilités du système, des virus informatiques, des attaques de réseau ou des intrusions de réseau, doivent se conformer aux dispositions nationales applicables.
Article 27 : Les individus et organisations ne doivent pas procéder à des intrusions illégales dans les réseaux d'autres parties, perturber le fonctionnement normal des réseaux d'autres parties, ou voler des données de réseau ou se livrer à d'autres activités compromettant la cybersécurité ; ils ne doivent pas fournir des programmes ou des outils utilisés spécifiquement dans les intrusions de réseau qui perturbent les fonctions normales des réseaux et les mesures de protection, voler des données de réseau ou se livrer à d'autres agissements compromettant la cybersécurité ; et lorsqu'ils constatent que des tiers mènent manifestement des activités compromettant la cybersécurité, ils ne doivent pas leur apporter une aide pouvant prendre la forme d'un soutien technique, de supports publicitaires et promotionnels ou d'une prise en charge de dépenses.
Article 28 : Les opérateurs de réseau fourniront un soutien technique et une assistance aux organismes en charge de la sécurité publique et de la sécurité nationale qui assurent la sauvegarde de la sécurité nationale et mènent des enquêtes sur des activités criminelles conformément à la loi.
Article 29 : L'État soutient la coopération entre les opérateurs de réseau dans des domaines tels que la collecte, l'analyse, la communication et le traitement en urgence d'informations liées à la cybersécurité, en renforçant les capacités de protection de la sécurité des opérateurs de réseau.
Les organisations industrielles compétentes doivent définir et mettre en place des mécanismes pour la normalisation et la coordination de la cybersécurité dans leur secteur, renforcer leur analyse et évaluation de la cybersécurité, et lancer des alertes de sécurité et assurer le soutien et la coordination des membres en cas de risques à la cybersécurité.

Article 30 : Les données obtenues par le département de la cybersécurité et de l'informatisation et autres départements chargés de la protection de la cybersécurité peuvent être utilisées uniquement lorsque cela est nécessaire pour la protection de la cybersécurité et ne doivent pas être utilisées à d'autres fins.

Section 2. Sécurité des opérations des infrastructures critiques en matière d'information

Article 31 : L'État met en place une solide protection fondée sur le système de protection de la cybersécurité à plusieurs niveaux pour les services de communication et d'information publiques, l'énergie, le trafic, les ressources hydriques, la finance, les services publics, l'e-gouvernement et autres infrastructures critiques en matière d'information qui, en cas de destruction, de perte de fonctionnalités ou de fuite de données, pourraient gravement compromettre la sécurité nationale, le bien-être national, les moyens de subsistance des personnes ou l'intérêt public. Le Conseil des affaires de l'État définira le champ d'application spécifique et les mesures de protection de la sécurité pour les infrastructures critiques en matière d'information.

L'État encourage les opérateurs de réseau ne relevant pas des systèmes d'infrastructures critiques en matière d'information [désignés] à participer volontairement au système de protection des infrastructures critiques en matière d'information.

Article 32 : Conformément aux missions et à la répartition des tâches prévues par le Conseil des affaires de l'État, les départements responsables des travaux de protection de la sécurité pour les infrastructures critiques en matière d'information doivent séparément compiler et organiser les plans de mise en œuvre de la sécurité pour leur secteur ou les infrastructures critiques en matière d'information de leur secteur, et orienter et superviser les activités de protection de la sécurité pour les opérations des infrastructures critiques en matière d'information.

Article 33 : Les infrastructures critiques en matière d'information en construction doivent veiller à disposer des capacités requises pour apporter un soutien à la stabilité commerciale et aux opérations au long cours, et garantir simultanément la planification, la mise en place et l'application des mesures techniques de sécurité.

Article 34 : Outre les dispositions de l'article 21 de la présente loi, les opérateurs d'infrastructures critiques en matière d'information doivent également exécuter les missions suivantes liées à la protection de la sécurité :

(1) Créer des organismes de gestion de la sécurité spécialisées, déterminer les personnes responsables de la gestion de la sécurité et effectuer des vérifications d'antécédents en matière de sécurité de ces responsables et du personnel occupant des postes clés ;

(2) Mener périodiquement des activités éducatives en matière de cybersécurité, des formations techniques et des évaluations des compétences des employés ;

(3) Procéder à des sauvegardes d'importants systèmes et bases de données suite à un sinistre ;

(4) Élaborer des plans d'intervention d'urgence en cas d'indicents de cybersécurité, et organiser périodiquement des exercices ;

(5) D'autres missions prévues par les lois ou règlements administratifs.

Article 35 : Les opérateurs d'infrastructures critiques en matière d'information qui achètent des produits et services de réseau susceptibles d'avoir un impact sur la sécurité nationale doivent être soumis à un examen de la sécurité nationale organisé par le département de la cybersécurité et de l'informatisation de l'État et les départements concernés du Conseil des affaires de l'État.

Article 36 : Les opérateurs d'infrastructures critiques en matière d'information qui achètent des produits et services de réseau doivent respecter les dispositions applicables et signer un accord

de sécurité et confidentialité avec le fournisseur précisant les missions et responsabilités en matière de sécurité et confidentialité.
Article 37 : Les opérateurs d'infrastructures critiques en matière d'information qui collectent ou produisent des données personnelles ou des données importantes dans le cadre d'opérations menées sur le territoire continental de la République populaire de Chine doivent stocker ces données en Chine continentale. Lorsqu'en raison d'impératifs commerciaux il est vraiment nécessaire de les fournir en dehors des frontières de la Chine continentale, ils doivent respecter les mesures élaborées conjointement par le département de la cybersécurité et de l'informatisation de l'État et les départements concernés du Conseil des affaires de l'État afin de procéder à une évaluation de la sécurité ; en cas de dispositions contraires des lois et règlements administratifs, il convient de respecter ces dispositions.
Article 38 : Au moins une fois par an, les opérateurs d'infrastructures critiques en matière d'information doivent procéder à un contrôle et une évaluation de la sécurité de leurs réseaux et des potentiels risques, soit d'eux-mêmes soit en faisant appel à un organisme fournissant des services de cybersécurité ; les opérateurs d'infrastructures critiques en matière d'information doivent soumettre un rapport de cybersécurité sur les circonstances du contrôle et de l'évaluation ainsi que sur les mesures d'amélioration, rapport à envoyer au département responsable des activités de protection de la sécurité des infrastructures critiques en matière d'information.
Article 39 : Le département de la cybersécurité et de l'informatisation de l'État doit coordonner les départements concernés eu égard à l'adoption des mesures suivantes de protection de la sécurité des infrastructures critiques en matière d'information :

(1) Effectuer des tests ponctuels sur les risques menaçant la sécurité des infrastructures critiques en matière d'information, mettre en place des mesures d'amélioration et, si nécessaire, faire appel à un organisme fournissant des services de cybersécurité afin qu'il effectue des tests et une évaluation des risques de cybersécurité ;

(2) Faire en sorte que les opérateurs d'infrastructures critiques en matière d'information organisent périodiquement des exercices d'intervention d'urgence en cas d'atteinte à la cybersécurité, de façon à renforcer le niveau, la coordination et les capacités d'intervention en cas d'incidents de cybersécurité.

(3) Promouvoir le partage d'informations relatives à la cybersécurité entre les départements compétents, les opérateurs d'infrastructures critiques en matière d'information ainsi que les instituts de recherche et organismes fournissant des services de cybersécurité concernés.

(4) Apporter un soutien technique et une assistance pour la gestion des interventions d'urgence en matière de cybersécurité et la reprise d'activités, etc.

Chapitre IV : Sécurité des informations de réseau

Article 40 : Les opérateurs de réseau doivent préserver scrupuleusement la confidentialité des données d'utilisateur qu'ils collectent, et définir et mettre en place des systèmes de protection des données.
Article 41 : Les opérateurs de réseau qui collectent et utilisent des données personnelles doivent respecter les principes de légalité, propriété et nécessité ; ils doivent publier des règles relatives à la collecte et à l'utilisation énonçant explicitement les objectifs, les moyens et la portée de la collecte ou de l'utilisation des données, et obtenir le consentement des individus dont les données sont collectées.
Les opérateurs de réseau ne doivent pas collecter de données personnelles sans rapport avec les services qu'ils fournissent ; ne doivent pas enfreindre les dispositions des lois, règlements administratifs ou accords conclus entre les parties à des fins de collecte ou d'utilisation de données personnelles ; et doivent respecter les dispositions des lois, règlements administratifs

et accords conclus avec les utilisateurs à des fins de traitement des données personnelles qu'ils ont stockées.
Article 42 : Les opérateurs de réseau ne doivent pas divulguer, falsifier ou détruire les données personnelles qu'ils collectent ; et, en l'absence de consentement de la personne dont les données ont été collectées, ne doivent pas fournir les données personnelles à des tiers. Toutefois, une exception prévoit que les données peuvent être fournies si, après traitement, il n'existe aucune façon d'identifier un individu donné et que son identité ne peut être retrouvée.
Les opérateurs de réseau doivent adopter des mesures techniques et autres mesures requises afin de garantir la sécurité des données personnelles qu'ils collectent et de prévenir leur fuite, leur destruction ou leur perte. En cas de fuite, destruction ou perte réelle ou présumée de données personnelles, des mesures correctives doivent être prises immédiatement, et il convient de respecter les dispositions imposant d'en informer les utilisateurs et de rapporter de tels faits aux départements concernés dans de brefs délais, conformément aux règlements.
Article 43 : Si des individus constatent que des opérateurs de réseau ont enfreint des dispositions des lois, règlements administratifs ou accords conclus entre les parties à des fins de collecte ou d'utilisation de leurs données personnelles, ils sont en droit de demander aux opérateurs de réseau de supprimer leurs données personnelles ; s'ils constatent que les données personnelles collectées ou stockées par les opérateurs de réseau contiennent des erreurs, ils sont en droit de demander aux opérateurs de réseau d'apporter les corrections requises. Les opérateurs de réseau doivent adopter des mesures pour la suppression et la correction.
Article 44 : Les individus ou organisations ne doivent pas voler de données personnelles ou utiliser d'autres méthodes illégales afin d'obtenir de telles données, et ne doivent pas vendre ou fournir illégalement à des tiers des données personnelles.
Article 45 : Les départements devant exécuter, en vertu de la loi, des missions de supervision et gestion de la cybersécurité, ainsi que leur personnel, doivent préserver scrupuleusement la confidentialité des données personnelles, des données privées et des secrets commerciaux dont ils prennent connaissance dans le cadre de leurs missions, et ne doivent pas provoquer une fuite de ces données, les vendre ou les fournir illégalement à des tiers.
Article 46 : L'ensemble des individus et organisations seront responsables de l'utilisation de leurs sites web et ne doivent pas créer des sites web ou des groupes de communication à des fins de fraude, de communication de méthodes criminelles, de création ou vente de produits interdits ou contrôlés, ou autres activités criminelles, et les sites web ne doivent pas être exploités afin de publier des données liées à une fraude, à la création ou vente de produits interdits ou contrôlés, ou autres activités illégales.
Article 47 : Les opérateurs de réseau doivent renforcer la gestion des données publiées par les utilisateurs et, s'ils prennent connaissance de données dont la loi ou les règlements administratifs interdisent la publication ou la transmission, doivent cesser immédiatement la transmission de ces données, adopter des mesures de traitement telles que la suppression des données, empêcher la diffusion des données, conserver les dossiers correspondants, et effectuer un signalement auprès des départements compétents.
Article 48 : Les données électroniques envoyées, ou logiciels d'application fournis par un individu ou une organisation, ne doivent pas installer des programmes malveillants, et ne doivent pas contenir de données dont la loi ou les règlements administratifs interdisent la publication ou la transmission.
Les fournisseurs de services de diffusion de données électroniques et les fournisseurs de services de téléchargement de logiciels d'application doivent exécuter des missions de gestion de la sécurité ; s'ils prennent connaissance que leurs utilisateurs se sont livrés aux activités indiquées dans le paragraphe précédent, ils doivent : prendre des mesures telles que la cessation de la fourniture de services et la suppression de données ou programmes

malveillants ; conserver les dossiers correspondants ; et effectuer un signalement auprès des départements compétents.
Article 49 : Les opérateurs de réseau doivent mettre en place des systèmes de plainte et de signalement en cas d'atteinte à la sécurité des données de réseau, divulguer au public des données telles que les méthodes de dépôt de plaintes ou signalements, et accepter et traiter dans de brefs délais les plaintes et signalements liés à une atteinte à la sécurité des données de réseau.
Les opérateurs de réseau doivent coopérer avec les départements de la cybersécurité et de l'informatisation et les départements concernés pour la mise en œuvre de la supervision et des contrôles conformément à la loi.
Article 50 : Le département de la cybersécurité et de l'informatisation de l'État et les départements concernés mèneront des activités de supervision et de gestion de la sécurité des données de réseau conformément à la loi ; et s'ils constatent la publication ou la transmission de données interdites par les lois ou règlements administratifs, ils doivent demander aux opérateurs de réseau de cesser la transmission, prendre des mesures telles que la suppression, et conserver les dossiers correspondants ; pour les données décrites ci-dessus qui proviennent d'au-delà des frontières de la Chine continentale, ils doivent demander à l'organisation concernée d'adopter des mesures techniques et autres mesures requises afin de bloquer la transmission.

