DS NEWSLETTER savoir faire
NEWSLETTER – INFORMATIONS JURIDIQUES PROPOSÉES PAR LE CABINET DS AVOCATS

Aperçu des nouveautés juridiques sur la protection des données et la cybersécurité en 2021

ASIE

2021 est une grande année pour la protection des données et la cybersécurité, et constitue notamment une étape importante pour la protection des informations personnelles ("IP"). Outre *la célèbre Loi sur la sécurité des données* ("DSL") et la *Loi sur la protection des informations personnelles* ("PIPL"), il existe également d'autres réglementations et directives déjà promulguées ou en projet, qui peuvent dans une certaine mesure affecter les activités des entreprises en Chine. Quelle tendance se dégage de cette année 2021 ?

CYBERSECURITÉ

- *La loi sur la cybersécurité* ("CSL", entrée en vigueur en 2017) fixe les obligations de base (le système de protection à plusieurs niveaux (Multi-Level Protection Scheme, "MLPS") pour les opérateurs de réseaux, mais elle ne donne aucun détail sur la façon de gérer les incidents. Face à la multiplication des cyberincidents et des fraudes, il était urgent d'adopter une réglementation sur le sujet. Le 12 juillet 2021, l*es Dispositions administratives sur les vulnérabilités de sécurité dans les équipements de réseaux* ont été promulguées et sont entrées en vigueur le 1er septembre 2021.

  Elles réglementent les fournisseurs d'équipements de réseaux (matériel et logiciel), les opérateurs de réseaux et d'autres entités (organisations, individus). Lorsqu'une faille est découverte, l'entreprise concernée doit l'examiner, la signaler aux autorités compétentes dans les deux jours, prendre immédiatement des mesures correctives et en informer les parties concernées qui pourraient être affectées. Les registres concernant les failles découvertes doivent être conservés pendant au moins 6 mois, ce qui est conforme à l'une des obligations fondamentales fixées par la CSL concernant les registres de réseaux. Il est à noter que la violation peut entraîner une sanction administrative sévère (amende pour l'entreprise et parfois aussi pour la personne responsable, révocation de la licence d'exploitation, etc.) selon la CSL.

- D'après la CSL, les opérateurs d'infrastructures d'information critiques (*critical information infrastructure operators*, "CIIO") ont des obligations plus nombreuses et plus strictes en matière de cybersécurité et de gestion des données que les opérateurs de réseaux normaux. Cependant, la CSL reste vague sur la plupart des obligations des CIIO. Depuis le 1er septembre 2021, *le Règlement sur la protection de la sécurité des infrastructures d'information critiques* est entré en vigueur. Il résout, dans une certaine mesure, le manque de clarté des obligations des CIIO et prévoit des sanctions administratives supplémentaires en plus de celles déjà incluses dans la CSL pour les CIIO.

  Bien qu'en pratique, il soit moins probable que les entreprises à capitaux étrangers soient considérées comme des CIIO, elles peuvent coopérer commercialement avec certains CIIO qui auront ou ont déjà des exigences plus strictes pour leurs fournisseurs par le biais d'un audit ou pour leurs clients par le biais du processus KYC (Know Your Client). Il est donc conseillé aux entreprises à capitaux étrangers de vérifier leur niveau de conformité en matière de cybersécurité, en particulier le statut de conformité MLPS, qui est obligatoire pour tous les opérateurs de réseaux et plus fréquemment contrôlé par les autorités en pratique.

GESTION DES DONNÉES ET PROTECTION DES INFORMATIONS PERSONNELLES

La Chine a publié sa première loi régissant la sécurité des données et sa première loi régissant la protection des informations personnelles, à savoir la DSL (en vigueur le 1er septembre 2021) et la PIPL (en vigueur le 1er novembre 2021). Ces lois ont un effet juridique extraterritorial et ont un impact sur les opérations quotidiennes de la plupart des multinationales qui ont des filiales en Chine.

Actuellement, la DSL et la PIPL sont trop générales pour guider les entreprises dans leurs projets de mise en conformité. Toutefois, en 2022, il y aura

davantage de règlements, de lignes directrices et d'instructions pour préciser certains points peu clairs. Par exemple, les deux projets suivants, publiés en octobre et novembre 2021, apportent un éclairage sur le transfert transfrontalier de données.

- *Règlement sur la gestion de la sécurité des données en réseau (Projet)*

  Selon le Projet actuel, les entreprises qui sont responsables de traitement de données doivent remplir leurs obligations en matière de documentation (rendre le flux de données traçable en conservant des registres), procéder à une auto-évaluation dans des scénarios tels que les incidents liés aux données, le traitement des données sensibles, le profilage, le transfert de données vers des pays tiers, etc.

  En ce qui concerne la protection des données personnelles, les parties suivantes du projet attirent l'attention :

  - les entreprises qui traitent les données personnelles de plus d'un million de personnes doivent passer un examen de cybersécurité (qui est plus complet qu'une évaluation de la sécurité) mené par les autorités compétentes avant de lancer tout projet d'introduction en bourse à l'étranger.
  - les droits des personnes concernées sont assortis de délais et de restrictions. Par exemple, les responsables de traitement de données doivent répondre aux demandes des personnes concernées dans un délai de quelques jours et la fréquence des demandes doit être raisonnable, sinon les responsables de traitement peuvent facturer des frais aux personnes concernées.
  - en ce qui concerne le sujet brûlant du transfert de données personnelles vers l'étranger, le Projet précise les seuils déclencheur de l'évaluation de sécurité organisée par l'Administration du cyberespace de Chine ("CAC"). En outre, afin d'empêcher le flux illégal des données personnelles, ce projet renforce les exigences selon lesquelles *"il est interdit à toute personne ou organisation de fournir des programmes, des outils, etc. pour pénétrer et contourner le portail de sécurité des transferts de données transfrontaliers , l'accès à Internet, l'hébergement de serveurs, l'assistance technique, la diffusion et la promotion, le paiement et le règlement, le téléchargement d'applications et d'autres services pour pénétrer et contourner le portail de sécurité des transferts de données transfrontaliers."*
  - Les responsables de traitement ne doivent pas forcer les personnes concernées à donner leur consentement dans le but d'améliorer la qualité du service, l'expérience de l'utilisateur, de développer de nouveaux produits, etc.
  - Les données biométriques (données sensibles), notamment le visage, la démarche, les empreintes digitales, l'iris, l'empreinte vocale, etc. ne doivent pas être utilisées comme seul moyen d'authentification de l'identité d'une personne.

