

Etes-vous concernés par le «RGPD» chinois ? Soyez prêts pour la loi sur la protection des informations personnelles en Chine



ASIE

■ PRÉSENTATION GÉNÉRALE

Bien qu'il s'agisse d'une loi chinoise, de nombreuses entités étrangères traitant des données en Chine ont longuement attendu ce « *Règlement général sur la protection des données* » (« *RGPD* ») chinois. Après avoir été discutée et révisée pendant près d'un an, la *Loi sur la protection des informations personnelles de la République populaire de Chine* (« *PIPL* ») a finalement été publiée le 20 août 2021. Dernier arrivée des lois Cyber chinoises (i.e. Loi sur la cybersécurité (« *CSL* ») et Loi sur la sécurité des données (« *DSL* »)), la PIPL entrera en vigueur le 1er novembre 2021.

L'effet extraterritorial de la PIPL peut expliquer pourquoi elle occupe le devant de la scène. En effet, la PIPL sera applicable aux entités en Chine (individus, entreprises privées, autorités gouvernementales, institutions, etc.) mais aussi à celles qui n'ont pas de présence en Chine mais qui ciblent des personnes physiques en Chine par leurs activités de traitement des informations personnelles (« *PI* »).

Par conséquent, la PIPL affectera non seulement les entités chinoises mais aussi les entités étrangères soumises à l'application extraterritoriale de la PIPL. Afin de répondre à vos questions sur la PIPL, nous allons la présenter dans cet article sous un angle juridique et pratique.

■ STATUT DE LA PIPL DANS LA LÉGISLATION CHINOISE

Bien qu'il s'agisse de la première loi spéciale sur la protection des informations personnelles, la PIPL ne marque pas le début de la réglementation en la matière en Chine. Début 2012, sous l'impulsion du développement du numérique et des problèmes émergents en matière de protection des PI, la Chine a commencé à protéger « *les informations électroniques qui peuvent révéler l'identité des personnes et qui concernent la vie privée des citoyens* ». Par la suite, le Code civil, la CSL, la DSL, des règlements au niveau de l'État et au niveau local, des directives officielles et des standards nationaux ont été progressivement publiés, mais certains d'entre eux restent encore à l'état de projet. D'un point de vue juridique, ils font partie de la base juridique de la protection des PI, reflètent les principes généraux (le principe de notification-consentement) et ont ainsi ouvert la voie à la PIPL.

Parmi les lois chinoises en vigueur, il convient de noter la relation entre le Code civil, la CSL, la DSL et la PIPL.

Code Civil ¹
Loi chinoise fondamentale
*Reconnaissance du droit à la vie privée et des PI comme faisant partie du droit à la dignité humaine. Elle définit la vie privée et les PI et confirme les principes généraux du traitement des PI.

¹ Publiée le 28 mai 2020 et entrée en vigueur le 1er janvier 2021.

CSL ²	DSL ³	PIPL
Loi spéciale sur la cyber-sécurité	Loi spéciale sur les activités de traitement des données	Loi spéciale sur les activités de traitement des PI
- Elle régit les activités de cybersécurité des opérateurs de réseaux. - Elle inclut également les principes de base de la protection des PI et exige des CIIO (« Critical Information Infrastructure Operators ») qu'ils hébergent les PI localement et que tout transfert hors de Chine soit strictement encadré.	- Elle régit les activités de traitement des données en Chine et à l'étranger. - Les PI sont également considérées comme des données réglementées par la DSL, qui fournit des principes plus généraux (stratégies nationales) applicables à la plupart des types de données.	- Il s'agit de la loi spéciale régissant de manière exhaustive la protection des PI. - Elle consolide les principes généraux mais prévoit également des exigences plus spécifiques pour les responsables de traitement et les sous-traitants. - Elle prévoit des sanctions administratives sévères en cas de violation.

■ COMPARAISON AVEC LE RGPD

La PIPL est très similaire au RGPD, notamment en ce qui concerne les principales obligations du responsable de traitement et du sous-traitant, les droits de la personne concernée, ainsi que les exigences relatives aux scénarios de violation des données, etc. Le tableau ci-dessous expose une comparaison entre la PIPL et le RGPD sur certains aspects fondamentaux.

