Juillet 2023

– LÉGISLATION COMPARÉE –

NOTES

réalisées à la demande de la commission d'enquête sur l'utilisation du réseau social TikTok

———

- Le droit américain en matière de protection des données, de modération des contenus et de lutte contre la désinformation

- L'extraterritorialité du droit chinois

———

Ces notes ont été réalisées à la demande de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence dont le rapport est disponible sur le site du Sénat : https://www.senat.fr/notice-rapport/2022/r22-831-1-notice.html

DIRECTION DE L'INITIATIVE PARLEMENTAIRE ET DES DÉLÉGATIONS

LC 322

AVERTISSEMENT

Ce document constitue un instrument de travail élaboré à la demande des sénateurs, à partir de documents en langue originale, par la Division de la Législation comparée de la direction de l'initiative parlementaire et des délégations. Il a un caractère informatif et ne contient aucune prise de position susceptible d'engager le Sénat.

S O M M A I R E

Pages

À la demande de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence, la Division de la Législation comparée a réalisé deux notes :

– la première sur « *les aspects essentiels de la législation américaine en matière de protection des données, de modération et de lutte contre la désinformation* » ;

– la seconde sur « *les lois à portée extraterritoriale adoptées par la Chine, en particulier en matière de numérique, d'accès aux données, de modération et de (prétendue) lutte contre la désinformation* ».

LE DROIT AMÉRICAIN EN MATIÈRE DE PROTECTION DES DONNÉES, DE MODÉRATION DES CONTENUS ET DE LUTTE CONTRE LA DÉSINFORMATION

À la demande de la commission d'enquête du Sénat sur l'utilisation du réseau social TikTok, son exploitation des données, sa stratégie d'influence, la Division de la Législation comparée a réalisé une étude sur « *les aspects essentiels de la législation américaine en matière de protection des données, de modération et de lutte contre la désinformation* ».

La présente note présente un aperçu de la législation fédérale et des États - en particulier de la Californie - dans ce domaine, tout en faisant référence au cadre constitutionnel et, le cas échéant, à la jurisprudence récente.

1. La protection des données personnelles

La notion de « protection des données » (***data protection***) est récente en droit américain. Elle est généralement assimilée au concept anglo-saxon de « ***data privacy*** » qui peut être traduite par « données relatives à la vie privée » mais fait plus largement référence à la façon dont les informations personnelles[1] sont collectées, utilisées et partagées. Selon le service de recherche du Congrès des États-Unis, du point de vue législatif, le concept de *data protection* mêle les notions de *data privacy* et de *data security* (ce dernier concernant la façon les données personnelles sont protégées de l'accès ou de l'utilisation par des personnes non autorisées)[2]. La présente note retient cette définition de la protection des données.

a) L'absence de cadre juridique global au niveau fédéral

Aux États-Unis, ni le droit coutumier (*common law*), ni la Constitution ne fournissent un cadre suffisant pour protéger les individus et les consommateurs des nombreuses menaces potentielles qui pèsent sur leurs données dans l'espace numérique. Les normes les plus importantes en matière de protection des données relèvent de la loi, avec une multitude de textes législatifs aux niveaux fédéral et des États[3].

---

[1] *Le droit américain se réfère généralement au terme « informations » personnelles plutôt que « données ».*

[2] *Congressional Research Service (CRS), Data protection and Privacy Law: an Introduction, 2022, IF11207, p. 1.*

[3] *CRS, Data Protection Law : an Overview, 2019, R45631, p. 4.*

Influencé par un article de Louis Brandeis et Samuel Warren publié en 1890 dans la *Harward Law Review* et intitulé « *The Right to Privacy* », le **droit coutumier** de la plupart des États fédérés reconnaît quatre délits en matière de protection de la vie privée (« *privacy torts* ») : l'intrusion dans la vie privée, la divulgation publique de faits privés, l'appropriation du nom ou de l'image d'une personne et la publicité donnant une fausse image d'une personne. Cependant, ces délits se concentrent sur la divulgation publique d'informations privées, ce qui limite leur pertinence dans le cadre des débats actuels sur la protection des données, qui concernent essentiellement la façon dont les données sont collectées, protégées et utilisées[1].

Sur le **plan constitutionnel**, bien que la Cour suprême ait interprété la Constitution des États-Unis comme accordant aux individus un droit à la vie privée (*right to privacy*), ce droit protège généralement les individus uniquement contre les intrusions de l'État et non contre celles des acteurs privés[2]. Ainsi, en 1967, dans sa décision *Katz v. United States*[3], la Cour suprême a considéré que le Quatrième amendement[4], sans créer un « *droit général à la vie privée* », protégeait néanmoins « *les personnes, et non les lieux* » ainsi que la vie privée des individus contre certains types d'intrusion gouvernementale[5]. Ce principe a évolué au fil du temps et en est venu à protéger, dans une certaine mesure, l'intérêt des individus dans le cadre de leur vie privée numérique. Par exemple, dans l'affaire *Carpenter v. United States*[6] de 2018, la Cour suprême a conclu que la protection de la vie privée prévue par le Quatrième amendement s'étendait à la protection de certaines informations - comme l'enregistrement des déplacements physiques par un téléphone portable - contre l'intrusion de l'État, même lorsque ces informations étaient partagées avec un tiers[7]. Dans l'arrêt *Whalen v. Roe*[8] de 1977, la Cour suprême a également conclu que la garantie de liberté énoncée par le Quatorzième amendement impliquait l'existence d'un droit plus général à la vie privée, protégeant les individus contre l'intrusion de l'État, et ce même en dehors du contexte de perquisition et de saisie. Selon la Cour suprême, ce droit constitutionnel à la vie privée « implique en fait au moins deux types d'intérêts différents. L'un est l'intérêt individuel à éviter de divulguer des informations personnelles, et l'autre est l'intérêt de prendre en

---

[1] Ibid., *p. 7.*
[2] *CRS, Data protection and Privacy Law: an Introduction,* op. cit., *p. 1.*
[3] *389 U.S. 347 (1967).*
[4] *« Le droit des citoyens d'être garantis dans leur personne, leur domicile, leurs papiers et leurs effets contre les perquisitions et saisies non motivées ne sera pas violé et il ne sera émis aucun mandat si ce n'est sur présomption sérieuse, corroborée par serment ou déclaration solennelle et décrivant avec précision le lieu à perquisitionner et les personnes ou choses à saisir », https://www.state.gov/wp-content/uploads/2020/02/French-translation-U.S.-Bill-of-Rights.pdf*
[5] *CRS, Data Protection Law: an Overview,* op. cit., *p. 5.*
[6] *138 St. Ct. 2206 (2018).*
[7] *CRS, Data Protection Law: an Overview, op. cit., p. 5.*
[8] *429 U.S. 589 (1977).*

toute indépendance certains types de décisions importantes »[1] (en l'occurrence la décision de mettre fin à une grossesse). Cet intérêt, le droit d'éviter la divulgation d'informations personnelles est désormais connu sous le nom de droit à la confidentialité des informations (*informational privacy*)[2].