Chapitre V : Suivi, alerte précoce et intervention d'urgence

Article 51 : L'État mettra en place un système de suivi, d'alerte précoce et de communication d'informations en matière de cybersécurité. Le département de la cybersécurité et de l'informatisation de l'État doit assurer la coordination globale des départements concernés de sorte à renforcer les activités de collecte, d'analyse et de signalement de données liées à la cybersécurité, et respecter les règlements portant sur la publication unifiée d'informations relatives au suivi et aux alertes précoces en matière de cybersécurité.
Article 52 : Les départements responsables des activités de protection de la sécurité des infrastructures critiques en matière d'information doivent définir et mettre en place des systèmes de suivi, d'alerte précoce et de communication d'informations en matière de cybersécurité pour leur industrie ou secteur, et communiquer les informations relatives au suivi et aux alertes précoces en matière de cybersécurité conformément aux règlements.
Article 53 : Le département de la cybersécurité et de l'informatisation de l'État assurera la coordination avec les départements concernés afin de définir et mettre en place des mécanismes pour les activités d'évaluation des risques et d'intervention d'urgence en matière de cybersécurité, élaborera des plans d'intervention d'urgence en cas d'incidents de cybersécurité, et organisera régulièrement des exercices.
Les départements responsables des activités de protection de la sécurité des infrastructures critiques en matière d'information doivent élaborer des plans d'intervention d'urgence en cas d'incidents de cybersécurité pour leur industrie ou secteur respectif, et organiser régulièrement des exercices.
Les plans d'intervention d'urgence en cas d'incidents de cybersécurité doivent classer les incidents de cybersécurité en tenant compte de facteurs tels que l'ampleur des dommages après l'incident et la portée de l'impact, et prévoir des mesures correspondantes de gestion des interventions d'urgence.
Article 54 : Lorsque le risque d'incidents de cybersécurité augmente, les départements concernés des gouvernements populaires à l'échelle provinciale et supraprovinciale doivent respecter les compétences et les procédures prévues, et adopter les mesures suivantes en prenant en compte les caractéristiques du risque menaçant la cybersécurité et les dommages qu'il est susceptible de causer :

(1) Imposer aux départements, institutions et personnel concernés de collecter et communiquer dans de brefs délais les informations pertinentes, et renforcer le suivi des risques menaçant la cybersécurité ;

(2) Faire en sorte que les départements, institutions et personnel spécialisé mènent des analyses et évaluations des informations relatives au risque menaçant la cybersécurité, et se prononcent sur la probabilité d'apparition d'incidents, l'ampleur de l'impact et le niveau des dommages ;

(3) Émettre des alertes destinés au public en cas de risque de cybersécurité, et adopter des mesures permettant d'éviter et de réduire les dommages.

Article 55 : En cas d'incident de cybersécurité, le plan d'intervention d'urgence doit être immédiatement lancé, une évaluation de l'incident de cybersécurité doit être menée, les opérateurs de réseau doivent adopter des mesures techniques et autres mesures requises, les potentiels risques liés à la sécurité doivent être supprimés, la menace doit être empêchée de se développer, et des alertes destinés au public doivent être rapidement émis.

Article 56 : Lorsque, dans l'exécution de leurs missions de supervision et gestion de la cybersécurité, les départements concernés des gouvernements populaires à l'échelle provinciale et supraprovinciale constatent que les réseaux sont exposés à un risque lié à la sécurité relativement important ou qu'un incident de sécurité s'est produit, ils peuvent demander au représentant légal ou au responsable de l'opérateur du réseau en question de mener des entretiens dans le respect des compétences et procédures prévues. Les opérateurs de réseau doivent respecter les exigences imposant de respecter les procédures, d'apporter des corrections et de supprimer les dangers cachés.

Article 57 : Les urgences soudaines ou accidents liés à la sécurité de la production découlant d'incidents de cybersécurité doivent être gérés conformément aux dispositions de la « Loi relative à l'intervention d'urgence de la République populaire de Chine », la « Loi sur la sécurité de la production de la République populaire de Chine » et autres lois et règlements administratifs applicables.

Article 58 : Afin de répondre à la nécessité de protéger la sécurité nationale et l'ordre public social, et afin de respecter les exigences liées aux incidents de sécurité majeurs au sein de la société, il est possible, tel que prévu et approuvé par le Conseil des affaires de l'État, de prendre des mesures temporaires relatives aux communications en réseau dans une région spécialement désignée, par exemple la limitation desdites communications.

Chapitre VI : Responsabilité juridique

Article 59 : Si les opérateurs de réseau ne s'acquittent pas de leurs missions de protection de la cybersécurité prévues aux articles 21 et 25 de la présente loi, les départements compétents ordonneront d'apporter des corrections et donneront des avertissements ; si les corrections sont refusées ou si elles entraînent une atteinte à la cybersécurité ou autres conséquences similaires, une amende comprise entre 10 000 RMB et 100 000 RMB sera imposée ; et le personnel directement responsable de la gestion se verra infliger une amende comprise entre 5000 RMB et 50 000 RMB.

Si les opérateurs d'infrastructures critiques en matière d'information ne s'acquittent pas de leurs missions de protection de la cybersécurité prévues aux articles 33, 34, 36 et 38 de la présente loi, les départements compétents ordonneront d'apporter des corrections et donneront des avertissements ; si les corrections sont refusées ou si elles entraînent une atteinte à la cybersécurité ou autres conséquences similaires, une amende comprise entre 100 000 RMB et 1 000 000 RMB sera imposée ; et le personnel directement responsable de la gestion se verra infliger une amende comprise entre 10 000 RMB et 100 000 RMB.

Article 60 : En cas de violation des paragraphes 1 ou 2 de l'article 22 ou du paragraphe 1 de l'article 48 de la présente loi liée à l'un des agissements suivants, les départements compétents

concernés doivent ordonner d'apporter des corrections et donner des avertissements ; si les corrections sont refusées ou si elles entraînent une atteinte à la cybersécurité ou autres conséquences, une amende comprise entre 50 000 RMB et 500 000 RMB sera imposée ; et les responsables directs se verront infliger une amende comprise entre 10 000 RMB et 100 000 RMB.

(1) Installation de programmes malveillants ;

(2) Incapacité à prendre des mesures correctives immédiates si les produits ou services présentent des défauts de sécurité ou des vulnérabilités, ou le fait de ne pas informer les utilisateurs et de ne pas procéder aux signalements requis aux départements compétents conformément aux règlements ;

(3) Interruption non autorisée du maintien de la sécurité de leurs produits ou services.

Article 61 : Les opérateurs de réseau qui n'exigent pas aux utilisateurs de fournir des informations exactes concernant leur identité ou qui fournissent des services aux utilisateurs ne fournissant pas d'informations exactes concernant leur identité, et violent donc le paragraphe 1 de l'article 24 de la présente loi, sont sommés par le département compétent d'apporter des corrections ; si les corrections sont refusées ou si la gravité des circonstances l'exige, une amende comprise entre 50 000 RMB et 500 000 RMB sera imposée, et le département compétent pourra ordonner une suspension temporaire des opérations, une suspension des activités afin d'apporter des corrections, une fermeture des sites web, une annulation des permis d'exploitation requis ou une annulation des licences commerciales ; les responsables directs et autre personnel directement responsable se verront infliger une amende comprise entre 10 000 RMB et 100 000 RMB.

Article 62 : En cas de violation de l'article 26 de la présente loi liée à la réalisation de certifications, tests ou évaluations des risques ou à la publication de données liées à la cybersécurité telles que les vulnérabilités du système, les virus informatiques, les cyberattaques ou les intrusions de réseau, des corrections doivent être imposées et un avertissement doit être donné ; si les corrections sont refusées ou si la gravité des circonstances l'exige, une amende comprise entre 10 000 RMB et 100 000 RMB sera imposée, et le département compétent pourra ordonner une suspension temporaire des opérations, une suspension des activités afin d'apporter des corrections, une fermeture des sites web, une annulation des permis d'exploitation requis ou une annulation des licences commerciales ; les responsables directs et autre personnel directement responsable se verront infliger une amende comprise entre 5 000 RMB et 50 000 RMB.

Article 63 : En cas de violation de l'article 27 de la présente loi liée à la réalisation d'activités portant atteinte à la cybersécurité, à la fourniture de logiciels ou d'outils spécialisés permettant de réaliser des activités portant atteinte à la cybersécurité ou à la fourniture à des tiers réalisant des activités portant atteinte à la cybersécurité d'une assistance pouvant prendre la forme d'un soutien technique, de supports publicitaires et promotionnels ou d'une prise en charge de dépenses, et lorsque cela ne constitue pas un crime, les organisations en charge de la sécurité publique confisqueront les gains illicites et imposeront jusqu'à 5 jours de détention et pourront imposer une amende comprise entre 50 000 RMB et 500 000 RMB ; et si la gravité des circonstances l'exige, elles imposeront entre 5 et 15 jours de détention et pourront imposer une amende comprise entre 100 000 RMB et 1 000 000 RMB.

Si des unités se livrent à l'une des activités indiquées dans le précédent paragraphe, les organisations en charge de la sécurité publique confisqueront les gains illicites et imposeront une amende comprise entre 100 000 RMB et 1 000 000 RMB, et les responsables directs et autre personnel directement responsable se verront infliger une amende conformément au précédent paragraphe.

En cas de violation de l'article 27 de la présente loi, les personnes soumises à des sanctions administratives émanant d'organisations en charge de la sécurité publique ne doivent pas

mener d'activités de gestion de la cybersécurité ou occuper des postes clés liés à des opérations de réseau pendant 5 ans ; les personnes soumises à des sanctions pénales ne pourront mener d'activités de gestion de la cybersécurité et occuper des postes clés liés à des opérations de réseau pendant toute leur vie.