Aspects\Lois	RGPD	PIPL
Entités soumises à la loi	Responsable du traitement Sous-traitant	Responsable de traitement Sous-traitant
Données personnelles / informations personnelles	Ils sont similaires dans la définition des PI qui met l'accent sur leur fonction « <i>tout type d'information relative à une personne physique identifiée ou identifiable (article 4 de la PIPL)</i> » et excluent les « <i>données/informations anonymisées</i> » de la catégorie des PI.	
Champ d'application territorial.	Les deux sont dotés d'une compétence extraterritoriale fondée sur un principe de ciblage similaire. <u>- Critère de l'établissement :</u> Les activités liées au traitement des données personnelles par les responsables de traitement ou les sous-traitants établis dans l'UE, que le traitement ait lieu ou non dans l'UE. <u>- Critère du ciblage :</u> Les activités de traitement des données à caractère personnel sont liées à : (1) la fourniture de biens ou de services à une personne concernée au sein de l'UE, que la personne concernée ait l'obligation ou non de payer une contrepartie ; ou (2) le suivi du comportement de personnes dans l'UE. <u>- Critère territorial :</u> Les activités de traitement des PI ont lieu en Chine. <u>- Critère du ciblage :</u> Les activités de traitement des PI ont lieu en dehors de la Chine mais visent des personnes physiques en Chine : (1) pour la fourniture de produits et/ou de services ; ou, (2) pour l'analyse de leur comportement.	

² Publiée le 7 novembre 2016 et entrée en vigueur le 1er juin 2017.

³ Publiée le 10 juin 2021, entrée en vigueur le 1er septembre 2021.

La Newsletter a pour but de donner un aperçu des développements juridiques récents. Son contenu n'exprime pas un avis juridique et ne saurait se substituer à une consultation juridique.

Traitement	Ils sont similaires et comprennent l'ensemble du cycle de vie des données/informations à caractère personnel, y compris, mais sans s'y limiter, « <i>la collecte, le stockage, l'utilisation, le traitement, la transmission, la mise à disposition, la communication et la suppression (article 4 de la PIPL, liste non exhaustive)</i> ».	
Principes généraux du traitement	Ils sont également similaires pour la plupart des principes.	
	1. Légalité, équité et transparence ; 2. Finalité légitime 3. Minimisation des données ; 4. Exactitude ; 5. Limitation du stockage ; et, 6. Intégrité et confidentialité.	1. Légalité, légitimité, nécessité et bonne foi ; 2. Finalité légitime 3. Minimisation des données ; 4. Ouverture et transparence ; 5. Exactitude et exhaustivité ; 6. Sécurité.
Base légale du traitement	Bien que certaines formulations soient différentes, les bases légales sont similaires dans les aspects suivants. Le RGPD et la PIPL exigent tous deux que les responsables de traitement remplissent au moins l'une des conditions suivantes pour le traitement des PI.	
	1. Consentement éclairé ; 2. Contrat ; 3. Obligation légale ; 4. Intérêt vital des personnes ; 5. Intérêt public ;	1. Consentement éclairé ; 2. Contrat et gestion des ressources humaines ; 3. Obligation légale ; 4. Urgence (santé publique/intérêt vital des personnes) ; 5. Reportage d'actualité ou à des fins d'intérêt public ;
	Ils diffèrent dans les conditions suivantes énumérées. Le RGPD prévoit une base légale large via « <i>l'intérêt légitime</i> » pour le traitement des PI, tandis que la PIPL ne contient pas une telle clause mais précise que le traitement des PI légalement divulguées au public ne nécessite pas le consentement de la personne concernée (dans une certaine limite toutefois).	
	6. Intérêt légitime.	6. IP divulguée au public ; et, 7. autre base légale spécifiée par d'autres lois et règlements.
Droits des personnes concernées	Ils sont également similaires dans la plupart des droits de la personne concernée : 1. Droit à l'information ; 2. Droit d'accès ; 3. Droit de rectification ; 4. Droit à l'effacement/à l'oubli ; 5. Droit à la restriction du traitement ; 6. Droit à la portabilité des données ; 7. Droit d'opposition ; 8. Droit de ne pas faire l'objet d'une prise de décision automatisée.	
	La loi PIPL prévoit deux droits supplémentaires pour les personnes concernées et ne mentionne aucune restriction des droits des personnes concernées.	