La portée de la jurisprudence constitutionnelle est cependant limitée par la **doctrine de l'action de l'État** (state action doctrine) selon laquelle seule l'action des autorités est soumise à un contrôle en vertu de la Constitution. En revanche, la conduite purement privée ne peut être interdite, « peu importe à quel point cette conduite peut être injuste »[3]. L'objectif de cette doctrine est de protéger les libertés individuelles en veillant à ce que l'action privée ne soit pas soumise à des limitations constitutionnelles. Le raisonnement de la Cour suprême est ainsi de «préserver un espace de liberté individuelle en limitant la portée de la loi fédérale et du pouvoir judiciaire fédéral»[4].

Compte tenu des limites inhérentes au droit coutumier et au droit constitutionnel, le Congrès a adopté un certain nombre de lois fédérales destinées à protéger les informations personnelles des individus. Contrairement au cadre juridique existant en Europe, les États-Unis ne disposent pas d'une seule loi couvrant l'ensemble des données personnelles, mais d'**un « *patchwork* » de lois fédérales** qui s'appliquent à certains secteurs ou à certaines données[5]. L'objectif, le périmètre, les moyens de mise en œuvre et les sanctions prévues diffèrent considérablement d'une loi à l'autre. Les lois fédérales jouant un rôle en matière de protection des données sont présentées de façon succincte ci-après, en commençant par celles dont le champ d'application est le plus étroit[6] :

- la **loi Gramm-Leach-Bliley** (*Gramm-Leach-Bliley Act, GBLA*) réglemente l'utilisation par les institutions financières des données personnelles non publiques (*nonpublic personal information, NPI*). Ces règles concernent essentiellement le partage des NPI avec des tiers, l'obligation de fournir des avis de communication de NPI au consommateur et la sécurisation des NPI contre les accès non autorisés ;

- la **loi sur la portabilité et la responsabilité de l'assurance maladie** (*Health Insurance Portability and Accountability Act, HIPAA*) encadre la collecte et la divulgation d'une catégorie de données de santé appelées « informations de santé protégées » (*protected health information*). Ces règles s'appliquent aux prestataires de soins et aux centres de soins de santé et aux entreprises associées ;

---

[1] Ibid. *at. 600.*
[2] *CRS, Data Protection Law: an Overview, op. cit., p. 6.*
[3] Ibid., *p.7.*
[4] *Lugar v. Edmondson Oil Co., 457 U.S. 922 (1982), dans: Ruben de Bruin, "A Comparative Analysis of the EU and U.S. Data Privacy Regimes and the Potential for Convergence, Hastings Science and Technology Law JournalHastings Science and Technology Law Journal, Volume 13, Number 2, Spring 2022.*
[5] *CRS, Data Protection Law: an Overview,* op. cit., *p. 7.*
[6] *CRS, Data Protection Law: an Overview,* op. cit., *pp. 8 et suivantes.*

- la **loi sur l'information équitable relative au crédit** (*Fair Credit Reporting Act, FCRA)* couvre la collecte et l'utilisation des informations de crédit des consommateurs et l'accès à leurs rapports de crédit ;

- la **loi sur les communications** (*Communications Act*), adoptée en 1934, prévoit des dispositions en matière de protection des données applicables aux entreprises de téléphonie et aux opérateurs du câble et du satellite ;

- la **loi sur la protection de la confidentialité en matière de vidéos** (*Video Privacy Protection Act*) assure la confidentialité des données liées à la location de vidéos et au *streaming* ;

- la **loi sur les droits de la famille relatifs à l'éducation et la protection de la vie privée** (*Family Educational Rights and Privacy Act, FERPA*) prévoit des règles concernant la protection et la divulgation des informations contenues dans les dossiers scolaires des élèves ;

- **les lois fédérales sur les valeurs mobilières** (*Federal Securities Laws*) exigent des contrôles en matière de sécurité des données et instaurent des obligations de signalement en cas de violation de la confidentialité des données ;

- la **loi sur la protection de la vie privée en ligne des enfants** (*Children's Online Privacy Protection Act, COPPA*) encadre la collecte en ligne et l'utilisation des informations personnelles des enfants. Cette loi s'applique à tout opérateur d'un site internet ou d'un service en ligne s'adressant aux enfants ou à tout opérateur qui a connaissance du fait qu'il collecte des données personnelles appartenant à des enfants. Elle interdit la collecte en ligne de données concernant des enfants de moins de 13 ans sans accord parental préalable. La Commission fédérale du commerce (*Federal Trade Commission*) est responsable de la mise en œuvre de ces dispositions ;

- la **loi sur la protection des communications électroniques** (*Electronic Communications Privacy Act, ECPA*) interdit l'accès ou l'interception non autorisés de données électroniques stockées ou en transit. « L'ECPA est peut-être la loi fédérale la plus complète sur la protection des données personnelles électroniques, car elle n'est pas spécifique à un secteur et bon nombre de ses dispositions s'appliquent à un large éventail d'acteurs privés et publics. Néanmoins, son impact sur les pratiques de confidentialité en ligne a été limité. Comme certains commentateurs l'ont observé, l'ECPA » a été conçue pour réglementer les écoutes téléphoniques et l'espionnage électronique plutôt que la collecte de données commerciales « , et les justiciables qui tentent d'appliquer l'ECPA à la collecte de données en ligne ont généralement échoué »[1] ;

[1] *CRS, Data Protection Law: an Overview,* op. cit.*, p. 25.*

- la **loi sur la fraude et les abus en matière informatique** (*Computer Fraud and Abuse Act*) interdit l'accès non autorisé (en particulier le *hacking*) à tout « ordinateur protégé » défini au sens large comme tout ordinateur connecté à Internet ;

- la **loi sur la protection financière des consommateurs** (*Consumer Financial Protection Act, CFPA*) réglemente les pratiques ou les actes trompeurs ou abusifs en rapport avec le consommateur de produits ou de services financiers. Le Bureau de protection financière des consommateurs (*Consumer Financial Protection Bureau, CFPB*) veille au respect de ses dispositions ;

- et, enfin, la **loi sur la Commission fédérale du commerce** (*Federal Trade Commission (FTC) Act*) interdit les actes ou les pratiques déloyaux ou trompeurs (*unfair or deceptive acts or practices, UDAPs*). Il s'agit d'une loi particulièrement importante en matière de protection des données car la FTC a utilisé son autorité en vertu de cette loi pour devenir **l'agence de référence en matière de protection de la vie privée**, comblant ainsi en partie les lacunes laissées par les lois fédérales susmentionnées[1].