Article 64 : Les opérateurs de réseau ainsi que les fournisseurs de produits ou services de réseau coupables d'une violation du paragraphe 3 de l'article 22 ou des articles 41-43 de la présente loi pour avoir porté atteinte à des données personnelles protégées par la loi seront contraints, par le département compétent, d'apporter des corrections et pourront, séparément ou conjointement, recevoir des avertissements, se voir confisquer les gains illicites qu'ils ont obtenus et/ou se voir infliger une amende comprise entre 1 et 10 fois le montant des gains illicites ; s'il n'y a pas de gains illicites, l'amende pourra atteindre 1 000 000 RMB et une amende comprise entre 10 000 RMB et 100 000 RMB sera infligée aux responsables directs et autre personnel directement responsable ; si la gravité des circonstances l'exige, le département compétent pourra ordonner une suspension temporaire des opérations, une suspension des activités afin d'apporter des corrections, une fermeture des sites web, une annulation des permis d'exploitation requis ou une annulation des licences commerciales.

En cas de violation de l'article 44 de la présente loi liée au vol ou au recours à d'autres moyens illégaux afin d'obtenir, de vendre illégalement ou de fournir illégalement à des tiers des données personnelles, et lorsque cela ne constitue pas un crime, les organisations en charge de la sécurité publique confisqueront les gains illicites et imposeront une amende comprise entre 1 et 10 fois le montant des gains illicites, et s'il n'y a pas de gains illicites, elles imposeront une amende pouvant atteindre 1 000 000 RMB.

Article 65 : En cas de violation, par les opérateurs d'infrastructures critiques en matière d'information, de l'article 35 de la présente loi liée au recours à des produits ou services de réseau n'ayant pas fait l'objet de contrôles de sécurité ou dont les contrôles de sécurité n'ont pas été concluants, le département compétent imposera la cessation du recours auxdits produits ou services et imposera une amende équivalant à entre 1 et 10 fois le prix d'achat ; les responsables directs et autre personnel directement responsable se verront infliger une amende comprise entre 10 000 RMB et 100 000 RMB.

Article 66 : En cas de violation, par les opérateurs d'infrastructures critiques en matière d'information, de l'article 37 de la présente loi liée au stockage de données de réseau hors des frontières du territoire continental ou à la fourniture de données de réseau à des tiers basés en dehors des frontières du territoire continental, le département compétent : imposera des mesures correctives, donnera un avertissement, confisquera les gains illicites et imposera des amendes comprises entre 50 000 RMB et 500 000 RMB; et pourra ordonner une suspension temporaire des opérations, une suspension des activités afin d'apporter des corrections, une fermeture des sites web, une annulation des permis d'exploitation requis ou une annulation des licences commerciales. Les responsables directs et autre personnel directement responsable se verront infliger une amende comprise entre 10 000 RMB et 100 000 RMB.

Article 67 : En cas de violation de l'article 46 de la présente loi liée à la création d'un site web ou d'un groupe de communication utilisé afin de réaliser des activités illégales ou criminelles ou liée à l'utilisation du réseau à des fins de publication de données relatives à la réalisation d'activités illégales ou criminelles, mais sans qu'un crime n'ait été commis, les organisations en charge de la sécurité publique imposeront jusqu'à 5 jours de détention et pourront imposer une amende comprise entre 10 000 RMB et 15 000 RMB ; et si la gravité des circonstances l'exige, elles pourront imposer entre 5 et 15 jours de détention et pourront imposer une amende comprise entre 50 000 RMB et 500 000 RMB. Elles pourront également imposer la fermeture des sites web et groupes de communication utilisés afin de réaliser des activités illégales ou criminelles.

Si des unités se livrent à l'une des activités indiquées dans le précédent paragraphe, une amende comprise entre 100 000 RMB et 500 000 RMB sera imposée par les organisations en charge de la sécurité publique, et les principaux responsables et organisations en charge de la sécurité publique se verront infligés une amende conformément au paragraphe précédent.

Article 68 : En cas de violation, par les opérateurs de réseau, de l'article 47 de la présente loi liée à l'incapacité de cesser la transmission de données, données dont la transmission et la publication sont interdites par les lois ou règlements administratifs, à l'incapacité de prendre des mesures telles que la suppression ou à l'incapacité de conserver les dossiers correspondants, le département compétent imposera d'apporter des corrections, donnera un avertissement et confisquera les gains illicites ; si les corrections sont refusées ou si la gravité des circonstances l'exige, des amendes comprises entre 100 000 RMB et 500 000 RMB seront imposées, et une suspension temporaire des opérations, une suspension des activités afin d'apporter des corrections, une fermeture des sites web, une annulation des permis d'exploitation requis ou une annulation des licences commerciales pourront être ordonnées ; et les responsables directs et autre personnel directement responsable se verront infliger une amende comprise entre 10 000 RMB et 100 000 RMB.

Si les fournisseurs de services de diffusion de données électroniques et les fournisseurs de services de téléchargement de logiciels d'application n'exécutent pas leurs missions de gestion de la sécurité prévues au paragraphe 2 de l'article 48 de la présente loi, des sanctions leur seront imposées conformément aux dispositions du précédent paragraphe.

Article 69 : Les opérateurs de réseau qui ont enfreint les dispositions de la présente loi en se rendant coupables d'un des agissements suivants seront contraints d'apporter des corrections par les départements compétents ; si les corrections sont refusées ou si la gravité des circonstances l'exige, une amende comprise entre 50 000 RMB et 500 000 RMB sera imposée, et les responsables directs et autre personnel directement responsable se verront infliger une amende comprise entre 10 000 RMB et 100 000 RMB :

(1) Non-respect des obligations, imposées par les départements compétents, d'adopter des mesures telles que la cessation de la diffusion ou la suppression de données dont la publication ou la diffusion est interdite par les lois ou règlements administratives ;

(2) Refus des ou entrave aux activités légales de supervision et de contrôle des départements compétents ;

(3) Refus de fournir un soutien technique et une assistance aux organisations en charge de la sécurité publique et de la sécurité de l'État.

Article 70 : La publication ou transmission de données interdite par le paragraphe 2 de l'article 12 de la présente loi ou d'autres lois ou règlements administratifs sera sanctionnée conformément aux dispositions des lois et règlements administratifs applicables.

Article 71 : Tout agissement contraire aux dispositions de la présente loi sera enregistré dans des registres de crédit et rendu public conformément aux lois et règlements administratifs applicables.

Article 72 : Si les opérateurs de réseau des affaires gouvernementales de l'organisation d'État n'exécutent pas les missions de protection de la cybersécurité prévues par la présente loi, l'organisation relevant de l'échelon supérieur ou les organisations compétentes leur imposeront d'apporter des corrections ; les responsables directs et autre personnel directement responsable se verront infliger des sanctions.

Article 73 : En cas de violation, par le département de la cybersécurité et de l'informatisation et autres départements concernés, des dispositions de l'article 30 de la présente loi liée à l'utilisation de données personnelles acquises dans le cadre de leurs missions de protection de la cybersécurité à des fins autres que les fins prévues, les responsables directs et autre personnel directement responsable se verront infliger des sanctions.

Si le personnel du département de la cybersécurité et de l'informatisation et autres départements concernés manque à ses missions, abuse de son pouvoir, fait preuve de favoritisme, sans que cela ne constitue un crime, des sanctions seront imposées conformément à la loi.

Article 74 : Si les violations des dispositions de la présente loi portent atteinte à des tiers, la responsabilité civile sera engagée conformément à la loi.

En cas de violation des dispositions de la présente loi, constituant une violation de la gestion de l'ordre public, des sanctions administratives seront imposées conformément à la loi ; en cas de crime, la responsabilité pénale sera engagée conformément à la loi.

Article 75 : Si des instituts, organisations ou individus étrangers sont coupables d'attaques, d'intrusions, d'interférences, de dommages ou autres activités qui compromettent les infrastructures critiques en matière d'information de la République populaire de Chine et ont de graves conséquences, la responsabilité légale sera engagée conformément à la loi ; les départements en charge de la sécurité publique relevant du Conseil des affaires de l'État et autres départements compétents pourront également décider de geler les actifs des institutions, organisations ou individus ou prendre d'autres mesures punitives nécessaires.

Chapitre VII : Dispositions supplémentaires

Article 76 : Dans la présente loi, les termes indiqués ci-dessous ont les significations suivantes :

(1) « Réseau » [网络, également « cyber »] désigne un système comprenant des ordinateurs ou autres terminaux d'information et équipements connexes qui respectent certaines règles et procédures à des fins de collecte, stockage, transmission, échange et traitement de données.

(2) « Cybersécurité » [网络安全, également « sécurité des réseaux »] désigne l'ensemble des mesures requises afin de prévenir les cyberattaques, les intrusions, les interférences, les destructions, les utilisations illicites et les accidents fortuits, de garantir le fonctionnement stable et fiable des réseaux, et de veiller à ce que les données de réseau soient exhaustives, confidentielles et exploitables.

(3) « Opérateurs de réseau » [网络运营者] désigne les propriétaires et responsables de réseaux ainsi que les fournisseurs de services de réseau.

(4) « Données de réseau » [网络数据] désigne tous les types de données électroniques collectées, stockées, transmises, traitées et produites par les réseaux.

(5) « Données personnelles » [个人信息] désigne tous les types de données, enregistrées par voie électronique ou via d'autres moyens, qui, seules ou avec d'autres données, sont suffisantes pour identifier une personne physique, notamment les noms, prénoms, dates de naissance, numéros d'identification nationaux, données biométriques personnelles, adresses, numéros de téléphone, etc. de personnes physiques.

Article 77 : La protection de la sécurité opérationnelle des réseaux qui stockent ou traitent des données portant sur des secrets nationaux doit respecter la présente loi ainsi que les dispositions des lois et règlements administratifs relatifs à la protection des secrets.

Article 78 : Les règles concernant la protection de la sécurité des réseaux militaires sont élaborées par la Commission militaire centrale.

Article 79 : La présente loi entrera en vigueur le 1er juin 2017.

Annexe 2

Mesures relatives à la gestion des noms de domaine Internet du ministère chinois de l'Industrie et des Technologies de l'information[31] (extraits)

En vertu de l'**article 3** des mesures, le ministère de l'Industrie et des Technologies de l'information est tenu d'assurer « la supervision et la gestion des services liés aux noms de domaine au niveau national, ses principales tâches consistant à : (1) élaborer des règles et politiques pour la gestion des noms de domaine Internet ; (2) concevoir un système de noms de domaine Internet et un plan pour le développement de ressources de noms de domaine ; (3) superviser les organismes assurant le fonctionnement des serveurs racine de noms de domaine nationaux et les organismes chargés de l'enregistrement et de la gestion des noms de domaine ; (4) prendre en charge la gestion de la sécurité des réseaux et des informations du système des noms de domaine ; (5) protéger les données personnelles, droits et intérêts des utilisateurs conformément à la loi ; (6) prendre en charge la coordination internationale des noms de domaine ; (7) assurer la gestion des services de résolution des noms de domaine nationaux ; (8) assurer la gestion d'autres activités en rapport avec les services liés aux noms de domaine. »

L'**article 10** des mesures prévoit que « les entités faisant une demande d'établissement d'un serveur racine de nom de domaine ou d'un organisme assurant le fonctionnement des serveurs racine de noms de domaine doivent satisfaire aux conditions suivantes : (1) le serveur racine de nom de domaine doit être créé sur le territoire, être conforme aux plans de développement d'Internet en vigueur et respecter l'exigence de fonctionnement sécurisé et stable du système des noms de domaine ».