Droits des personnes concernées	*Une communication transparente est requise et les droits des personnes concernées sont limités.	9. Droit de faire des copies (associé au droit d'accès) ; 10. Droit de décider des activités de traitement (associé au droit de restriction et au droit de refus).
*Veuillez nous contacter si vous souhaitez en savoir plus sur la comparaison entre le RGPD et la PIPL.		

Compte tenu de ces similitudes entre la PIPL et le RGPD, les entreprises européennes devraient être familières avec le cadre réglementaire de la PIPL et il leur sera donc plus facile de s'y conformer que les entreprises n'ayant pas fait l'expérience du RGPD.

■ POINTS PARTICULIERS DE LA PIPL

1. Élargissement du champ d'application des PI sensibles

Les PI des mineurs dont l'âge est inférieur à 14 ans sont considérées comme des PI sensibles.

2. Protection des PI des défunts

Pour les PI d'une personne décédée, un proche parent peut exercer les droits d'accès, de copie, de correction ou de suppression et d'autres droits sur les PI de la personne décédée, à moins que cette dernière n'ait pris d'autres dispositions avant son décès.

3. Test officiel des applications mobiles

L'autorité compétente a le droit d'organiser des tests et l'évaluation de tout programme d'application, pour la protection des PI, et de divulguer les résultats au public.

4. Restrictions sur l'utilisation des PI rendues publiques

Les responsables de traitement peuvent traiter les PI d'une personne lorsqu'elles ont été divulguées par celle-ci ou autrement divulguées légalement, sauf si ce traitement est expressément refusé par la personne concernée. Pour le traitement de toute PI divulguée d'une personne qui aurait un impact matériel sur cette dernière, le responsable de traitement doit obtenir le consentement de la personne.

5. Audit juridique

Les responsables de traitement devront faire régulièrement vérifier la conformité de leurs activités de traitement des PI avec les lois et règlements.

6. Représentant/succursale (exigence de présence) pour les entités étrangères

Les entités étrangères qui ne sont pas présentes en Chine mais qui sont soumises à la PIPL du fait de son application extraterritoriale, doivent établir une succursale ou désigner un représentant basé en Chine. Cette succursale ou le représentant désigné sera responsable des questions liées à la protection des PI et leurs informations de contact seront communiquées aux autorités compétentes concernées.

7. Droit d'action de la personne concernée

Les personnes concernées par un traitement peuvent engager une action devant les tribunaux contre un responsable de traitement en cas de refus de ce dernier à l'exercice de leurs droits.

8. Renversement de la charge de la preuve

Lorsque des dommages sont causés en raison d'une violation des PI, si le responsable de traitement n'est pas en mesure de prouver qu'il n'y a pas de faute de sa part, il doit assumer la responsabilité délictuelle, y compris la responsabilité des dommages. Par conséquent, l'entreprise doit non seulement mettre

en œuvre des mesures organisationnelles, techniques et de gestion pour assurer la conformité, mais aussi rendre le processus « visible » en conservant des enregistrements.

■ IMPLICATIONS POUR LES ENTREPRISES

1. Sanctions administratives

Violation de l'une des exigences de PIPL	Sanctions
Cas normaux	- Injonction de régularisation; - Avertissement ; - Confiscation des gains illégaux (le cas échéant) ; - (pour les applications) ordre de suspension ou de résiliation du service.
Lorsque le contrevenant refuse de rectifier les activités illégales	En plus de ce qui précède, - Amende pécuniaire (inférieure à 1 million de RMB) pour le contrevenant ; - Amende pécuniaire (de 10 000 RMB à 100 000 RMB) pour la personne directement responsable du contrevenant.
Cas graves	- Injonction de régularisation par l'autorité compétente au niveau des provinces ; - Confiscation des gains illégaux (le cas échéant) ; - Amende pécuniaire (inférieure à 50 millions de RMB ou inférieure à 5% du chiffre d'affaires de l'année précédente du contrevenant) pour le contrevenant ; - Suspension ou cessation d'activité, et annulation des agréments ou de la licence d'exploitation concernés ; - Amende pécuniaire (de 100 000 RMB à 1 million de RMB) à la personne directement responsable ; et, - La personne directement responsable du contrevenant peut se voir interdire pendant un certain temps d'exercer les fonctions de directeur, de superviseur, de cadre supérieur ou de responsable de la protection des PI.