La FTC a intenté des centaines d'actions en justice sur la base du motif selon lequel les pratiques des entreprises relatives aux données des consommateurs violaient l'interdiction d'actes ou de pratiques trompeurs ou déloyaux. Selon la FTC, les entreprises agissent de manière trompeuse lorsqu'elles traitent des informations personnelles d'une manière qui contredit leurs politiques de confidentialité ou d'autres déclarations publiées ou lorsqu'elles ne protègent pas de manière adéquate les informations personnelles contre tout accès non autorisé, malgré les promesses faites en ce sens. En plus des promesses non tenues, la FTC a soutenu que certaines pratiques de protection des données sont injustes, comme lorsque les entreprises ont des paramètres de confidentialité par défaut difficiles à modifier ou lorsque les entreprises appliquent rétroactivement des politiques de confidentialité révisées. Même si l'action de la FTC comble certaines lacunes de la loi fédérale, son autorité a des limites. Contrairement à de nombreuses lois sectorielles sur la protection des données, la loi sur la FTC n'oblige pas les entreprises à respecter des politiques ou des pratiques spécifiques en matière de protection des données et a toujours été interprétée comme n'affectant pas les entités n'ayant pas fait de promesses explicites concernant la protection des données. En août 2022, la FTC a ainsi publié une proposition de réglementation et une consultation publique sur l'opportunité de mettre en place des règles plus complètes en matière de protection des données[2].

[1] *CRS, Data Protection Law : an Overview,* op. cit., *p. 30.*
[2] *CRS, Data protection and Privacy Law: an Introduction,* op. cit., *p. 1.*

De plus, plusieurs projets de loi fédéraux proposant une approche globale en matière de protection des données personnelles ont été déposés devant le Congrès des États-Unis au cours des dernières années[1].

b) Le projet de loi fédérale sur la confidentialité et la protection des données (ADPPA)

Le **projet de loi fédérale sur la confidentialité et la protection des données** (***American Data Privacy and Protection Act***, **ADPPA**) est un texte bipartisan, présenté en 2022 par les députés Frank Pallone Jr. et Cathy McMorris Rogers[2], proposant un cadre juridique global en matière de protection des données au niveau fédéral. Des textes similaires ont été présentés par le passé mais il s'agit du seul ayant franchi l'étape d'un vote positif en commission[3] en juillet 2022, en vue d'un examen en plénière par la Chambre des représentants.

Ce projet de loi fixe des exigences sur la manière dont les entreprises et les organisations à but non lucratif, quelle que soit leur taille, traitent les données personnelles, qui comprennent des informations identifiant ou raisonnablement liées à un individu. Plus précisément, le projet de loi oblige la plupart des entreprises à limiter la collecte, le traitement et le transfert de données personnelles à ce qui est raisonnablement nécessaire pour fournir un produit ou un service demandé et à d'autres circonstances spécifiées. De manière générale, elle interdit également aux entreprises de transférer les données personnelles des individus sans leur consentement exprès et affirmatif. Le texte prévoit des droits pour les consommateurs, y compris le droit d'accéder, de corriger et de supprimer leurs données personnelles et oblige les entreprises à fournir aux particuliers un moyen de se retirer de la publicité ciblée. Le projet de loi prévoit également des protections supplémentaires pour les données personnelles des mineurs de moins de 17 ans, dont l'interdiction de la publicité ciblée. Ces protections supplémentaires ne s'appliqueraient que lorsque l'entité couverte sait que l'individu en question a moins de 17 ans, sauf pour les réseaux sociaux et les grands détenteurs de données qui sont réputés connaître l'âge d'un individu. Le projet de loi interdit en outre aux entreprises d'utiliser les données personnelles pour discriminer sur la base de caractéristiques protégées spécifiées. Les entreprises devraient mettre en œuvre des pratiques de sécurité pour protéger et sécuriser les données personnelles contre tout accès non autorisé, et la FTC pourrait émettre des règlements en la matière[4]. La FTC et les procureurs généraux des États seraient responsables de la mise en application de l'ADPPA.

---

[1] *Voir notamment : CRS, Overview of the American Data Privacy and Protection Act, H.R. 8152, LSB10776, 2022.*

[2] *https://www.congress.gov/bill/117th-congress/house-bill/8152/text*

[3] *Par la commission de l'énergie et du commerce. https://www.congress.gov/congressional-report/117th-congress/house-report/669/1*

[4] *https://www.congress.gov/bill/117th-congress/house-bill/8152*

L'ADPPA diffère des précédents projets de loi fédéraux en matière de protection des données sur trois questions, qui pourraient permettre de lever les obstacles auxquels se sont heurtés les textes précédents[1] :

- il prévoit l'introduction, dans les quatre ans suivant l'entrée en vigueur du projet de loi, d'un **droit d'action en justice** devant le juge civil pour les **particuliers** qui considéreraient que des dispositions du texte n'ont pas été respectées ;

- en règle générale, le projet de loi primerait sur toutes les lois des États. Cependant, il **préserverait seize catégories de lois des États**, y compris les lois sur la protection des consommateurs et les lois sur la notification des violations de la confidentialité des données. Le texte ne prévaudrait pas non plus sur certaines lois spécifiques des États fédérés, telles que la loi sur la confidentialité des informations biométriques et la loi sur la confidentialité des informations génétiques de l'Illinois et le droit d'action privée de la Californie pour les victimes de violations de données ;

- enfin, l'ADPPA ne prévoit pas de restriction générale sur l'engagement dans des pratiques « préjudiciables » (*harmful*) en matière de données vis-à-vis des utilisateurs finaux, contrairement au « devoir de loyauté » proposé dans des projets de loi au Sénat.

L'avenir de l'ADPPA demeure incertain à la suite du changement de majorité à la Chambre des représentants, contrôlée par le parti républicain depuis novembre 2022, et en raison des réticences de certains élus californiens, certains craignant que l'ADPPA garantisse une moindre protection par rapport à la loi californienne (cf. *infra*). Dans son discours sur l'état de l'Union de février 2023, le président des États-Unis, Joe Biden, a néanmoins rappelé qu'« *il* [était] *temps d'adopter une législation bipartite pour empêcher les* Big Tech *de collecter des données personnelles sur les enfants et les adolescents en ligne, d'interdire la publicité ciblée aux enfants et d'imposer des limites plus strictes aux données personnelles que ces entreprises collectent sur nous tous* »[2].

c) Les législations des États fédérés

Outre la mosaïque complexe de lois fédérales, de nombreux États ont développé leurs propres cadres législatifs en matière de protection des données. En particulier, tous les États ont adopté une forme de réponse législative en matière de fuite de données personnelles et de nombreux États ont des lois de protection des consommateurs qui couvrent en partie la protection des données personnelles[3].