Article 11 : Les entités faisant une demande d'établissement d'un organisme chargé de l'enregistrement et de la gestion des noms de domaine doivent satisfaire aux conditions suivantes :

(1) le système de gestion des noms de domaine de premier niveau doit être établi sur le territoire, et les noms de domaine de premier niveau qui le composent doivent être conformes aux lois et règlements applicables et respecter l'exigence de fonctionnement sécurisé et stable du système des noms de domaine ;

(2) [elles doivent] être des personnes morales légalement constituées sur le territoire, ces personnes morales ainsi que leurs principaux investisseurs et membres du personnel opérationnel et de gestion devant présenter des registres de crédit satisfaisants ;

(3) elles doivent disposer de plans de développement professionnels et plans technologiques irréprochables, de locaux, de financements, d'un personnel expert capable d'assurer la gestion et les opérations liées aux noms de domaine de premier niveau, et de systèmes de gestion de l'information répondant aux exigences de l'organisme de gestion des télécommunications ;

(4) elles doivent avoir pris des mesures de gestion de la sécurité des réseaux et des informations, notamment un personnel de gestion, des structures de gestion de la sécurité des réseaux et des informations, des plans d'intervention d'urgence et des mesures technologiques et de gestion correspondantes ;

(5) elles doivent être en mesure de procéder à des vérifications des informations d'identité, d'assurer la protection des données personnelles des utilisateurs, de fournir des services

[31] Ministère de l'Industrie et des Technologies de l'information, mesures relatives à la gestion des noms de domaine Internet, 24 août 2017 https://www.chinalawtranslate.com/en/internet-domain-name-management-measures/ (traduction non officielle). Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.cac.gov.cn/2017-09/28/c_1121737753.htm.

durables ainsi que des mécanismes de cessation des services ;
(6) elles doivent disposer de structures de gestion des services d'enregistrement de noms de domaines et de mécanismes de supervision pour les organismes fournissant des services d'enregistrement de noms de domaine ;
(7) autres exigences prévues par les lois et règlements administratifs.
Article 12 : Les entités faisant une demande d'établissement d'un organisme fournissant des services d'enregistrement de noms de domaine doivent satisfaire aux conditions suivantes :
(1) le système des services d'enregistrement de noms de domaine, la base de données d'enregistrement et les systèmes de résolution doivent être établis sur le territoire ;
(2) [elles doivent] être des personnes morales légalement constituées sur le territoire, ces personnes morales ainsi que leurs principaux investisseurs et membres du personnel opérationnel et de gestion devant présenter des registres de crédits satisfaisants ;
(3) elles doivent disposer de locaux, de financements, d'un personnel expert capable d'assurer les services d'enregistrement de noms de domaine, et de systèmes de gestion de l'information répondant aux exigences de l'organisme de gestion des télécommunications ;
(4) elles doivent être en mesure de procéder à des vérifications des informations d'identité, d'assurer la protection des données personnelles des utilisateurs, de fournir des services durables ainsi que des mécanismes de cessation des services ;
(5) elles doivent disposer de structures de gestion des services d'enregistrement de noms de domaines et de mécanismes de supervision pour les organismes fournissant des services d'enregistrement de noms de domaine ;
(6) elles doivent avoir pris des mesures de protection de la sécurité des réseaux et des informations, notamment un personnel de gestion, des structures de gestion de la sécurité des réseaux et des informations, des plans d'intervention d'urgence et des mesures technologiques et de gestion correspondantes.
(7) autres exigences prévues par les lois et règlements administratifs.
Article 13 : Les entités faisant une demande d'établissement d'un serveur racine de nom de domaine, d'un organisme assurant le fonctionnement des serveurs racine ou d'un organisme chargé de l'enregistrement et de la gestion des noms de domaine doivent présenter un dossier de candidature au ministère de l'Industrie et des Technologies de l'information. Les entités faisant une demande d'établissement d'un organisme fournissant des services d'enregistrement de noms de domaine doivent présenter un dossier de candidature au département en charge de la gestion des télécommunications au niveau de la province, de la région autonome ou de la municipalité.
Le dossier de candidature doit comprendre les éléments suivants :
(1) des informations générales sur l'unité de travail faisant la demande ;
(2) des certificats attestant de la gestion effective des services de nom de domaine, dont des certificats attestant des systèmes, locaux, capacités de service, structures de gestion et accords conclus avec d'autres organismes ;
(3) des structures et mesures de protection de la sécurité des réseaux et des informations ;
(4) des documents attestant de la réputation de l'unité de travail faisant la demande ;
(5) une lettre d'engagement à mener des activités en toute sincérité et conformément à la loi signée par le représentant désigné. »
Article 37 : « Dans le cadre de la fourniture de services de résolution de noms de domaine, les informations liées à la résolution ne peuvent être falsifiées sans autorisation. La résolution de noms de domaine ne peut être redirigée à des fins malveillantes vers les adresses IP d'autres personnes par une organisation ou un individu.
L'**article 41** des mesures prévoit ce qui suit : « Lorsque cela s'avère nécessaire pour des raisons de sécurité nationale ou pour gérer des situations d'urgence, les organismes assurant le fonctionnement des serveurs racine de noms de domaine, les organismes chargés de

l’enregistrement et de la gestion des noms de domaine et les organismes fournissant des services d’enregistrement de noms de domaine doivent obéir aux ordres unifiés et aux impératifs de coordination des organismes de gestion des télécommunications et respecter leurs exigences en matière de gestion. »

Article 46 : « Les organismes de gestion des télécommunications doivent mettre en place des structures de registres de crédits pour les organismes assurant le fonctionnement des serveurs racine de noms de domaine, les organismes chargés de l’enregistrement et de la gestion des noms de domaine et les organismes fournissant des services d’enregistrement de noms de domaine, et doivent consigner dans le registre de crédits leurs violations des présentes mesures ainsi que les sanctions administratives associées. »

Annexe 3
Système des noms de domaine Internet chinois[32] (extraits)

I. Au sein de notre nation, tous les niveaux des noms de domaine Internet peuvent comprendre des lettres (indifféremment des lettres majuscules et minuscules, A-Z, a-z), des chiffres (0-9), des tirets (-) ou des caractères chinois ; et tous les domaines doivent utiliser des points (.) en tant que connecteurs, et tous les niveaux des noms de domaine de langue chinoise doivent utiliser soit des points soit des points chinois (。) en tant que connecteurs.

II. En plus des domaines de premier niveau « .CN » et « .中国 », le système des noms de domaine Internet de notre nation met en place plusieurs domaines de premier niveau en langue anglaise et chinoise, dont les domaines de premier niveau « 政务 » [.gov] et « .公益 » [.org - intérêt public] qui doivent être des domaines de premier niveau en langue chinoise spécialisés pour les groupes et organes du Parti et gouvernementaux à tous les échelons et autres départements des affaires gouvernementales, et pour les organismes à but non lucratif. Le diagramme du système des noms de domaine Internet de notre nation est disponible sur http://中国互联网域名体系.中国, http://中国互联网域名体系.政务 ou http://中国互联网域名体系.信息.

III. Sous le domaine de premier niveau national « .CN », deux types de domaines de second niveau sont mis en place : les « domaines de catégorie » et les « domaines de région administrative ». Neuf « domaines de catégorie » sont mis en place, à savoir : « 政务 » utilisé pour les groupes et organes du Parti et gouvernementaux à tous les échelons et autres départements des affaires gouvernementales ; « 公益 » utilisé pour les organismes à but non lucratif ; « GOV » utilisé pour les organes gouvernementaux ; « ORG » utilisé pour les organismes à but non lucratif ; « AC » utilisé pour les instituts de recherche scientifique ; « COM » utilisé pour les entreprises industrielles, commerciales, financières et autres ; « EDU » utilisé pour les établissements d'enseignement ; « MIL » utilisé pour les instituts de défense nationaux ; et « NET » utilisé pour les instituts fournissant des services Internet.
Trente-quatre « domaines de région administrative » sont mis en place afin d'être utilisés pour chacune des provinces, régions autonomes, municipalités sous contrôle direct et régions administratives spéciales […].

IV. Des demandes peuvent être déposées afin d'enregistrer directement des noms de domaine de second niveau sous les domaines de premier niveau nationaux « .CN » et « .中国 ».

[32] China Law Translate, système des noms de domaine Internet chinois, 5 mars 2018 https://www.chinalawtranslate.com/en/chinese-internet-domain-name-system/ (traduction non officielle). Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://xn--eqrt2g.xn--vuq861b/#.

Annexe 4
Loi sur la sécurité des données (DSL) de la République populaire de Chine[33] (extraits)

Article 3 : Dans le contexte de la présente loi, « données » désigne tout élément d'information disponible sous forme électronique ou autre.
- Le traitement des données comprend la collecte, le stockage, l'utilisation, la gestion, la transmission, la fourniture, la divulgation, etc. de données.
- La sécurité des données désigne la mise en œuvre des mesures requises afin de veiller à ce que les données soient réellement protégées et utilisées dans le respect de la loi, et le fait d'être en mesure de garantir durablement la sécurité.

Article 7 : L'État doit protéger les droits et intérêts des individus et des organisations eu égard aux données ; encourager l'utilisation légitime, raisonnable et judicieuse des données ; assurer une circulation des données libre, légale et ordonnée ; et promouvoir le développement d'une économie numérique avec des données comme principal moteur.

Article 11 : L'État doit activement mettre en place des échanges et une coopération au niveau international dans les secteurs de la gouvernance de la sécurité des données et du développement et de l'utilisation des données, participer à l'élaboration de règles et normes internationales en matière de sécurité des données, et promouvoir la circulation libre et sécurisée des données entre les pays.

Article 14 : L'État doit mettre en place une stratégie relative aux mégadonnées, promouvoir la mise en place d'infrastructures de données, et encourager et soutenir des applications innovantes de données dans tous les secteurs et domaines.

Article 17 : L'État doit promouvoir la mise en place d'un système de normes pour le développement des données, les technologies d'exploitation et la sécurité des données. Dans le cadre de leurs missions respectives, les départements du Conseil des affaires de l'État en charge de la normalisation et autres départements du Conseil des affaires de l'État concernés doivent assurer l'élaboration et la révision de normes liées aux technologies et produits pour le développement et l'utilisation de données et à la sécurité des données. L'État doit apporter un soutien aux entreprises, groupes sociaux, établissements d'enseignement et de recherche, etc. participant à l'élaboration de normes.

Article 21 : Les données liées à la sécurité nationale, aux moteurs de l'économie nationale, aux principaux moyens de subsistance des individus, aux principaux intérêts publics et autres aspects relevant des données essentielles de la nation doivent s'inscrire dans un système de gestion plus strict.

Article 25 : L'État doit mettre en place des contrôles des exportations conformément à la loi pour les données qui constituent des biens contrôlés, liées à la préservation de la sécurité nationale et à l'exécution d'obligations internationales.

