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

Tout ce qu'il faut savoir sur les données des véhicules connectés

ASIE

CONTEXTE

De toute évidence, l'année 2021 est une année phare pour la protection des données en Chine. Après l'entrée en vigueur du Code Civil de la République Populaire de Chine en début d'année, la Loi sur la Sécurité des Données ("***DSL***") et la Loi sur la Protection des Informations Personnelles ("***PIPL***") ont été successivement promulguées, formant ainsi le cadre légal de la protection des données en Chine.

Simultanément, ces dernières années, suivant la tendance de la protection des données et le développement de l'industrie automobile, réglementation et normes nationales relatives aux véhicules connectés ont également été publiées. D'une part, la Chine encourage et promeut le développement de l'industrie automobile et l'utilisation des données massives relatives au transport. D'autre part, jusqu'à récemment, il n'y avait quasiment aucune réglementation spéciale sur la supervision des données de véhicules connectés.

Pour pallier ce manque, le Règlement relatif à la gestion de la sécurité des données de véhicules (pour une mise en œuvre à titre expérimental) («***Règlement***») a été publié le 16 août 2021, et est entré en vigueur le 1er octobre 2021.

CONCEPTS IMPORTANTS

Bien que la DSL et la PIPL définissent certains grands principes sur les données, le Règlement redéfinit des concepts similaires en les adaptant aux caractéristiques de l'automobile, comme indiqué dans les parties soulignées ci-dessous.

	Définition
Données du véhicule	comprend les données personnelles et les données importantes impliquées dans le processus de conception, fabrication, vente, utilisation, fonctionnement ou entretien du véhicule.
Traitement de données du véhicule	comprend la collecte, le stockage, l'utilisation, le traitement, la transmission, la fourniture et la divulgation des données du véhicule.
Responsable de traitement des données du véhicule	désigne les organisations qui exercent une activité de traitement de données du véhicule, notamment les constructeurs automobiles, les fournisseurs de pièces détachées et de logiciels, les concessionnaires, les prestataires de services de réparation et d'entretien, les sociétés de services de réservation de voitures, etc.
Donnée personnelle	désigne tout type d'informations relatives à un propriétaire, un conducteur ou un passager de véhicule, ou à toute personne se trouvant à l'extérieur du véhicule, identifié ou identifiable, enregistrées électroniquement ou d'une autre manière, à l'exclusion des données anonymisées.
Donnée personnelle sensible	désigne toute information personnelle qui, une fois divulguée ou utilisée illégalement, peut entraîner une discrimination ou une atteinte grave à la sécurité personnelle ou matérielle d'un propriétaire, d'un conducteur ou d'un passager de véhicule ou de toute personne se trouvant à l'extérieur du véhicule, y compris les données de localisation du véhicule, les informations audio, vidéo, image, biométriques et autres.

Le Règlement mentionne également 5 types de données considérées comme des données importantes. Conformément à la Loi sur la cybersécurité ("*CSL*") et au Règlement, les données importantes doivent être stockées en Chine, et tout transfert transfrontalier est soumis à un examen de sécurité conduit par les autorités compétentes. Il s'agit des données suivantes :

No.	Champ d'application des données importantes spécifiées par le Règlement
1	Informations géographiques, flux de personnes ou de véhicules et autres données relatives à toute zone sensible importante telle qu'une zone militaire, une zone d'une entité de développement scientifique et technologique de la défense nationale, ou d'une agence gouvernementale ;
2	Volume du trafic, logistique et autres données qui reflètent les performances de l'économie ;
3	Données de fonctionnement d'un véhicule collectées par le réseau utilisé pour la recharge ;
4	Vidéos ou images recueillies à l'extérieur d'un véhicule, y compris les visages des individus, les informations sur la plaque d'immatriculation, etc ;
5	Données personnelles concernant plus de 100 000 personnes ;
6	Autres types de données que les autorités compétentes considèrent comme susceptibles de mettre en danger la sécurité nationale ou les intérêts publics, ou de porter atteinte aux droits et intérêts légitimes d'un individu ou d'une organisation si ces données devaient faire l'objet d'une fuite.

Il convient de noter que les données personnelles peuvent être considérées comme des données importantes dans le contexte de l'industrie automobile lorsqu'elles concernent des données sensibles (information faciale) ou atteignent un certain volume (100 000 individus).

LES PRINCIPES DU TRAITEMENT DE DONNÉES DE VÉHICULES

Outre le principe de minimisation et de nécessité du traitement des données, et le système de protection à plusieurs niveaux («MLPS») requis par la CSL, le Règlement prévoit des exigences supplémentaires pour le traitement des données de véhicules :

1) Principe du traitement à l'intérieur du véhicule. Le traitement hors du véhicule ne peut être effectué que s'il est nécessaire de fournir des données à un destinataire extérieur au véhicule.

2) Principe de non-collecte par défaut. Cela signifie que le paramètre par défaut doit être «aucune collecte de données» pour chaque trajet, sauf si le conducteur en décide autrement de manière indépendante ;

3) Principe de précision et de couverture appropriées. Cela signifie que la portée de la couverture et la résolution de toute caméra, de tout radar, etc. sont déterminées en fonction des exigences de précision des données par les fonctions ou services fournis ; et,

4) Principe de désensibilisation. Cela signifie que les données sont anonymisées ou désidentifiées le mieux possible.