---

[1] *CRS, Overview of the American Data Privacy and Protection Act, H.R. 8152,* op. cit., *p. 3.*
[2] *https://www.whitehouse.gov/briefing-room/speeches-remarks/2023/02/07/remarks-of-president-joe-biden-state-of-the-union-address-as-prepared-for-delivery/*
[3] *CRS, Data protection and Privacy Law: an Introduction,* op. cit., *p.1.*

De plus, au 9 juin 2023, neuf États américains[1] - contre seulement quatre en janvier de la même année[2] - avaient adopté un projet de loi instaurant un régime juridique complet en matière de protection des données personnelles[3] :

- en 2018, la Californie a été le premier État américain à adopter un cadre juridique global en matière de protection des données personnelles, proche du règlement général sur la protection des données (RGPD) européen, à travers le ***California Consumer Privacy Act*** (CCPA). Entré en vigueur en 2020, le CCPA a été par la suite amendé par le *California Privacy Rights Acts* (CPRA)[4].

Le CCPA couvre toute les entreprises qui collectent des données personnelles auprès de consommateurs californiens, au-delà de certains seuils de chiffre d'affaires annuel (25 millions de dollars, soit environ 23 millions d'euros) ou de nombres de consommateurs (100 000 ou plus) ou de revenus issus de la vente ou du partage des données (50 % ou plus). Les entreprises qui ne disposent pas d'adresse en Californie mais dont les sites internet sont accessibles depuis l'État sont également couvertes. Le CCPA accorde aux consommateurs trois principaux « droits » : premièrement, les consommateurs ont le droit de connaître les informations que les entreprises ont collectées ou vendues à leur sujet, ce qui oblige les entreprises à informer les consommateurs des données personnelles collectées (« *right to know* ») ; deuxièmement, le CCPA offre aux consommateurs le droit de refuser la vente de leurs informations personnelles (« *right to opt out* ») et, troisièmement, cette loi californienne donne aux consommateurs le droit, dans certains cas, de demander à une entreprise de supprimer toute information recueillie le concernant (« *right to delete* »). Les entreprises doivent également respecter les préférences des consommateurs en matière de *cookies*, définies par le biais des paramètres du navigateur (*Global Privacy Controls*), en donnant la priorité à ces paramètres par rapport à toute préférence conflictuelle déclarée par l'utilisateur. Depuis les amendements entrés en vigueur le 1er janvier 2023, le CCP distingue la catégorie des informations personnelles « sensibles » - comme les numéros de sécurité sociale, les coordonnées bancaires, les données précises de géolocalisation ou encore les données génétiques et biométriques - pour lesquelles les consommateurs disposent d'un droit de limiter l'utilisation et la divulgation (par exemple, le consommateur peut demander à une entreprise de limiter l'usage de certaines données personnelles sensibles uniquement à des fins de fourniture du service demandé)[5].

---

[1] *Californie, Colorado, Connecticut, Indiana, Iowa, Montana, Tennessee, Utah, Virginie.*
[2] *https://www.ncsl.org/technology-and-communication/2023-consumer-data-privacy-legislation*
[3] *https://iapp.org/resources/article/us-state-privacy-legislation-tracker/*
[4] *https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5*
[5] *https://www.cppa.ca.gov/faq.html#faq_res_1*

Le CCPA est appliqué par le biais des actions intentées par le procureur général de Californie, qui peut prononcer des amendes dont le montant peut aller jusqu'à 7 500 dollars (6 800 euros) par violation individuelle. En août 2022, le procureur général de Californie a ainsi constaté que l'entreprise Sephora n'avait pas respecté plusieurs dispositions du CCPA, notamment en procédant à la vente des informations personnelles de ses consommateurs sans leur autorisation. Ce litige s'est conclu par la négociation d'un accord prévoyant le versement d'une amende de 1,2 million de dollars (environ 1 million d'euros) par l'entreprise française de vente de cosmétiques. Par ailleurs, les particuliers disposent d'une voie de recours directe mais uniquement dans les cas où des informations personnelles non cryptées ou non expurgées des informations confidentielles ont fait l'objet d'un accès non autorisé, d'une exfiltration, d'un vol ou d'une divulgation[1].

Depuis 2020, la Californie dispose d'une agence pour la protection de la vie privée (*California Privacy Protection Agency*), composée de cinq experts et chargée de sensibiliser le public à leurs droits et les entreprises à leurs obligations, d'adopter des règlements de mise en œuvre du CCPA et, depuis le 1er juillet 2023, de faire appliquer la loi. Elle peut enquêter sur d'éventuelles violations, donner aux entreprises la possibilité de remédier à la situation et prendre des mesures d'exécution[2] ;

- d'autres États, comme la **Virginie**, l'**Utah**, le **Colorado** et le **Connecticut**, ont retenu une approche consistant à s'inspirer de projets de loi fédéraux en cours d'examen, dont l'ADPPA, pour leur propre législation. Contrairement à la Californie, ces quatre États ne prévoient ni obligation de notifier le consommateur au stade de la collecte, ni de droit de restreindre l'utilisation des données sensibles à certaines fins[3].

La plupart des législations récemment adoptées par les États autres que la Californie entreront en vigueur en 2023 ou dans les années à venir. De nombreux projets de loi concernant la protection des données sont en cours d'examen dans les États ne disposant pas encore de cadre juridique global.

2. La modération des réseaux sociaux et la lutte contre la désinformation

Aux États-Unis, la modération des contenus sur les réseaux sociaux et la lutte contre la désinformation reposent essentiellement sur l'autorégulation des acteurs privés. Le droit américain accorde en effet une place prééminente à la liberté d'expression, y compris sur Internet. Les deux principales dispositions relatives à la liberté d'expression en ligne sont :

---

[1] *CRS, Data Protection Law: an Overview,* op. cit.*, p. 30.*
[2] *https://www.cppa.ca.gov/faq.html#faq_res_1*
[3] *https://iapp.org/resources/article/us-state-privacy-laws-overview/*

- le **Premier amendement de la Constitution** des États-Unis, en vertu duquel « ***Le Congrès ne fera aucune loi*** *qui touche l'établissement ou interdise le libre exercice d'une religion, ni* ***qui restreigne la liberté de parole ou de la presse*** »[1]. La Cour suprême applique depuis longtemps cette disposition au-delà du pouvoir législatif pour empêcher les actions des autres organes de l'État fédéral ainsi que celles des États fédérés. Ainsi, le Premier amendement limite la capacité du gouvernement à restreindre les discours mais il ne limite pas les actions des parties privées[2], tels que les fournisseurs de réseaux sociaux qui peuvent, en principe, adopter leurs propres politiques de contenu et codes de conduite ;