Article 26 : Si un pays ou une région a recours à des mesures discriminatoires, restrictives ou autres mesures similaires à l'encontre de la République populaire de Chine dans des domaines tels que les investissements ou le commerce de données et technologies à des fins d'exploitation et de développement de données, la République populaire de Chine pourra

[33] Traduction de la loi sur la sécurité des données de la République populaire de Chine, 11 juin 2021 : https://www.secrss.com/articles/31844 (traduction non officielle, la publication originale est disponible ici : http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm). Ce document a été traduit dans plusieurs langues, à titre informatif uniquement. Seule la version originale (en chinois) fait foi. Elle peut être consultée sur : http://www.cac.gov.cn/2021-06/11/c_1624994566919140.htm.

prendre des mesures du même ordre à l'encontre de ce pays ou de cette région en fonction des circonstances.
Article 27 : La réalisation d'activités de traitement de données via des réseaux d'information, par exemple Internet, doit assurer la protection de la sécurité des données fondée sur le système de protection de la cybersécurité à plusieurs niveaux.
Article 31 : Les dispositions de la loi sur la cybersécurité de la République populaire de Chine s'appliquent à la gestion de la sécurité pour l'exportation de données provenant du territoire [continental] qui ont été collectées ou produites par les opérateurs d'infrastructures critiques en matière d'information sur le territoire [continental] de la République populaire de Chine ; des règles relatives à la gestion de la sécurité pour l'exportation d'importantes données provenant du territoire continental qui ont été collectées ou produites par d'autres responsables du traitement de données sur le territoire [continental] de la République populaire de Chine doivent être élaborées par le département de l'État en charge de l'information sur Internet conjointement avec les départements compétents du Conseil des affaires de l'État.
Article 32 : Les organisations ou individus qui collectent des données doivent avoir recours à des méthodes légales et adéquates et ne doivent pas voler ou obtenir des données en utilisant d'autres méthodes illégales. Lorsque les lois et règlements administratifs prévoient des dispositions concernant l'objectif ou la portée de la collecte et de l'utilisation de données, les données doivent être collectées ou utilisées dans le respect de l'objectif et de la portée prévus dans ces lois et règlements administratifs.
Article 33 : Lorsque des organismes fournissent des services d'intermédiaire pour des transactions de données, ils doivent imposer à la partie fournissant des données d'indiquer les sources des données, de vérifier l'identité des deux parties à la transaction et de tenir un registre de l'évaluation menée et de la transaction.
Article 36 : Les organes d'État compétents de la République populaire de Chine doivent, en vertu des dispositions des lois et traités ou accords auxquels la République populaire de Chine est partie, ou en vertu du principe d'égalité et d'avantages réciproques, traiter les demandes de fourniture de données des organismes judiciaires ou chargés de l'application de la loi étrangers. Sans l'approbation des organes d'État compétents de la République populaire de Chine, les organisations ou individus basés sur le territoire [continental] de la République populaire de Chine ne doivent pas fournir de données sur le territoire [continental] de la République populaire de Chine aux organismes judiciaires ou chargés de l'application de la loi étrangers.
Article 38 : L'exécution, par les organes d'État, de missions prévues par la loi qui nécessitent la collecte et l'utilisation de données doit relever du champ d'application des missions prévues par la loi et se conformer aux exigences et procédures prévues par les lois et règlements administratifs ; dans l'exécution des missions liées à la vie privée, les données personnelles, les secrets commerciaux, les données commerciales confidentielles et autres données doivent rester confidentiels conformément à la loi et ne doivent pas être divulgués ou fournis illégalement à des tiers.
Article 40 : Les organes d'État confiant à d'autres entités la mise en place ou le maintien de systèmes électroniques d'affaires gouvernementales ou le stockage ou le traitement de données relatives aux affaires gouvernementales doivent respecter des procédures d'approbation strictes et superviser l'exécution des obligations de protection de la sécurité des données correspondantes par lesdites entités. Ces entités doivent s'acquitter d'obligations de protection de la sécurité des données conformément aux dispositions des lois, règlements et accords contractuels, et ne doivent pas conserver, utiliser, divulguer ou fournir des données relatives aux affaires gouvernementales à des tiers sans autorisation.
Article 44 : Si les départements en charge de la réglementation exécutant des missions de supervision et de gestion de la sécurité des données constatent que des activités de traitement de données présentent des risques liés à la sécurité plus importants, ils pourront avoir une

discussion avec les organisations et individus concernés et imposer d'avoir recours à certaines procédures, d'apporter des corrections et de supprimer les dangers cachés conformément aux compétences et procédures prévues.
Article 49 : Si les organes d'État ne s'acquittent pas des obligations de protection de la sécurité des données tel que prévu dans la présente loi, les responsables directs et autre personnel directement responsable se verront infliger des sanctions conformément à la loi.
Article 52 : Si les violations des dispositions de la présente loi portent atteinte à des tiers, la responsabilité civile sera engagée conformément à la loi.

Annexe 5
Loi sur la protection des données personnelles de la République populaire de Chine[34]

(Adoptée à l'occasion de la 30e réunion du Comité permanent de la 13e Assemblée nationale populaire du 20 août 2021)

Chapitre I : Dispositions générales

Article 1 : La loi est formulée, sur le fondement de la Constitution, de sorte à protéger les droits et intérêts relatifs aux données personnelles, à normaliser les activités de traitement de données personnelles, et à promouvoir l'utilisation rationnelle des données personnelles.
Article 2 : Les données personnelles de personnes physiques bénéficient d'une protection juridique : aucune organisation ou aucun individu ne peut enfreindre les droits et intérêts relatifs aux données personnelles de personnes physiques.
Article 3 : La présente loi s'applique aux activités de traitement des données personnelles de personnes physiques situées dans les frontières de la République populaire de Chine.
En cas de survenue d'une des circonstances suivantes dans le cadre des activités de traitement, menées hors des frontières de la République populaire de Chine, de données personnelles de personnes physiques situées dans les frontières de la République populaire de Chine, la présente loi s'applique également :

1. Si l'objectif consiste à fournir des produits ou services à des personnes physiques à l'intérieur des frontières ;
2. En cas d'analyse ou d'évaluation d'activités menées par des personnes physiques à l'intérieur des frontières ;
3. En cas d'autres circonstances prévues par les lois ou règlements administratifs.

Article 4 : Les données personnelles constituent toutes sortes de données enregistrées par voie électronique ou autre liées à des personnes physiques identifiées ou identifiables ; les données anonymisées ne sont pas comprises dans cette définition.

[34] Loi sur la protection des données personnelles de la République populaire de Chine, (adoptée à l'occasion de la 30e réunion du Comité permanent de la 13e Assemblée nationale populaire du 20 août 2021), http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml. La traduction de DigiChina est disponible ici : https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021

Le traitement des données personnelles comprend la collecte, le stockage, l'utilisation, la gestion, la transmission, la fourniture, la publication, la suppression, etc. de données personnelles.
Article 5 : Les principes de légalité, de propriété, de nécessité et de sincérité doivent être respectés lors du traitement de données personnelles. Il est interdit de traiter des données personnelles à des fins coercitives, de tromperie, d'escroquerie ou autres.
Article 6 : Le traitement des données personnelles doit avoir un objectif clair et raisonnable, doit être directement lié à l'objectif du traitement, et doit avoir recours à une méthode ayant le plus faible impact sur les droits et intérêts des individus.
La collecte de données personnelles doit être exclusivement limitée à la réalisation de l'objectif du traitement et la collecte de données personnelles excessives est interdite.
Article 7 : Les principes d'ouverture et de transparence doivent être respectés lors du traitement de données personnelles, de la divulgation des règles relatives au traitement des données personnelles, et de l'indication claire de l'objectif, de la méthode et de la portée du traitement.
Article 8 : Le traitement de données personnelles doit garantir la qualité des données personnelles et éviter tout effet indésirable sur les droits et intérêts des individus découlant de données personnelles inexactes ou incomplètes.
Article 9 : Les responsables du traitement de données personnelles seront responsables de leurs activités de traitement de données personnelles et adopteront les mesures requises pour la protection de la sécurité des données personnelles qu'ils traitent.
Article 10 : Aucune organisation ou aucun individu ne pourra collecter, utiliser, traiter ou transmettre illégalement des données personnelles de tiers, ou vendre, acheter, fournir ou divulguer illégalement des données personnelles de tiers, ou mener des activités de traitement de données personnelles portant atteinte à la sécurité nationale ou à l'intérêt public.
Article 11 : L'État met en place une structure de protection des données personnelles afin de prévenir et de sanctionner tout acte portant atteinte aux droits et intérêts liés aux données personnelles, de renforcer la sensibilisation et l'éducation à la protection des données personnelles, et de promouvoir la création d'un environnement favorable à la protection des données personnelles, avec la participation commune des gouvernements, des entreprises, des organisations sociales concernées et du grand public.
Article 12 : L'État participe activement à l'élaboration de règles [ou normes] internationales pour la protection des données personnelles, encourage la coopération et les échanges internationaux dans le domaine de la protection des données personnelles, et promeut la reconnaissance mutuelle des règles [ou normes] pour la protection des données personnelles avec d'autres pays, régions et organisations internationales.

Chapitre II : Règles relatives au traitement des données personnelles

Section 1 : Dispositions générales

Article 13 : Les responsables du traitement de données personnelles pourront uniquement traiter des données personnelles s'ils satisfont l'une des exigences suivantes :

1. Obtention du consentement des individus ;
2. Nécessité de conclure ou d'exécuter un contrat dans lequel l'individu est une partie intéressée, ou nécessité d'assurer la gestion des ressources humaines conformément aux règles et structures en matière de travail élaborées dans le respect de la loi et aux contrats collectifs conclus ;
3. Nécessité de s'acquitter de fonctions, d'obligations et de responsabilités prévues par la loi ;

4. Nécessité d'intervenir en cas d'incidents soudains liés à la santé publique ou de protéger la vie et la santé, la sécurité ou la propriété de personnes physiques, dans des situations d'urgence ;
5. Traitement des données personnelles dans la mesure du raisonnable à des fins de diffusion d'actualités, de supervision de l'opinion publique et autres activités connexes relevant de l'intérêt public ;
6. Traitement des données personnelles divulguées par des individus ou relevant déjà du domaine public, dans la mesure du raisonnable et conformément aux dispositions de la présente loi.
7. Autres circonstances prévues par les lois ou règlements administratifs.

Conformément aux autres dispositions pertinentes de la présente loi, lors du traitement de données personnelles, le consentement de l'individu concerné doit être obtenu. Toutefois, l'obtention du consentement de l'individu n'est pas requise dans les conditions prévues aux points 2 à 7 susmentionnés.

Article 14 : En cas de traitement de données personnelles sur le fondement du consentement d'un individu, ledit consentement sera donné par l'individu sous réserve d'une parfaite connaissance des questions en jeu et sous la forme d'une déclaration volontaire et explicite. Si les lois ou règlements administratifs prévoient qu'un consentement distinct ou un consentement écrit doit être obtenu à des fins de traitement de données personnelles, ces dispositions doivent être respectées.

En cas de changement de l'objectif du traitement de données personnelles, de la méthode de traitement ou des catégories des données personnelles traitées, le consentement de l'individu devra de nouveau être obtenu.

Article 15 : En cas de traitement de données personnelles sur le fondement d'un consentement individuel, les individus ont le droit de retirer leur consentement. Les responsables du traitement de données personnelles doivent prévoir un moyen pratique pour le retrait du consentement. Le retrait du consentement d'un individu n'a aucun impact sur l'effectivité des activités de traitement de données personnelles menées sur le fondement du consentement individuel avant le retrait du consentement.

Article 16 : Les responsables du traitement de données personnelles ne peuvent refuser de fournir des produits ou services au motif qu'un individu ne consent pas au traitement de ses données personnelles ou retire son consentement, sauf si le traitement des données personnelles est nécessaire à la fourniture des produits ou services.

Article 17 : Les responsables du traitement de données personnelles doivent, avant le traitement des données personnelles, indiquer expressément, fidèlement, précisément et intégralement, en utilisant une terminologie claire et facile à comprendre, les éléments suivants :

1. Le nom et le contact du responsable du traitement de données personnelles ;
2. L'objectif du traitement des données personnelles et les méthodes de traitement, les catégories des données personnelles traitées et la période de conservation ;
3. Les méthodes et procédures permettant aux individus d'exercer les droits prévus dans la présente loi ;
4. D'autres éléments prévus par les lois ou règlements administratifs.

En cas de changement des éléments prévus dans le précédent paragraphe, les individus doivent en être informés.

Si les responsables du traitement de données personnelles fournissent les éléments prévus au point 1 via la méthode de divulgation des règles relatives au traitement des données personnelles, les règles relatives au traitement doivent être mises à la disposition du public et être facilement lisibles et stockables.