- *Mesures pour l'évaluation de la sécurité du transfert transfrontalier de données (Projet)*

  Le transfert de données hors Chine est sans aucun doute le sujet de préoccupation majeur des entreprises multinationales ayant des filiales en Chine. Depuis la CSL, l'évaluation de la sécurité reste un mystère. Ce projet pourrait être le projet le plus proche des mesures officielles guidant l'évaluation de sécurité organisée par le CAC à l'avenir.

  Les scénarios liés à l'un des éléments suivants, à savoir les CIIO, les données importantes, les responsables de traitement qui traitent les données personnelles de plus d'un million de personnes ou qui transfèrent les données personnelles de plus de 100,000 personnes ou les données personnelles sensibles de plus de 10 000 personnes, déclencheraient l'évaluation de sécurité organisée par la CAC, avant tout transfert.

  Selon le projet, au moins deux documents sont requis pour l'évaluation de sécurité en plus du formulaire de demande (qui pourrait être fourni ultérieurement par les autorités au moyen de modèles). Il s'agit du rapport d'auto-évaluation et le contrat conclu entre l'exportateur de données et le destinataire étranger des données. Dans la pratique, certaines multinationales commencent déjà à intégrer le cadre réglementaire chinois du transfert de données dans leur stratégie globale de flux de données conformément aux lois et réglementations actuelles, même incomplètes, ce qui peut déjà améliorer la légitimité de l'exportation de données de la Chine vers d'autres pays.

AUTRES

- *Reconnaissance faciale*

  Avec la PIPL et une interprétation judiciaire (publiée par la Cour Suprême de Chine et entrée en vigueur le 1er août 2021), les entités utilisant la reconnaissance faciale sont confrontées à davantage de problèmes de conformité et de litiges avec les personnes concernées.

L'interprétation judiciaire énumère clairement les scénarios de violation des droits et intérêts des personnes concernées par le traitement illégal de leurs données de reconnaissance faciale, et les utilisateurs de la reconnaissance faciale (c'est-à-dire les entreprises, les institutions, etc.) doivent prouver leur conformité en cas de litige (renversement de la charge de la preuve). Ainsi, compte tenu du nombre croissant de litiges civils et de sanctions administratives en Chine, il est conseillé aux parties prenantes de vérifier si la reconnaissance faciale est nécessaire et légitimée par les lois et règlements en vigueur.

- *Algorithme*

  Au niveau national, les *Dispositions administratives relatives à la recommandation d'algorithmes pour les services d'information sur Internet* viennent d'être adoptées le 4 janvier 2022, et seront effectives le 1er mars 2022. Elles exigent des fournisseurs de services d'algorithmes qu'ils évaluent le mécanisme de l'algorithme, qu'ils contrôlent le niveau de sécurité, qu'ils mettent en œuvre des mesures de sécurité des données et de protection des données personnelles, et qu'ils obtiennent l'enregistrement auprès des autorités compétentes si l'algorithme affecte l'opinion publique, etc. En outre, des modèles d'algorithmes incitant les utilisateurs à consommer ou à consommer à un prix élevé ne doivent pas être proposés par les fournisseurs.

  Au niveau régional, les autorités de Shanghai ont publié un guide sur la supervision des algorithmes utilisés dans le marketing numérique du commerce électronique. Selon ces directives, les algorithmes ne doivent pas être utilisés pour influer injustement sur les prix ou sur le traitement des consommateurs, etc., ce qui limitera plus ou moins le profilage et d'autres formes d'activités de data marketing.

***

Ce qui précède n'est qu'un aperçu de quelques aspects des mesures de protection des données et de cybersécurité en 2021. Certaines industries (automobile, pharmaceutique, etc.) ont également publié des règles spécifiques au cours de l'année 2021 (vous pouvez trouver nos précédentes Newsletters sur ces sujets via les liens suivants). Il ne fait aucun doute qu'il y aura d'autres nouveautés en 2022 que nous continuerons à partager.

Précédentes newsletters :

Health data: control your risks!
EN: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210930%20EN.pdf
FR: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210930%20FR.pdf

What to know about data of connected vehicles?
EN: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020211104%20EN.pdf
FR: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020211104%20FR.pdf

"Face Pressure": what's new about facial recognition in 2020 and 2021?
EN: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210629%20EN.pdf
FR: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210629%20FR.pdf

Seek a quick path to know the new PRC Data Security Law? Check the FAQs!
EN: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210715%20EN.pdf
FR: https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210715%20FR.pdf

Will the Chinese "GDPR" affect you? Get ready for the PRC Personal Information Protection Law
EN : https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210901%20EN.pdf
FR : https://www.dsavocats.com/mailing/Asia%20News/Newsletter%20Asie%2020210901%20FR%20.pdf

Pour toute information complémentaire, merci de contacter :

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
DOYON@dsavocats.com