- l'**article 230**, titre 47, du Code des États-Unis[3], tel que modifié par la loi de 1996 sur la décence des communications (***Communications Decency Act***). En particulier, l'article 230, paragraphe (c), alinéa 1 exonère les fournisseurs et les utilisateurs de réseaux sociaux de toute responsabilité concernant la publication d'informations fournies par des utilisateurs tiers : « *aucun fournisseur ou utilisateur d'un service informatique interactif ne doit être considéré comme l'éditeur ou le locuteur d'une information fournie par un autre fournisseur de contenu d'information* »[4]. L'alinéa 2 de ce même article prévoit qu'« *aucun fournisseur ou utilisateur d'un service informatique interactif ne peut être tenu pour responsable du fait de (a) toute mesure prise volontairement et de bonne foi pour restreindre l'accès ou la disponibilité de matériel que le fournisseur ou l'utilisateur considère comme obscène, lubrique, lascif, répugnant, excessivement violent, harcelant ou autrement répréhensible, que ce matériel soit ou non protégé par la Constitution ou (b) toute mesure prise pour permettre aux fournisseurs de contenu d'information ou à d'autres de disposer des moyens techniques nécessaires pour restreindre l'accès au matériel décrit* »[5] au paragraphe précédent.

Un grand nombre d'**actions en justice** ont été introduites à l'encontre des fournisseurs de réseaux sociaux, au sujet de leur politique de modération des contenus, la plupart leur reprochant une censure infondée et d'autres l'absence de retraits de contenus dangereux. Ainsi, de nombreux requérants ont soutenu que la politique de modération des contenus des plateformes privées contrevenait à leur liberté d'expression, au regard du Premier amendement. Dans l'immense majorité des cas, les juridictions de première instance ont rejeté ces recours en invoquant soit l'article 230 précité, qui prévoit une protection spécifique pour les fournisseurs de contenu en ligne, soit le Premier amendement, en précisant que ce dernier ne s'applique pas aux réseaux sociaux en tant qu'acteurs privés opérant indépendamment de l'État[6]. À titre d'illustration, le 6 mai 2022, le juge de la cour de district fédéral de Californie a rejeté le recours de l'ancien président

---

[1] *https://www.state.gov/wp-content/uploads/2020/02/French-translation-U.S.-Bill-of-Rights.pdf*
[2] *CRS, Online content moderation and government coercion, LSB10742, 2022, p. 1.*
[3] *U.S. Code Title 47, section 230.*
[4] *U.S. Code Title 47, section 230 (c) (1).*
[5] *U.S. Code Title 47, section 230 (c) (2).*
[6] *CRS, Online content moderation and government coercion*, op. cit., *p. 3.*

des États-Unis, Donald Trump, à l'encontre de Twitter qui avançait le motif selon lequel le réseau social aurait enfreint ses droits au titre du Premier amendement en l'excluant de Twitter[1].

En mai 2023, la Cour suprême s'est également prononcée dans deux affaires, ***Twitter v. Taamneh***[2] et ***Gonzalez v. Google***[3], dans lesquelles les plaignants, des familles de victimes de l'organisation terroriste État islamique, ont fait valoir que les algorithmes qui recommandent des contenus sur Twitter, Facebook et YouTube avaient aidé et encouragé le groupe terroriste en promouvant activement son contenu auprès des utilisateurs. Dans les deux cas, la Cour suprême a refusé de tenir pour responsables les réseaux sociaux des contenus postés par leurs utilisateurs. Dans l'affaire *Twitter v. Taamneh*, la Cour suprême a rejeté le recours des plaignants au titre de l'article 2333 (d) (2) du Code des États-Unis[4] en concluant que « *les plaignants n'ont pas réussi à prouver que les défendeurs ont intentionnellement fourni une aide substantielle à l'attentat du Reina* [à Istanbul] *ou ont participé consciemment à l'attentat du Reina, et encore moins que les défendeurs ont aidé l'État islamique d'une manière si généralisée et systémique qu'elle les rende responsables de chaque attentat de l'État islamique* »[5].

L'affaire *Gonzalez v. Google* concernait quant à elle le champ d'application de l'article 230 et plus précisément la question de savoir si cet article protège ou non les réseaux sociaux comme YouTube des poursuites judiciaires concernant des vidéos faisant l'apologie du terrorisme. Les juges de la Cour suprême n'ont pas tranché cette question et ont conclu : « *Nous n'avons pas à nous prononcer sur la viabilité des revendications des plaignants dans leur ensemble ou sur la question de savoir si les plaignants devraient être autorisés à modifier leur requête. Nous pensons plutôt qu'il est suffisant de reconnaître que la majeure partie (sinon la totalité) de la plainte semble échouer en vertu de notre décision dans l'affaire Twitter ou des décisions non contestées de la Cour d'appel du neuvième circuit. Nous* ***refusons donc d'aborder l'application de l'article 230*** *à une plainte qui semble présenter peu, voire pas du tout, de demande de réparation plausible* »[6].

La Cour suprême a précisé que « *les deux affaires ont été soumises à la Cour au stade de la requête en irrecevabilité (*motion-to-dismiss*), sans dossier factuel. Et l'opinion de la Cour sur les faits, y compris sa caractérisation des plateformes de réseaux sociaux et des algorithmes en cause, repose à juste titre sur*

---

[1] *https://www.washingtonpost.com/technology/2022/05/06/trump-twitter-lawsuit-dismissed/*
[2] *598 U. S., No. 21–1496.*
[3] *598 U. S., No. 21–1333.*
[4] *Selon cet article* « Tout ressortissant des États-Unis blessé dans sa personne, ses biens ou son entreprise en raison d'un acte de terrorisme international, ou sa succession, ses survivants ou ses héritiers, peut intenter une action en justice devant tout tribunal de district approprié des États-Unis et recouvrer le triple des dommages qu'il a subis et des frais de justice, y compris les honoraires d'avocat ».
[5] *598 U. S., No. 21–1496, p. 38.*
[6] *598 U. S., No. 21–1333, p. 3.*

les allégations particulières contenues dans ces plaintes. D'autres affaires présentant des allégations et des dossiers différents pourraient conduire à des conclusions différentes »[1]. Selon la presse américaine, ces deux affaires représentent néanmoins une victoire pour les entreprises du secteur numérique et illustrent la difficulté d'amender l'article 230[2], en dépit de la mobilisation d'un nombre croissant de membres du Congrès pour modifier la loi fédérale et renforcer la responsabilité des plateformes en ligne.