2. Liste des missions pour la conformité PIPL

- Mise en œuvre de mesures internes efficaces

Impliquer les employés des différents services de l'entreprise et s'assurer qu'un responsable interne se consacre à la gestion de la protection des PI. Pour tout programme de conformité, toute question complexe ou toute formation et audit réguliers, des professionnels tiers (juristes, techniciens, etc.) doivent être impliqués.

- Mise à jour des Règles Internes

Politiques internes ;

Manuel des employés ;

Politique informatique ;

Plans d'urgence pour les incidents de sécurité PI, etc.

- Mise à jour des contrats

Contrats de travail ;

Contrats commerciaux impliquant le traitement de données personnelles (collecte, etc.) ;

Conditions générales et politique de confidentialité (y compris celles relatives aux programmes de fidélité) ;

Accords de confidentialité, etc.

- Vérifier les systèmes internes et les mesures techniques adoptées en interne

Système de contrôle d'accès (conception/classification du stockage des données en fonction des droits de l'utilisateur) ;

Système de sécurité à l'entrée (pour vérifier la nécessité et si des IP excessives et/ou sensibles sont collectées) ;

CRM (où vont les IP des clients et sont-elles contrôlées en toute sécurité) ; et,

ERP (gestion des IP des employés), etc.

- Vérifier si l'une des mesures techniques suivantes peut être prise pour améliorer la sécurité :

Désidentification / pseudonymisation ;

Anonymisation ;

Autres méthodes de cryptage, etc.

- Conformité globale (des exigences générales aux règles spécifiques)

Outre la PIPL, vérifier l'état de conformité avec la CSL, la DSL et d'autres réglementations régissant des secteurs particuliers (la santé, l'industrie pharmaceutique, l'automobile, l'industrie financière, le commerce électronique, les assurances, etc.), car ils peuvent avoir des exigences plus spécifiques pour le traitement des PI, comme par exemple, la période de conservation des PI des clients dans le secteur du commerce électronique.

■ POINTS NON RÉSOLUS

La PIPL est le point de départ de l'évolution législative chinoise en matière de protection des données personnelles, mais elle ne résout pas tous les problèmes qui préoccupent les entités impliquées dans le traitement des données personnelles, en particulier les entreprises multinationales.

1. Localisation des données

Les responsables de traitement, dont le traitement des PI atteint un certain seuil, tout comme les CIIO, doivent stocker en Chine les PI qu'ils ont collectées ou générées en Chine. Le seuil déclenchant l'obligation de localisation des données n'est pas encore spécifié et les non-CIIO devront donc attendre un peu plus longtemps pour obtenir des règles détaillées.

2. Transfert transfrontalier de PI

Les responsables de traitement soumis à l'obligation de localisation des données et les CIIO qui souhaitent transférer des PI hors de Chine doivent d'abord passer une évaluation de sécurité organisée par l'autorité nationale du cyberspace. Le contenu et l'organisation de l'évaluation sont soumis à des mesures qui n'ont pas encore été divulguées ou mises en œuvre.

3. Des définitions peu claires :

- « *Petits responsables de traitement* »

Outre la PIPL, les autorités compétentes publieront des règles et des normes spéciales pour la protection des PI concernant les « petits responsables de traitement », le traitement des PI sensibles, la reconnaissance faciale, l'intelligence artificielle et d'autres nouvelles technologies et nouvelles applications. La notion de « petit responsable de traitement » n'est pas définie.

- « Certification de protection PI »

Pour les responsables de traitement qui traitent des PI n'atteignant pas le seuil (pas encore défini) déclenchant l'obligation de localisation des données, la certification de protection des PI est l'une des options que ces responsables de traitement peuvent choisir afin de rendre possible le transfert transfrontalier des PI. Cependant, les détails concernant les prestataires de services et la procédure de demande de certification de protection des PI ne sont pas encore clairs.

- « Consentement spécifique »

Le PIPL mentionne que le consentement spécifique est requis dans plusieurs cas, mais aucune définition claire n'est encore fournie, et sa mise en œuvre n'est pas précisée.

Avec la mise en place de la PIPL, les entreprises qui sont impliquées dans le traitement des PI doivent dès à présent commencer à se mettre en conformité. Il s'agit d'un travail d'équipe s'inscrivant sur la durée. En pratique, tant que les données circulent, le traitement des PI est un processus dynamique, tout comme doit l'être leur protection.



Pour toute information complémentaire, merci de contacter :

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer - Shanghai Office
DOYON@dsavocats.com