Pour assurer la sécurité de la conduite, des données personnelles d'individus à l'extérieur du véhicule peuvent être collectées pendant la conduite. Dans ce cas, le Règlement précise que si ces données personnelles ne peuvent pas être collectées avec le consentement des personnes concernées, elles doivent être anonymisées, notamment en supprimant l'image contenant les personnes physiques, ou en effectuant un traitement local des contours sur les informations faciales de l'image.

Si des données personnelles sensibles sont en jeu, le responsable du traitement des données du véhicule doit obtenir le consentement séparé de la personne concernée. Le responsable du traitement des données du véhicule ne peut collecter des informations biométriques telles que les empreintes digitales, les empreintes vocales, les informations faciales, le rythme cardiaque, etc. que dans un but de sécurité routière et en cas de nécessité avérée. Si une personne concernée demande la suppression des données, le responsable de traitement des données du véhicule doit les supprimer dans un délai de 10 jours ouvrables.

CONTRÔLE DES RESPONSABLES DE TRAITEMENT ET TRANSFERTS DE DONNÉES TRANSFRONTALIERS

Outre l'hébergement local et l'évaluation du transfert transfrontalier exigés par la CSL pour les données importantes, le Règlement prévoit pour les entreprises dans le domaine des véhicules connectés qui traitent des données importantes, les obligations suivantes :

1) Soumettre chaque année des informations sur la gestion de la sécurité à l'autorité de régulation. Les informations soumises comprennent : la personne responsable de la gestion de la sécurité des données des véhicules, le type de données, le volume des données, les mesures de protection de la sécurité, les données partagées au niveau national, le traitement des événements liés à la sécurité et le traitement des plaintes des utilisateurs concernés ;

2) Quant au transfert transfrontalier de données, outre ce qui précède, de soumettre en plus : les informations de base des destinataires de données ; le type, le volume, la finalité et la nécessité des données transférées ; le lieu de stockage, la période de conservation, la portée et la méthode de stockage des données du véhicule ; le traitement des plaintes des utilisateurs impliqués dans le transfert des données du véhicule à l'étranger.

**Il est recommandé aux entreprises de vérifier si leur secteur d'activité impose une période de conservation minimale des données. Par exemple, pour les entreprises opérant une plateforme de réservation de voitures en ligne, les informations personnelles collectées et les données commerciales générées doivent être stockées et utilisées en Chine continentale, et la période de conservation ne doit pas être inférieure à 2 ans.*

AUTRES NOUVEAUTÉS JURIDIQUES POUR LES VÉHICULES CONNECTÉS

1) Politiques nationales

Il convient de mentionner qu'avant l'entrée en vigueur du Règlement, le *Ministère de l'industrie et des technologies de l'information* («***MIIT***») a publié deux politiques importantes sur les véhicules connectés. Elles montrent que les véhicules connectés sont progressivement tenus d'être «sûrs dès la conception» en matière de données du véhicule.

- Avis du MIIT sur le *Renforcement de l'administration de l'accès au marché aux fabricants de véhicules connectés*, en vigueur depuis le 30 juillet 2021.
- Circulaire du MIIT sur le *Renforcement de la cybersécurité et de la sécurité des données des véhicules connectés*, en vigueur depuis le 15 septembre 2021.

2) Standards nationaux

Les exigences en matière de conformité pour les données des véhicules dans le Règlement sont peut-être trop larges et trop vagues, mais il existe déjà des projets de normes nationales relatives aux données des véhicules, qui peuvent éclairer les entreprises sur la manière de se mettre en conformité.

Selon deux normes nationales récentes, *Sécurité des Technologies de l'Information - Guide pour la sécurité des données des services de réservation de voitures en ligne* (projet pour commentaire), et *Sécurité des Technologies de l'Information - Exigences de sécurité pour les données collectées par les véhicules en réseau* (projet pour commentaire), il est recommandé de stocker les données de suivi et d'enregistrement des trajets sur un serveur avec des mesures de protection et de sécurité, et certaines données du véhicule (la route, le bâtiment, le terrain, les participants au trafic et d'autres données collectées par le véhicule connecté à partir de l'environnement externe) ne doivent pas être transmises à l'étranger.

**Veuillez noter que les normes nationales susmentionnées sont encore à l'état de projet au moment de la publication de cet article.*

COMMENTAIRES

En raison des caractéristiques des données de véhicules, nous suggérons que les entreprises concernées procèdent à une auto-évaluation de leur conformité au regard de la CSL, DSL, PIPL et d'autres réglementations propre à leur industrie (comme le Règlement), des normes nationales, etc. En cas de non-respect de la règlementation, il est nécessaire de lancer le projet de mise en conformité le plus rapidement possible.

Selon le Règlement, le responsable du traitement de données de véhicules est susceptible de faire l'objet d'une supervision croisée de la part de multiples autorités de régulation, y compris, le Bureau d'Information, le Ministère du développement et de la réforme, le MIIT, le Ministère de la sécurité publique, le Ministère des transports, etc. Afin de faire face à la surveillance active des autorités, nous suggérons que, dans la pratique, les entreprises concernées accordent plus d'attention aux avis et aux mises à jour publiés par les diverses autorités, afin de rester proactif dans leur travail de conformité.

Pour toute information complémentaire, merci de contacter :

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
DOYON@dsavocats.com