Enfin, concernant spécifiquement la **lutte contre la désinformation**, il convient de relever la création en avril 2022 par le président des États-Unis, Joe Biden, d'un « **conseil de gouvernance relatif à la désinformation** » (*Disinformation Governance Board, DGB*), en tant que comité consultatif auprès du ministère américain de la sécurité intérieure (*Department of Homeland Security*). L'objectif de cet organe était de suivre les campagnes de désinformation diffusées par des États étrangers tels que la Russie, la Chine et l'Iran et par des organisations criminelles transnationales et de trafic d'êtres humains, ainsi que la désinformation diffusée lors de catastrophes naturelles (par exemple, sur la sécurité de l'eau potable lors de l'ouragan Sandy) et de diffuser les bonnes pratiques de lutte contre ces campagnes auprès des services du DHS chargés de défendre le pays contre ces menaces[3]. Dès mai 2022, l'activité du DGB a été suspendue, puis définitivement interrompue[4], à la suite de polémiques et d'attaques de sa responsable sur les réseaux sociaux[5].

---

[1] *598 U. S., No. 21–1496, p. 38.*
[2] *Voir notamment : https://www.washingtonpost.com/technology/2023/05/18/scotus-social-media-analysis/ et https://www.nytimes.com/2023/05/18/us/politics/supreme-court-google-twitter-230.html*
[3] *https://www.dhs.gov/news/2022/05/02/fact-sheet-dhs-internal-working-group-protects-free-speech-other-fundamental-rights*
[4] *https://www.dhs.gov/news/2022/08/24/following-hsac-recommendation-dhs-terminates-disinformation-governance-board*
[5] *https://www.washingtonpost.com/technology/2022/05/18/disinformation-board-dhs-nina-jankowicz/*

L'EXTRATERRITORIALITÉ DU DROIT CHINOIS

1. La notion d'extraterritorialité en droit international

L'extraterritorialité peut être définie, de façon large, comme « *la situation dans laquelle les compétences d'un État (législatives, exécutives ou juridictionnelle) régissent des rapports de droit situés en dehors du territoire dudit État* »[1] ou « *le fait pour l'État d'appréhender à travers son ordre juridique des situations extérieures à son territoire* »[2].

Le système international issu des traités de Westphalie de 1648 établit la souveraineté nationale et l'intégrité territoriale comme principes suprêmes du droit international, faisant ainsi de la territorialité un pilier fondamental du droit international. Dans l'affaire du Lotus, en 1927, la Cour permanente de justice internationale a retenu qu'un État peut exercer sa compétence normative ou juridictionnelle à des personnes, des biens et des actes en dehors de son territoire, dès lors qu'il existe un fondement. En revanche, l'arrêt Lotus interdit à tout État « *l'exercice de sa puissance sur le territoire d'un autre État* »[3], sauf règle de droit international contraire. « *En d'autres termes, seul le pouvoir de coercition de l'État ne peut s'exercer sur le territoire d'un autre État. Un État peut cependant légitimement adresser ses normes et prescriptions à ses nationaux et même aux étrangers hors de son territoire, sous réserve de l'existence d'un lien de rattachement suffisant entre la situation donnée et cet État* »[4]. La présente note se concentre sur l'extraterritorialité en tant que compétence normative ou juridictionnelle et non sur l'exécution extraterritoriale de la loi.

2. Quelques caractéristiques du droit chinois

En Chine, pays de droit continental, les textes législatifs sont la source principale du droit. La hiérarchie des normes juridiques, clarifiée par la loi de 2000 sur la législation, suit l'ordre suivant : « *la Constitution en premier lieu, puis les lois - y compris les lois fondamentales adoptées par l'Assemblée populaire nationale et les lois adoptées par son Comité permanent -, les règlements administratifs […], les règlements locaux […], enfin les décrets*

---

[1] *J. Salmon (dir.), Dictionnaire de droit international public, 2001, article « Extraterritorialité », p. 491.*
[2] *B. Stern, « Quelques observations sur les règles internationales relatives à l'application extraterritoriale du droit », Annuaire français de droit international, vol. 32, 1986, p. 10.*
[3] *CPJI, 4 janvier 1927, Lotus (France contre Turquie), Série A, N°10*
[4] *Laurent Cohen-Tanugi, Droits sans frontières : géopolitique de l'extraterritorialité, 2023, p. 18.*

ministériels et les actes des gouvernements locaux »[1]. En 2021, on comptait 288 lois et environ 800 règlements[2] ; le code civil chinois est entré en vigueur cette même année. Il convient de noter que la Cour populaire suprême et le Parquet populaire suprême - les deux institutions judiciaires suprêmes chinoises - ont un pouvoir important d'interprétation de la loi. En effet, « *l'interprétation judiciaire est une originalité chinoise. […] Née du besoin de juger les affaires en appliquant les lois qui étaient souvent trop générales ou vagues, l'interprétation judiciaire, dont l'importance s'accroît considérablement, sert effectivement de véritable source de droit et joue un rôle indispensable tant pour comprendre le droit chinois que pour le mettre en œuvre à l'occasion d'un litige.* »[3].

Par ailleurs, le droit chinois se caractérise par un certain pragmatisme, étroitement lié à la pensée traditionnelle chinoise. « *D'où une « propension à la flexibilité », l'application rigide d'une norme à des réalités diverses ne pouvant conduire qu'au « désordre ». L'approche du droit est donc tout sauf dogmatique : bien au contraire, elle est au plus près de la réalité concrète, des besoins, des circonstances, aucune vérité n'étant établie à l'avance* »[4].

Enfin, si la réforme judiciaire de 2014 a permis d'affirmer l'objectif de garantir l'impartialité et l'indépendance des cours et des parquets[5], la Constitution ne prévoit pas de principe de séparation des pouvoirs[6] et son préambule affirme le rôle prépondérant du Parti communiste chinois (PCC) et du marxisme-léninisme pour diriger et guider « *les différentes nationalités de Chine* »[7].

3. Les lois chinoises à portée extraterritoriale dans le domaine du numérique et de la protection des données

a) Aperçu général

En 2019, à l'issue de la deuxième session de la commission pour la gouvernance globale fondée sur le droit du PCC, ce dernier affirmait son ambition d'établir un système juridique d'application extraterritoriale (« [le pays] *devrait s'efforcer d'accélérer la construction d'un système juridique d'application extraterritoriale de notre droit national* »)[8]. Depuis, cette ambition a été réaffirmée à plusieurs reprises, notamment en 2022, lors d'une conférence sur « *les réalisations de la Chine en matière de promotion de l'État de droit dans la nouvelle ère* », organisée par le comité central du PCC[9].