Article 18 : Les responsables du traitement de données personnelles ne sont pas autorisés à indiquer aux individus les éléments prévus au point 1 du précédent article si les lois ou règlements administratifs prévoient que la confidentialité doit être garantie ou si une telle indication n'est pas nécessaire.
En cas d'urgence, s'il est impossible d'indiquer ces éléments aux individus en temps opportun afin de protéger la vie et la santé des personnes physiques ainsi que la sécurité de leurs biens, les responsables du traitement de données personnelles doivent les indiquer à l'issue de la situation d'urgence.
Article 19 : Sauf en cas de dispositions contraires des lois ou règlements administratifs, la période de conservation des données personnelles doit être la période permettant d'atteindre l'objectif du traitement des données personnelles la plus courte possible.
Article 20 : Si au moins deux responsables du traitement de données personnelles définissent conjointement un objectif et une méthode de traitement des données personnelles, ils doivent convenir des droits et obligations de chacun d'entre eux. Toutefois, cet accord n'a pas d'impact sur le droit dont dispose un individu de demander à l'un quelconque des responsables du traitement de données personnelles d'exécuter sa mission dans le respect des dispositions de la présente loi.
Si des responsables du traitement de données personnelles assurant un traitement conjoint des données personnelles portent atteinte aux droits et intérêts liés aux données personnelles, entraînant des dommages, ils seront tous deux tenus responsables en vertu de la loi.
Article 21 : Si les responsables du traitement de données personnelles confient le traitement des données personnelles, ils doivent conclure un accord avec la personne à qui est confié le traitement convenant de l'objectif du traitement confié, de sa durée, de la méthode de traitement, des catégories de données personnelles, des mesures de protection, et des droits et devoirs des deux parties à l'accord, etc., et assurer la supervision des activités de traitement des données personnelles assurées par la personne à qui est confié le traitement.
La personne à qui est confié le traitement doit traiter les données personnelles dans le respect des dispositions de l'accord ; elle ne doit pas traiter les données personnes à des fins ou en utilisant des méthodes, etc. non prévues par l'accord. Si l'accord conclu n'entre pas en vigueur, est frappé de nullité, est annulé ou est résilié, la personne à qui est confié le traitement doit restituer les données personnelles au responsable du traitement de données personnelles ou les supprimer, et ne peut les conserver.
Sans le consentement du responsable du traitement de données personnelles, une personne à qui est confié le traitement ne peut confier le traitement des données personnelles à des tiers.
Article 22 : Les responsables du traitement de données personnelles doivent, s'il est nécessaire de transférer des données personnelles suite à une fusion, une scission, une dissolution, une déclaration de faillite ou pour d'autres motifs, indiquer aux individus le nom et le contact de la partie destinataire. La partie destinataire doit continuer à s'acquitter des obligations du responsable du traitement de données personnelles. Si la partie destinataire modifie l'objectif ou la méthode du traitement original, elle doit de nouveau en informer l'individu conformément à la présente loi.
Article 23 : Si les responsables du traitement de données personnelles fournissent à d'autres responsables du traitement de données personnelles les données personnelles qu'ils traitent, ils doivent indiquer aux individus le nom du destinataire, son contact, l'objectif du traitement, la méthode de traitement et les catégories de données personnelles, et obtenir le consentement de chaque individu. Les destinataires doivent traiter les données personnelles dans le cadre susmentionné des objectifs de traitement, des méthodes de traitement, des catégories de données personnelles, etc. Si les destinataires modifient l'objectif ou la méthode du traitement original, ils doivent de nouveau obtenir le consentement des individus.

Article 24 : Lorsque les responsables du traitement de données personnelles utilisent des données personnelles afin de prendre des décisions automatisées, la transparence du processus de décision et l'équité du traitement doivent être garanties, et ils ne peuvent procéder à un traitement différentiel déraisonnable des individus eu égard aux conditions commerciales telles que le prix de l'opération, etc.
Les responsables qui effectuent des transmissions d'informations ou des ventes à des individus via des méthodes de prise de décision automatisée doivent également proposer l'option de ne pas cibler certaines caractéristiques des individus ou proposer aux individus une option de refus pratique.
Si le recours à une prise de décision automatisée génère des décisions ayant un impact non négligeable sur les droits et intérêts des individus, ces derniers sont en droit de demander aux responsables du traitement de données personnelles des explications et de refuser que les responsables du traitement de données personnelles prennent des décisions uniquement via des méthodes de prise de décision automatisée.
Article 25 : Les responsables du traitement de données personnelles ne peuvent divulguer les données personnelles qu'ils traitent, sauf s'ils obtiennent un consentement séparé.
Article 26 : L'installation d'équipements de collecte d'images ou de reconnaissance d'identité personnelle dans des espaces publics doit être effectuée de sorte à protéger la sécurité publique et dans le respect des réglementations de l'État, et une signalisation claire doit être mise en place. Les images personnelles et les données personnelles permettant de distinguer clairement l'identité d'une personne ne peuvent être utilisées qu'aux fins de protection de la sécurité publique ; elles ne peuvent être utilisées à d'autres fins, sauf si le consentement de chaque individu est obtenu.
Article 27 : Les responsables du traitement de données personnelles peuvent, dans la mesure du raisonnable, traiter des données personnelles qui ont déjà été divulguées par la personne concernée ou divulguées du fait de la loi, sauf si la personne oppose un refus clair. Les responsables du traitement de données personnelles qui traitent des données personnelles déjà divulguées, avec un impact non négligeable sur les droits et intérêts des individus, doivent obtenir le consentement de chaque individu conformément aux dispositions de la présente loi.

Section II : Règles relatives au traitement des données personnelles sensibles

Article 28 : Les données personnelles sensibles désignent les données personnelles qui, en cas de fuite ou d'utilisation illégale, peuvent aisément porter atteinte à la dignité des personnes physiques ou à leur sécurité personnelle ou à la sécurité de leurs biens, notamment des données relatives à des caractéristiques biométriques, à des croyances religieuses, à un statut spécifique, à la santé, à des comptes financiers, à la géolocalisation de l'individu, etc., ainsi que les données personnelles de mineurs âgés de moins de 14 ans.
Les responsables du traitement de données personnelles peuvent uniquement traiter des données personnelles sensibles s'ils ont un objectif spécifique, en cas de nécessité et s'ils ont mis en place des mesures de protection strictes.
Article 29 : Afin de traiter des données personnelles sensibles, le consentement de chaque individu doit être obtenu. Si les lois ou règlements administratifs prévoient qu'un consentement écrit doit être obtenu à des fins de traitement de données personnelles sensibles, ces dispositions doivent être respectées.
Article 30 : Les responsables du traitement de données personnelles qui traitent des données personnelles sensibles, en plus des éléments prévus au paragraphe 1 de l'article 17 de la présente loi, doivent également indiquer aux individus la nécessité en question et l'impact sur les droits et intérêts des individus du traitement des données personnelles sensibles, sauf si la présente loi prévoit qu'il est autorisé de ne pas indiquer ces éléments aux individus.

Article 31 : Si les responsables du traitement de données personnelles traitent les données personnelles de mineurs âgés de moins de 14 ans, ils doivent obtenir le consentement du parent ou tuteur du mineur.
Si les responsables du traitement de données personnelles traitent les données personnelles de mineurs âgés de moins de 14 ans, ils doivent élaborer des règles spécifiques relatives au traitement desdites données personnelles.
Article 32 : Si les lois ou règlements administratifs prévoient que des autorisations administratives doivent être obtenues ou si d'autres restrictions s'appliquent au traitement de données personnelles sensibles, ces dispositions doivent être respectées.

Section III : Dispositions spécifiques relatives au traitement de données personnelles par des organes d'État

Article 33 : La présente loi s'applique aux activités de traitement de données personnelles des organes d'État ; si la présente section contient des dispositions spécifiques, ces dispositions s'appliqueront.
Article 34 : Les organes d'État qui traitent des données personnelles afin de s'acquitter de leurs missions et responsabilités prévues par la loi doivent s'en acquitter dans le respect des compétences et procédures prévues dans les lois ou règlements administratifs ; ils ne peuvent outrepasser le cadre requis pour s'acquitter de leurs missions et responsabilités prévues par la loi.
Article 35 : Les organes d'État qui traitent des données personnelles afin de s'acquitter de leurs missions et responsabilités prévues par la loi doivent respecter des obligations de notification, sauf dans les cas prévus au paragraphe 1 de l'article 18 de la présente loi, ou si les obligations de notification empêchent les organes d'État de s'acquitter de leurs missions et responsabilités prévues par la loi.
Article 36 : Les données personnelles traitées par les organes d'État doivent être stockées sur le territoire continental de la République populaire de Chine. S'il est réellement nécessaire de les transférer à l'étranger, une évaluation de la sécurité doit être menée. Les autorités compétentes peuvent être tenues d'apporter un soutien et une assistance à l'évaluation de la sécurité.
Article 37 : Les dispositions de la présente loi relatives à la gestion de données personnelles par des organes d'État s'appliquent au traitement de données personnelles par des organisations autorisées par les lois et règlements à assurer la gestion de fonctions liées à des affaires publiques afin de s'acquitter de leurs missions prévues par la loi.

Chapitre III : Règles relatives à la fourniture transfrontalière de données personnelles

Article 38 : Si les responsables du traitement de données personnelles ont réellement besoin de fournir des données personnelles hors des frontières de la République populaire de Chine à des fins d'activités commerciales ou autres, ils doivent respecter l'une des conditions suivantes :

1. Réussir une évaluation de la sécurité organisée par le département de la cybersécurité et de l'informatisation de l'État conformément à l'article 40 de la présente loi ;
2. Obtenir une certification de protection des données personnelles délivrée par un organisme spécialisé conformément aux dispositions du département de la cybersécurité et de l'informatisation de l'État ;
3. Conclure avec la partie destinataire étrangère un contrat conforme à un contrat standard rédigé par le département de la cybersécurité et de l'informatisation de l'État, prévoyant les droits et responsabilités des deux parties ;

4. Autres conditions prévues par les lois et règlements administratifs ou par le département de la cybersécurité et de l'informatisation de l'État.

Si les traités ou accords internationaux auxquels la République populaire de Chine est partie contiennent des dispositions prévoyant par exemple les conditions de la fourniture de données personnelles hors des frontières de la République populaire de Chine, ces dispositions peuvent être appliquées.

Les responsables du traitement de données personnelles doivent adopter les mesures nécessaires afin que les activités de traitement des données personnelles des parties destinataires étrangères atteignent le niveau de protection des données personnelles prévu dans la présente loi.

Article 39 : Si les responsables du traitement de données personnelles fournissent des données personnelles hors des frontières de la République populaire de Chine, ils doivent indiquer aux individus concernés le nom et le contact de la partie destinataire étrangère, l'objectif du traitement, les méthodes de traitement et les catégories de données personnelles, ainsi que les moyens ou procédures permettant aux individus d'exercer les droits prévus dans la présente loi auprès de la partie destinataire étrangère, et tous autres éléments connexes, et obtenir le consentement de chaque individu.

Article 40 : Les opérateurs d'infrastructures critiques en matière d'information et les responsables du traitement de données personnelles qui traitent des données personnelles dans des quantités prévues par le département de la cybersécurité et de l'informatisation de l'État doivent stocker sur le territoire national les données personnelles collectées et produites à l'intérieur des frontières de la République populaire de Chine. S'ils sont tenus de les fournir à l'étranger, ils doivent réussir une évaluation de la sécurité menée par le département de la cybersécurité et de l'informatisation de l'État ; si les lois ou règlements administratifs et les dispositions du département de la cybersécurité et de l'informatisation de l'État permettent que l'évaluation de la sécurité ne soit pas menée, ces dispositions doivent être respectées.

Article 41 : Les autorités compétentes de la République populaire de Chine, conformément aux lois applicables et aux traités ou accords internationaux auxquels la République populaire de Chine est partie, ou conformément au principe d'égalité et d'avantages réciproques, doivent traiter les demandes des organismes judiciaires ou chargés de l'application de la loi étrangers de fourniture de données personnelles stockées sur le territoire national. Sans l'approbation des autorités compétentes de la République populaire de Chine, les responsables du traitement de données personnelles ne peuvent fournir de données personnelles stockées sur le territoire continental de la République populaire de Chine aux organismes judiciaires ou chargés de l'application de la loi étrangers.

Article 42 : Si des organisations ou individus étrangers mènent des activités de traitement de données personnelles en violation des droits et intérêts liés aux données personnelles des citoyens de la République populaire de Chine, ou portant atteinte à la sécurité nationale ou à l'intérêt public de la République populaire de Chine, le département de la cybersécurité et de l'informatisation de l'État peut les inscrire sur une liste restreignant ou interdisant la fourniture de données personnelles à certaines entités, leur donner un avertissement et adopter des mesures telles que la limitation ou l'interdiction de la fourniture de données personnelles auxdits organisations ou individus étrangers, etc.

Article 43 : Si un pays ou une région adopte des mesures discriminatoires, restrictives, d'interdictions ou autres mesures similaires à l'encontre de la République populaire de Chine dans le domaine de la protection des données personnelles, la République populaire de Chine pourra prendre des mesures du même ordre à l'encontre de ce pays ou de cette région en fonction des circonstances.

Chapitre IV : Droits des individus eu égard aux activités de traitement de données personnelles

Article 44 : Les individus ont le droit de savoir et le droit de décider eu égard à leurs données personnelles, et ont le droit de limiter ou de refuser le traitement de leurs données personnelles par des tiers, sauf disposition contraire des lois ou règlements administratifs.

Article 45 : Les individus ont le droit de consulter et de copier leurs données personnelles en possession des responsables du traitement de données personnelles, sauf dans les cas prévus au paragraphe 1 de l'article 18 ou à l'article 35 de la présente loi.

Si les individus demandent à consulter ou copier leurs données personnelles, les responsables du traitement de données personnelles doivent leur fournir ces données en temps opportun.

Si les individus demandent le transfert de leurs données personnelles à un responsable du traitement de données personnelles désigné, dans le respect des conditions prévues par le département de la cybersécurité et de l'informatisation de l'État, les responsables du traitement de données personnelles doivent fournir un moyen de les transférer.

Article 46 : Si les individus constatent que leurs données personnelles sont incorrectes ou incomplètes, ils ont le droit de demander aux responsables du traitement de données personnelles de corriger ou de compléter leurs données personnelles. Si les individus demandent à ce que leurs données personnelles soient corrigées, les responsables du traitement de données personnelles doivent vérifier les données personnelles et les corriger en temps opportun.

Si les individus demandent à ce que leurs données personnelles soient complétées, les responsables du traitement de données personnelles doivent vérifier les données personnelles et les compléter en temps opportun.

Article 47 : Les responsables du traitement de données personnelles doivent supprimer rapidement les données personnelles en cas de survenue d'une des circonstances suivantes ; à défaut, les individus ont le droit de demander leur suppression :

1. L'objectif du traitement a été atteint, est impossible à atteindre ou les [données personnelles] ne sont plus nécessaires afin d'atteindre l'objectif du traitement ;
2. Les responsables du traitement de données personnelles cessent de fournir les produits ou services, ou la période de conservation a expiré ;
3. Les individus retirent leur consentement ;
4. Les responsables du traitement de données personnelles ont traité des données personnelles en violation de lois, règlements administratifs ou accords ;
5. Autres circonstances prévues par les lois ou règlements administratifs.

Si la période de conservation prévue par les lois ou règlements administratifs n'a pas expiré, ou si la suppression des données personnelles est difficile à réaliser d'un point de vue technique, les responsables du traitement de données personnelles doivent cesser de traiter les données personnelles sauf à des fins de stockage et d'adoption de mesures nécessaires de protection de la sécurité.

Article 48 : Les individus ont le droit de demander aux responsables du traitement de données personnelles de leur expliquer les règles relatives au traitement des données personnelles.

Article 49 : En cas de décès d'une personne physique, ses proches parents peuvent, afin de préserver leurs propres intérêts légitimes, exercer les droits prévus dans le présent chapitre de sorte à consulter, copier, corriger, supprimer, etc., les données personnelles du défunt, sauf si le défunt en avait décidé autrement avant son décès.

Article 50 : Les responsables du traitement de données personnelles doivent mettre en place des mécanismes visant à accepter et traiter les demandes d'individus souhaitant exercer leurs droits. S'ils rejettent la demande d'un individu souhaitant exercer ses droits, ils doivent en indiquer la raison.

Si les responsables du traitement de données personnelles rejettent la demande d'un individu souhaitant exercer ses droits, ledit individu peut, conformément à la loi, engager des poursuites auprès d'un tribunal populaire.

Chapitre V : Missions des responsables du traitement de données personnelles

Article 51 : Les responsables du traitement de données personnelles doivent, en fonction de l'objectif du traitement des données personnelles, des méthodes de traitement, des catégories de données personnelles, de l'impact sur les droits et intérêts des individus, des éventuels risques liés à la sécurité, etc., adopter les mesures suivantes visant à garantir que le traitement des données personnelles soit conforme aux dispositions des lois et règlements administratifs, et à empêcher l'accès non autorisé aux données personnelles ainsi que leur fuite, falsification ou perte :

2. Mettre en place des structures de gestion internes et des règles de fonctionnement ;
3. Mettre en œuvre une gestion des données personnelles en fonction de leur catégorie ;
4. Adopter des mesures correspondantes relatives à la sécurité technique telles que le chiffrement, la désidentification, etc. ;
5. Déterminer des limites opérationnelles raisonnables pour le traitement de données personnelles et organiser régulièrement des séances de sensibilisation et de formation pour les employés ;
6. Formuler et organiser la mise en œuvre de plans d'intervention en cas d'incidents de sécurité liés aux données personnelles ;
7. Autres mesures prévues par les lois ou règlements administratifs.

Article 52 : Les responsables du traitement de données personnelles qui traitent des données personnelles dans des quantités prévues par le département de la cybersécurité et de l'informatisation de l'État doivent désigner des délégués à la protection des données personnelles qui seront chargés de superviser les activités de traitement de données personnelles ainsi que les mesures de protection adoptées, etc.

Les responsables du traitement de données personnelles publieront les contacts des délégués à la protection des données personnelles et transmettront leurs noms et contacts aux départements ayant des missions et responsabilités en matière de protection des données personnelles.

Article 53 : Les responsables du traitement de données personnelles basés hors des frontières de la République populaire de Chine, tel que prévu au paragraphe 2 de l'article 3 de la présente loi, créeront une entité dédiée ou désigneront un représentant à l'intérieur des frontières de la République populaire de Chine qui sera en charge des questions liées aux données personnelles qu'ils traitent, et transmettront le nom, le contact, etc. de l'entité ou du représentant aux départements ayant des missions et responsabilités en matière de protection des données personnelles.

Article 54 : Les responsables du traitement de données personnelles mèneront régulièrement des audits de leur traitement des données personnelles et de leur conformité aux lois et règlements administratifs.

Article 55 : Si l'un des cas suivants se présente, les responsables du traitement de données personnelles doivent effectuer au préalable une étude d'impact de la protection des données personnelles et consigner le statut du traitement :

1. Traitement de données personnelles sensibles ;
2. Utilisation de données personnelles à des fins de prise de décision automatisée ;
3. Sous-traitance du traitement de données personnelles, fourniture de données personnelles à d'autres responsables du traitement de données personnelles, ou divulgation de données personnelles ;

4. Fourniture de données personnelles à l'étranger ;
5. Autres activités de traitement de données personnelles ayant un impact non négligeable sur les individus.

Article 56 : L'étude d'impact de la protection des données personnelles doit indiquer :

1. Si l'objectif du traitement des données personnelles, la méthode de traitement, etc. sont légaux, légitimes et nécessaires ;
2. L'impact sur les droits et intérêts des individus et les risques liés à la sécurité ;
3. Si les mesures de protection adoptées sont légales, efficaces et adaptées au niveau de risque.

Les rapports de l'étude d'impact de la protection des données personnelles et les registres consignant le statut du traitement doivent être conservés pendant au moins trois ans.

Article 57 : En cas de fuite, de falsification ou de perte, avérée ou présumée, des données personnelles, les responsables du traitement de données personnelles doivent immédiatement adopter des mesures correctives et en notifier les départements ayant des missions et responsabilités en matière de protection des données personnelles ainsi que les individus. Cette notification doit comprendre les éléments suivants :

1. Les catégories de données, les causes et les éventuels dommages causés par la fuite, la falsification ou la perte qui s'est produite ou a pu se produire ;
2. Les mesures correctives prises par les responsables du traitement de données personnelles et les mesures que les individus peuvent adopter afin de réduire les dommages ;
3. Le contact du responsable du traitement de données personnelles.

Si les responsables du traitement de données personnelles adoptent des mesures à même d'éviter les dommages engendrés par la fuite, la falsification ou la perte, les responsables du traitement de données personnelles sont autorisés à ne pas en notifier les individus ; toutefois, si les départements ayant des missions et responsabilités en matière de protection des données personnelles estiment qu'il existe de réels dommages, ils peuvent imposer aux responsables du traitement de données personnelles d'en notifier les individus.

Article 58 : Les responsables du traitement de données personnelles fournissant d'importants services de plate-forme Internet, qui ont un grand nombre d'utilisateurs, et dont les modèles commerciaux sont complexes, doivent s'acquitter des obligations suivantes :

1. Définir et mettre en place des systèmes et structures de mise en conformité de la protection des données personnelles dans le respect des réglementations de l'État, et établir un organisme indépendant principalement composé de membres externes chargé de superviser l'état de la protection des données personnelles ;
2. Respecter les principes d'ouverture, d'équité et de justice ; élaborer des règles pour les plates-formes ; et préciser les normes pour le traitement par les fournisseurs de produits ou services d'intra-plate-forme de données personnelles et leurs missions liées à la protection des données personnelles ;
3. Interrompre la fourniture de services aux fournisseurs de produits ou services sur la plate-forme coupables d'une violation grave des lois ou règlements administratifs lors du traitement de données personnelles ;
4. Publier régulièrement des rapports sur la responsabilité sociale de la protection des données personnelles et accepter la supervision de la société.

Article 59 : Les personnes acceptant de se voir confier le traitement de données personnelles doivent, conformément aux dispositions de la présente loi et des lois et règlements administratifs applicables, prendre les mesures nécessaires afin de protéger la sécurité et les données personnelles qu'elles traitent, et aider les responsables du traitement de données personnelles à s'acquitter des obligations prévues dans la présente loi.

8. Chapitre VI : Départements ayant des missions et responsabilités en matière de protection des données personnelles

Article 60 Le département de la cybersécurité et de l'informatisation de l'État est chargé de planifier et de coordonner l'ensemble des activités en matière de protection des données personnelles et activités connexes de supervision et gestion. Les départements compétents du Conseil des affaires de l'État sont chargés de mener des activités de protection, de supervision et de gestion des données personnelles dans le cadre de leurs missions et responsabilités respectives, conformément aux dispositions de la présente loi et des lois et règlements administratifs applicables.

Les missions et responsabilités en matière de protection, de supervision et de gestion des données personnelles des départements compétents des gouvernements populaires des comtés et échelons supérieurs sont déterminées conformément aux dispositions des départements du Conseil des affaires de l'État applicables.

Les départements indiqués dans les deux précédents paragraphes sont tous des départements ayant des missions et responsabilités en matière de protection des données personnelles.

Article 61 : Les départements ayant des missions et responsabilités en matière de protection des données personnelles s'acquittent des missions et responsabilités en matière de protection des données personnelles suivantes :

1. Assurer des actions de sensibilisation et d'éducation à la protection des données personnelles, et orienter et superviser les activités menées par les responsables du traitement de données personnelles en matière de protection des données personnelles ;
2. Accepter et traiter les plaintes et rapports portant sur la protection des données personnelles ;
3. Procéder à l'évaluation de l'état de la protection des données personnelles, notamment les procédures utilisées, et publier les résultats de l'évaluation.
4. Mener des recherches sur les activités de traitement de données personnelles et assurer leur gestion ;
5. Autres missions et responsabilités prévues par les lois ou règlements administratifs.