---

[1] *Marie Goré et Ai-Qing Zheng, Le droit chinois, « Que sais-je ? », 2022, p. 27.*
[2] Ibid., *p. 15.*
[3] Ibid., *pp. 28-29.*
[4] Ibid., *p. 12.*
[5] Ibid., *p. 22.*
[6] *Selon l'article 2 de la Constitution chinoise, « Tout le pouvoir de la République populaire de Chine appartient au peuple ».*
[7] *Marie Goré et Ai-Qing Zheng,* op.cit., *p.7.*
[8] *Zhengxin Huo et Man Yip, « Extraterritoriality of Chinese Law: Myths, Realities and the Future", The Chinese Journal of Comparative Law, 2021, Vol. 9, No. 3, p. 330.*
[9] *http://english.scio.gov.cn/pressroom/2022-08/12/content_78369101.htm*

Bien que contestant régulièrement la pratique des États-Unis de la « juridiction étendue » (*long-arm jurisdiction*), la Chine a décidé de construire son propre système juridique d'extraterritorialité[1]. Si elle n'a pas encore mis en place un tel système juridique complet, il existe de nombreuses lois chinoises prévoyant des règles d'extraterritorialité fondées, selon les cas, sur des principes différents (principe de personnalité, principe de protection de la souveraineté de l'État, principe de compétence universelle et théorie des effets)[2]. Sans prétendre à l'exhaustivité, on peut citer, sur la base de l'inventaire réalisé par les professeurs Zhengxin Huo et Man Yip et des propres recherches de la division :

- en **matière pénale**, le code pénal[3] (articles 7 à 9) et la loi de 2020 sur la sécurité nationale de Hong Kong (article 37), qui se fondent notamment sur le principe de personnalité selon lequel un État a le droit d'exercer sa compétence sur ses ressortissants, même s'ils se trouvent en dehors de son territoire ;

- en **matière fiscale**, la loi sur l'impôt sur le revenu des personnes physiques (article 1) et la loi sur l'impôt sur le chiffre d'affaires des entreprises, dernièrement amendées en 2018 (principe de personnalité) ;

- en matière **économique et financière**, la loi de 2007 de lutte contre les monopoles (article 2), dernièrement amendée en 2022, la loi de 2008 sur les valeurs mobilières, telle que modifiée en 2019 (article 2) et la loi de 2022 sur les contrats à terme et les produits dérivés (article 2). Les projets de révision de la loi de 2007 sur les banques commerciales et de la loi de 2004 sur la supervision bancaire (article 47) prévoient des dispositions analogues relatives à la compétence extraterritoriale[4]. Dans tous ces cas, l'extraterritorialité se fonde sur la théorie des effets, selon laquelle un État peut exercer sa compétence sur des actes commis à l'étranger par des personnes étrangères lorsque ces actes ont des effets sur le territoire de l'État régulateur[5] ;

- en matière de **sécurité nationale**, la loi de 2014 de lutte contre l'espionnage (article 27) dernièrement amendée en 2023, la loi antiterroriste de 2015 (article 11), la loi de 2016 sur la cybersécurité (article 75) et la loi de 2017 sur le renseignement national (articles 7 et 10). Les dispositions extraterritoriales de ces textes sont fondées sur le principe de protection, en vue de prémunir l'État contre des actes perpétrés à l'étranger qui pourraient menacer sa souveraineté ou son indépendance politique ;

---

[1] *Zhengxin Huo et Man Yip,* op. cit., *pP. 329-330.*
[2] Ibid., *p. 336.*
[3] *http://www.npc.gov.cn/zgrdw/englishnpc/Law/2007-12/13/content_1384075.htm*
[4] *https://www.hankunlaw.com/en/portal/article/index/cid/8/id/12577*
[5] *Laurent Cohen-Tanugi,* op. cit., *pp. 18-19.*

- en matière de **protection des données** et de **numérique**, la loi de 2021 sur la sécurité des données (article 2) et la loi de 2021 sur la protection des données personnelles (PIPL[1], article 2). Le projet de mesures administratives visant à réguler les services d'intelligence artificielle générative, publié en avril 2023 par l'administration du cyberespace de Chine (CAC), a également une portée extraterritoriale dans la mesure où il s'appliquerait à tout fournisseur de service en Chine, y compris aux entreprises étrangères[2].

Les textes pouvant présenter un intérêt spécifique pour les travaux de la commission d'enquête - c'est-à-dire, d'une part, les trois textes formant le cadre juridique de la protection des données en Chine (loi sur la cybersécurité, loi sur la sécurité des données et PIPL) et, d'autre part, les lois sur le renseignement et la lutte contre l'espionnage, sont présentés plus en détail ci-après.

b) Le cadre juridique de la protection des données

La **loi sur la cybersécurité**, adoptée en 2016 par le Comité permanent de l'Assemblée populaire nationale et entrée en vigueur le 1er juin 2017, traite principalement de la sécurité des réseaux et des informations numériques. Avant l'adoption, en 2021, de la loi sur la sécurité des données et de la loi sur la protection des données personnelles (PIPL), il s'agissait du seul texte législatif régissant le traitement des données[3]. Cette loi marque, en outre, une étape importante dans le développement de l'extraterritorialité du droit chinois : « *Une innovation frappante de la loi sur la cybersécurité est la prescription de l'extraterritorialité, qui ne figure pas dans les règles précédentes.* […] *Elle intègre non seulement la compétence normative sur les actes extraterritoriaux énumérés, mais elle énonce également les sanctions juridiques concrètes visant à garantir l'extraterritorialité dans la pratique. Il s'agit d'une étape importante dans l'histoire législative chinoise : c'est la première règle sur l'extraterritorialité qui a été dotée de « dents » pour en renforcer l'applicabilité ; il ne s'agit pas d'un simple tigre de papier* »[4]. L'article 75 de la loi sur la cybersécurité, tel que traduit dans le cadre du projet de recherche de l'université de Stanford « Digichina » prévoit en effet que : « *Lorsque des institutions, des organisations ou des individus étrangers se livrent à des attaques, des intrusions, des interférences, des dommages ou d'autres activités qui mettent en danger l'infrastructure d'information critique de la République populaire de Chine et entraînent de graves conséquences, la responsabilité légale doit être recherchée conformément à la loi ; les départements de la sécurité publique relevant du Conseil d'État et les départements concernés peuvent également décider de geler les avoirs des institutions, des organisations ou des individus ou de prendre d'autres mesures punitives nécessaires* »[5].