Article 62 : Le département de la cybersécurité et de l'informatisation de l'État assure la coordination de l'ensemble des activités suivantes de protection des données personnelles menées par les départements compétents :

1. Élaborer des règles et normes de protection des données personnelles ;
2. Élaborer des règles et normes spécifiques de protection des données personnelles pour les responsables du traitement de données personnelles de petite taille et les nouvelles technologies et applications pour le traitement des données personnelles sensibles, la reconnaissances faciale, l'intelligence artificielle, etc. ;
3. Soutenir la recherche, le développement et l'adoption à grande échelle de technologies d'authentification d'identité numérique sécurisées et pratiques, et promouvoir la conception de services publics d'authentification d'identité numérique ;
4. Faire progresser la conception de systèmes de services visant à socialiser la protection des données personnelles et encourager les organisations concernées à lancer des services d'évaluation et de certification de la protection des données personnelles ;
5. Mettre au point des mécanismes de plainte et signalement pour la protection des données personnelles.

Article 63 : Lorsque les départements ayant des missions et responsabilités en matière de protection des données personnelles s'acquittent de missions et responsabilités en matière de protection des données personnelles, ils peuvent adopter les mesures suivantes :

1. Interviewer les parties concernées, et enquêter sur l'état des activités de traitement des données personnelles ;

2. Consulter et reproduire les contrats, registres et reçus d'une partie concernée ainsi que tous autres supports liés aux activités de traitement des données personnelles ;
3. Effectuer des contrôles sur site et enquêter sur des activités de traitement des données personnelles prétendument illégitimes ;
4. Contrôler les équipements et articles utilisés dans le cadre des activités de traitement des données personnelles ; et s'il est prouvé que les équipements ou articles sont utilisés afin de mener des activités de traitement des données personnelles illégales, après en avoir informé le responsable de leur département par écrit et après avoir reçu une approbation, les sceller ou les confisquer.

Lorsque les départements ayant des missions et responsabilités en matière de protection des données personnelles s'acquittent de leurs missions et responsabilités conformément à la loi, les parties concernées doivent prêter assistance et coopérer et ne peuvent entraver leurs missions ou les empêcher de s'en acquitter.

Article 64 : Lorsque les départements ayant des missions et responsabilités en matière de protection des données personnelles constatent que des activités de traitement des données personnelles comportent des risques ou que des incidents liés à la sécurité des données personnelles se sont produits, ils peuvent avoir une discussion avec le représentant légal ou le supérieur du responsable du traitement des données personnelles dans le respect des compétences et procédures réglementaires, ou imposer aux responsables du traitement de données personnelles de faire appel à des instituts spécialisés pour mener des audits de conformité de leurs activités de traitement des données personnelles. Les responsables du traitement de données personnelles doivent adopter des mesures conformément aux obligations d'apporter des corrections et de supprimer les vulnérabilités.

Lorsque les départements ayant des missions et responsabilités en matière de protection des données personnelles constatent, dans le cadre de leurs missions, un traitement illégal de données personnelles susceptible de constituer un crime, ils doivent saisir les autorités chargées de la sécurité publique qui devront alors se prononcer conformément à la loi.

Article 65 : Les organisations ou individus ont le droit de déposer une plainte ou de signaler des activités de traitement de données personnelles illégales aux départements ayant des missions et responsabilités en matière de protection des données personnelles. Les départements recevant des plaintes ou signalements doivent les traiter dans de brefs délais et conformément à la loi, et transmettre leurs conclusions à la personne à l'origine de la plainte ou du signalement.

Les départements ayant des missions et responsabilités en matière de protection des données personnelles doivent publier les contacts pour les plaintes et signalements.

Chapitre VII : Responsabilité légale

Article 66 : Si les données personnelles sont traitées en violation de la présente loi ou si les données personnelles sont traitées sans s'acquitter des missions de protection des données personnelles conformément aux dispositions de la présente loi, les départements ayant des missions et responsabilités en matière de protection des données personnelles doivent imposer d'apporter des corrections, confisquer les gains illégitimes et ordonner la suspension temporaire ou la cessation de la fourniture de services des logiciels d'application procédant au traitement des données personnelles ; si une correction est refusée, une amende maximale de 1 million de yuans doit en plus être imposée ; les responsables directs et autre personnel directement responsable se verront infliger une amende comprise entre 10 000 et 100 000 yuans.

Si la gravité des agissements illégitimes indiqués dans le précédent paragraphe l'exige, les départements à l'échelle de la province ou à l'échelon supérieur ayant des missions et responsabilités en matière de protection des données personnelles doivent imposer d'apporter des corrections, confisquer les gains illégitimes et imposer une amende maximale de 50

millions de yuans, ou 5 % des revenus annuels. Ils peuvent également ordonner la suspension des activités commerciales connexes ou la cessation des activités afin d'apporter des corrections, et en informer le département compétent à des fins d'annulation des autorisations administratives correspondantes ou d'annulation des licences commerciales. Le responsable direct et autre personnel directement responsable doivent se voir infliger une amende comprise entre 100 000 yuans et 1 million de yuans, et il peut également être décidé de leur interdire d'occuper des postes de directeur, superviseur, haut responsable ou délégué à la protection des données personnelles pendant une certaine période.

Article 67 : En cas d'agissements illégaux tel que prévu dans la présente loi, ces agissements seront consignés dans les registres de crédits conformément aux lois et règlements administratifs applicables, et feront l'objet d'une publication.

Article 68 : En cas d'incapacité des organes d'État à s'acquitter des missions de protection des données personnelles prévues par la présente loi, les organes hiérarchiquement supérieurs ou les départements ayant des missions et responsabilités en matière de protection des données personnelles doivent imposer d'apporter des corrections ; le responsable direct et autre personnel directement responsable doivent se voir infliger des sanctions conformément à la loi. Si le personnel des départements ayant des missions et responsabilités en matière de protection des données personnelles manque à ses missions, abuse de son pouvoir ou fait preuve de favoritisme, sans que cela ne constitue un crime, des sanctions seront imposées conformément à la loi.

Article 69 : Si le traitement des données personnelles viole les droits et intérêts liés aux données personnelles et entraîne des dommages, et que les responsables du traitement de données personnelles ne peuvent prouver qu'ils ne sont pas en tort, ils devront verser des indemnités et assumer la responsabilité de leur violation.

Ce versement d'indemnités au titre de la violation sera déterminé en tenant compte des pertes subies par l'individu ou des avantages dont a profité le responsable du traitement de données personnelles. S'il est difficile de déterminer les pertes subies par l'individu et les avantages dont a profité le responsable du traitement de données personnelles, les indemnités seront déterminées en fonction des conditions pratiques.

Article 70 : Si les responsables du traitement de données personnelles traitent les données personnelles en violation des dispositions de la présente loi et portent atteinte aux droits et avantages de nombreux individus, les parquets populaires, les organisations de défense des consommateurs désignées par la loi et les organisations désignées par le département de la cybersécurité et de l'informatisation de l'État peuvent engager des poursuites auprès d'un tribunal populaire conformément à la loi.

Article 71 : Si une violation des dispositions de la présente loi constitue une violation liée à la gestion de la sécurité publique, une sanction doit être imposée conformément à la loi ; si elle constitue un crime, la responsabilité pénale doit être engagée conformément à la loi.

Chapitre VIII : Dispositions supplémentaires

Article 72 : La présente loi ne s'applique pas aux personnes physiques qui traitent des données personnelles dans un cadre personnel ou familial.

Si la loi contient des dispositions relatives au traitement de données personnelles par des gouvernements populaires à tous échelons et par leurs départements et organisations concernés mettant en œuvre des activités de gestion des statistiques et archives, ces dispositions s'appliqueront.

Article 73 : Dans le contexte de la présente loi, les termes suivants sont définis tel que suit :

1. « Responsable du traitement de données personnelles » désigne les organisations et individus qui, dans le cadre d'activités de traitement de données personnelles, décident en toute indépendance des objectifs et des méthodes de traitement.

2. « Prise de décision automatisée » désigne le recours à des programmes informatiques afin d'analyser ou d'évaluer automatiquement des comportements, habitudes, intérêts ou passions d'une personne, ou sa situation financière, son état de santé, ses crédits ou autres, et de prendre des décisions [sur la base de cette analyse ou évaluation].
3. « Désidentification » désigne le processus visant à traiter des données personnelles de sorte à ce qu'il soit impossible d'identifier les personnes physiques concernées sans avoir recours à des informations complémentaires.
4. « Anonymisation » désigne le processus visant à traiter des données personnelles de sorte à ce qu'il soit impossible de distinguer les personnes physiques concernées et impossible de restaurer leur identité.

Article 74 : La présente loi entrera en vigueur le 1er novembre 2021.

Annexe 6
Règlement relatif à la protection de la sécurité d'infrastructures critiques en matière d'information [35] (extraits)

Article 2 : Les infrastructures critiques en matière d'information faisant l'objet du présent règlement désignent les importantes infrastructures de réseau, infrastructures d'information, etc., dans d'importants secteurs et industries tels que les services de communication et d'information publiques, l'énergie, les transports, les ressources hydriques, la finance, les services publics, l'e-gouvernement, la défense nationale, les sciences, les technologies et l'industrie, etc., qui, en cas de destruction, de perte de fonctionnalités ou de fuite de données, pourraient gravement compromettre la sécurité nationale, l'économie nationale, les moyens de subsistance des personnes ou l'intérêt public.
Article 8 : Les départements compétents ainsi que les départements en charge de la supervision et de la gestion d'importants secteurs et industries indiqués à l'article 2 du présent règlement sont les départements responsables des activités de protection des infrastructures critiques en matière d'information (ci-après les « départements en charge des activités de protection »).
Article 9 : Les départements en charge des activités de protection doivent élaborer des règles d'identification des infrastructures critiques en matière d'information en tenant compte de la situation concrète de leurs secteurs et industries, et les communiquer au département en charge de la sécurité publique du Conseil des affaires de l'État à des fins de dépôt.
Lors de l'élaboration des règles d'identification, les facteurs suivants doivent être pris en compte :

1. L'importance de l'infrastructure de réseau, du système d'information, etc., pour les principales activités critiques du secteur ou de l'industrie ;
2. Les dommages susceptibles de découler de la destruction, de la perte de fonctionnalités ou de la fuite de données de l'infrastructure de réseau, du système d'information, etc. ;
3. L'impact sur d'autres secteurs et industries.

Article 18 : En cas d'incidents de cybersécurité majeurs ou de menaces importantes à la cybersécurité dans les infrastructures critiques en matière d'information, les opérateurs doivent les signaler aux départements en charge des activités de protection et aux autorités chargées de la sécurité publique conformément aux réglementations applicables.
Si les infrastructures critiques en matière d'information cessent complètement de fonctionner ou que leurs principales fonctions sont entravées, en cas de fuite d'informations nationales de base ou autres données importantes, en cas de fuite de données personnelles à relativement grande échelle, en cas de dommages économiques relativement importants, en cas de diffusion de données illégales à relativement grande échelle, ou en cas d'incidents de cybersécurité de ce type particulièrement graves, ou si des menaces à la cybersécurité particulièrement graves sont constatées, les départements en charge des activités de protection doivent, après en avoir été informés, les signaler au département national de la cybersécurité et de l'informatisation et au département en charge de la sécurité publique du Conseil des affaires de l'État.

[35] Décision n° 745 du Conseil des affaires de l'État de la République populaire de Chine, 30 juillet 2021, http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm?trs=1, traduite par DigiChina : https://digichina.stanford.edu/news/translation-critical-information-infrastructure-security-protection-regulations-effective-sept