---

[1] *Couramment dénommée en anglais* Personal Information Protection Act *(PIPL).*
[2] *http://www.cac.gov.cn/2023-04/11/c_1682854275475410.htm*
[3] *https://www.dataguidance.com/opinion/china-interplay-between-pipl-dsl-and-csl*
[4] *Zhengxin Huo et Man Yip,* op. cit.*, pp. 339-340.*
[5] *https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/*

La **loi sur la sécurité des données** a été adoptée en juin 2021 par le Comité permanent de l'Assemblée populaire de Chine et est entrée en vigueur le 1er septembre 2021. Elle concerne l'ensemble des traitements (collecte, stockage, utilisation, transmission…) de données, personnelles ou non, et instaure deux catégories de données sensibles : les « données nationales essentielles » (*national core data*) et les « données importantes » (*important data*). Les données nationales essentielles sont définies à l'article 21 comme des données concernant la sécurité nationale, les intérêts économiques, le bien-être des citoyens chinois ou l'intérêt public, et sont considérées comme le type de données le plus sensible. Les données importantes sont classées au deuxième rang des données les plus sensibles, mais ne sont pas clairement définies dans le texte[1]. Des amendes de maximum 10 millions de yuans (1,3 million d'euros) et la révocation du permis d'exploitation peuvent être prononcées à l'égard des organisations ou personnes ne respectant pas les règles de traitement des données nationales essentielles (article 45). De plus, quiconque fournit des données importantes à l'étranger peut se voir ordonner de procéder à des rectifications et infliger une amende pouvant s'élever jusqu'à 10 millions de yuans si les circonstances sont graves (article 46). Une compétence extraterritoriale est prévue, sur la base du principe de protection. Selon l'article 2 de cette loi, traduite en anglais par les autorités chinoises, « *La présente loi s'applique aux activités de traitement des données ainsi qu'à la supervision et à la réglementation de la sécurité de ces activités sur le territoire de la République populaire de Chine. Lorsque le traitement de données* ***en dehors du territoire*** *de la République populaire de Chine porte atteinte à la sécurité nationale, aux intérêts publics ou aux droits et intérêts légitimes de personnes ou d'organisations de la République populaire de Chine, la responsabilité juridique sera examinée conformément à la loi* »[2].

La **loi sur la protection des données personnelles** (PIPL), adoptée en août 2021 et entrée en vigueur le 1er novembre 2021, est considérée comme l'équivalent du règlement général sur la protection des données (RGPD) de l'Union européenne. La PIPL couvre toutes les activités liées aux données personnelles des résidents chinois, qu'elles soient collectées en Chine ou à l'étranger. Selon la traduction officielle, l'article 3 indique en effet : « *La présente loi s'applique au traitement des données à caractère personnel des personnes physiques sur le territoire de la République populaire de Chine. La présente loi s'applique également au traitement,* ***en dehors du territoire*** *de la République populaire de Chine, d'informations à caractère personnel concernant des personnes physiques se trouvant sur le territoire de la République populaire de Chine, dans l'une des circonstances suivantes : (1) dans le but de fournir des produits ou des services à des personnes physiques sur le territoire de la République populaire de Chine ; (2) pour analyser ou évaluer le comportement de personnes physiques sur le territoire de la République populaire de Chine ; et (3) toute autre*

[1] *https://foreignpolicy.com/2022/01/28/china-data-governance-security-law-privacy/*
[2] *http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml*

circonstance prévue par une loi ou un règlement administratif »[1]. Comme le RGPD, la PIPL introduit le droit de limiter ou de refuser le traitement des données à caractère personnel et l'exigence d'obtenir un consentement explicite avant de transférer les données personnelles à des tiers (articles 13 et 14). Le texte s'applique à la collecte de données par les entreprises privées et publiques et comprend des dispositions obligeant les agences gouvernementales chinoises à informer les individus et à obtenir leur consentement. Cependant, une dérogation est prévue en cas de traitement « *dans l'intérêt public* » (article 13 (15)).

c) Les lois sur le renseignement et sur la lutte contre l'espionnage

La **loi sur le renseignement national**, adoptée en 2017 et modifiée en 2018[2], codifie la pratique existante en matière de renseignement, établit une distinction entre les fonctions du renseignement civil et du renseignement militaire et des principes juridiques pour le fonctionnement des agences de sécurité de l'État, sans précisément les nommer ni définir la notion de « renseignement »[3]. En son article 7, elle énonce le devoir, pour les citoyens et les entreprises, de coopérer avec les agences de renseignement et de sécurité de l'État : « *Toutes les organisations et tous les citoyens doivent soutenir, assister et coopérer aux efforts des services de renseignement nationaux conformément à la loi, et protéger les secrets des services de renseignement nationaux dont ils ont connaissance* ». L'article 10 donne une portée extraterritoriale à cette loi : « *Dans la mesure où cela est nécessaire à leur travail, les services nationaux de renseignement doivent utiliser les moyens, les tactiques et les canaux nécessaires pour mener à bien leurs activités de renseignement, tant à l'intérieur qu'à l'extérieur du pays* ». La combinaison des articles 7 et 10 peut ainsi faire craindre que des données personnelles appartenant à des citoyens étrangers et détenues par des entreprises chinoises soient transmises aux services de renseignement chinois[4].

En avril 2023, le Comité permanent de l'Assemblée populaire de Chine a modifié la **loi de 2014 de lutte contre l'espionnage**, prévoyant non seulement une extension du périmètre des activités considérées comme des « activités d'espionnage » ainsi qu'une extension extraterritoriale de son champ d'application[5]. Aux termes de l'article 4, « *Cette loi s'applique aux organisations d'espionnage et à leurs agents sur le territoire de la République populaire de Chine, ou en profitant des citoyens, des organisations ou d'autres conditions de la République populaire de Chine pour se livrer à des activités d'espionnage contre un pays tiers, mettant en danger la sécurité nationale de la*

[1] *http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm*
[2] *http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml. Contrairement à de nombreuses autres lois, les autorités chinoises n'ont publié aucune traduction officielle de ce texte en anglais.*
[3] *https://www.canada.ca/en/security-intelligence-service/corporate/publications/china-and-the-age-of-strategic-rivalry/chinas-intelligence-law-and-the-countrys-future-intelligence-competitions.html*
[4] *https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense*
[5] *https://www.jdsupra.com/legalnews/china-s-new-anti-espionage-law-raises-2116858/*

République populaire de Chine »[1]. L'article 8 prévoit également que « *Tous les citoyens et toutes les organisations ont l'obligation de soutenir et d'aider légalement les efforts de contre-espionnage et doivent préserver les secrets des services de contre-espionnage dont ils ont connaissance* »[2].

4. Les incertitudes entourant la portée réelle de l'extraterritorialité dans le domaine du numérique et des données

Hormis en matière de politique de la concurrence où les agences gouvernementales chinoises jouent un rôle très actif dans la mise en œuvre des dispositions extraterritoriales, la portée réelle de l'extraterritorialité des lois sur la protection des données, le renseignement et l'espionnage demeure floue.

Un recensement de la jurisprudence effectué en juin 2020 indiquait que, tous domaines confondus, le nombre d'affaires dans lesquelles les juridictions chinoises avaient conclu à la compétence extraterritoriale était très faible et qu'aucun de ces cas ne se fondait sur le principe de protection[3]. « *En général, les tribunaux chinois sont réticents à reconnaître l'extraterritorialité du droit national* »[4].

[1] *http://www.npc.gov.cn/npc/c30834/202304/a386e8ffa3d94047ab2f0d89b1ea73c4.shtml*
[2] Ibid.
[3] *Zhengxin Huo et Man Yip,* op. cit., *p. 341*
[4] Ibid.