**Par Prudence Cadio,**
avocate associée,

**et Fanny Nguyen,**
avocate locale (Shanghai),
LPA-CGR avocats

# RGPD/PIPL : superposition et empiétement des réglementations sur la protection des données personnelles des citoyens d'Europe et de Chine

**Tous les continents sont aujourd'hui dotés de lois et règlements afin de protéger les données personnelles de leurs concitoyens. Que ce soit la CCPA (California Consumer Privacy Act), la LGPD (Brazilian Data Protection Law), le RGPD (règlement général de la protection des données), la PIPL (Personal Information Protection Law) ou encore l'APP (Asutralian Prinvacy Policies), chacun de ces textes permet non seulement de garantir un niveau de protection nationale ou régionale, mais aussi, dans certains cas, une protection transfrontalière au titulaire de ces données, dans le cadre de leur collecte et exploitation. De manière assez étendue, les données qualifiées de « personnelles » sont celles qui permettent d'identifier un individu, que ce soit dans une sphère privée ou professionnelle. Chaque texte et régulateur a, par la suite, affiné la définition de cette notion première.**

L'un des enjeux de ce droit des données émergent réside dans l'extranéité de sa mise en œuvre et, par conséquent, de l'ingérence éventuelle des autres lois dans la protection et l'utilisation des données de ces citoyens dans un pays qui n'est pas le leur. Comment conjuguer ces nouvelles réglementations, souvent protectionnistes, avec la mondialisation ? Vous trouverez ci-après quelques éléments de réponse concernant l'axe Europe-Chine et l'articulation de la PIPL avec le RGPD.

## 1. Extranéité des réglementations sur les données personnelles, première raison des superpositions réglementaires

### 1.1. Le RGPD : une application au-delà de l'Europe

Le RGPD[1] et la loi informatique et libertés[2] (la LIL) en France qui gouvernent la collecte et le traitement de données à caractère personnel contiennent également des éléments d'extranéité. Pour rappel, les données personnelles concernées par ces textes

sont toute information se rapportant à une personne physique identifiée directement ou indirectement, notamment par une donnée de localisation ou un numéro client.
Par la combinaison des articles 3 du RGPD et 4 de la LIL, sont couverts par cette réglementation tous les traitements réalisés par des opérateurs qui sont situés en France, que ces traitements visent ou non des résidents européens ou français. Le RGPD et la LIL gouvernent donc l'exploitation de données de personnes partout dans le monde, en ce compris la Chine, si une telle collecte ou exploitation est monitorée depuis la France. Cela peut notamment être le cas de sites d'e-commerce édités en France ou bien encore d'un groupe dont la société mère située en France décide de piloter, pour certaines finalités de management RH, les données de ses salariés localisés partout dans le monde, y compris en Chine.
Par effet miroir, le RGPD prévoit également que les opérateurs (responsables de traitement ou sous-traitants) situés hors du territoire de l'UE mais qui proposent des biens ou services à des personnes dans l'UE ou qui suivent le comportement des personnes dans l'UE, devront s'y soumettre. En ce sens, une société chinoise qui proposerait, depuis la Chine, des produits à des résidents de l'UE devra se conformer au RGPD ainsi qu'à la PIPL.

### 1.2. La PIPL : au-delà de la Chine, sur le modèle européen

La PIPL[3] régit la collecte et le traitement des données à caractère personnel en Chine. La notion de donnée à caractère personnel est entendue largement par ce dispositif, sur le modèle du RGPD, et inclut ainsi toute information de quelque nature que ce soit, identifiant ou pouvant identifier les personnes physiques.
La PIPL se veut nationaliste et protectionniste, à l'image de la politique actuelle de la Chine, d'autant que la criminalité de l'information est en forte croissance en Chine.
Ce protectionnisme s'illustre dans la façon dont les lois protègent strictement les données de toute personne installée en Chine.
A l'image du RGPD, la PIPL s'appliquera non seulement à tout opérateur qui met en œuvre des traitements depuis le territoire chinois mais également à tout opérateur en dehors de Chine, lorsque le traitement qu'il met en œuvre concerne une personne située en Chine, aux fins de lui proposer un produit et service en Chine ou permet d'analyser son comportement sur le territoire chinois. La PIPL se laisse d'ailleurs la possibilité d'élargir les hypothèses d'application transfrontalière par toute autre loi ou texte réglementaire.
Cette protection dépasse les frontières et cette extraterritorialité est exprimée fermement avec des pénalités fortes en cas d'infraction (en cas de violation grave, environ 7 millions d'euros ou 5 % du chiffre d'affaires) et des interdictions de devenir destinataires de données de résidents chinois pour les entités hors de Chine.
Les lois précédentes, et notamment la Cyber Security Law publiée en 2017, avaient déjà exprimé le fait que les données personnelles chinoises collectées par les exploitants des infrastructures d'information clés ne pouvaient pas être délocalisées en dehors de Chine et qu'à défaut, ce n'était jamais pour les stocker en dehors de Chine.

***Une société chinoise qui proposerait, depuis la Chine, des produits à des résidents de l'UE devra se conformer au RGPD ainsi qu'à la PIPL.***

La PIPL renforce ce dispositif et contraint les sociétés à mettre en place une organisation complexe et coûteuse.
Cet ensemble de lois rend ainsi la tâche difficile pour les sociétés multinationales qui se développent en Chine ou pour lesquelles les consommateurs chinois représentent une part importante de leur chiffre d'affaires.

### 1.3. Le retail : un secteur particulièrement touché par les doubles obligations de conformité

Parmi les nombreux secteurs concernés par ces flux de données, les sociétés dans le secteur du retail ont été dans les premières à être sensibilisées à la nécessité d'une mise en conformité compte tenu du volume de données traitées et de l'importance de connaître le « parcours client » des consommateurs, notamment dans le cadre de magasins d'une même enseigne. Quand dans une boutique en Chine d'une enseigne de luxe ou de retail, un client chinois achète un sac et s'inscrit dans le fichier client de l'enseigne, la question du recueillement du consentement de cette personne se pose immédiatement. Le consentement individuel est en effet au cœur de la PIPL. Il doit être obtenu par écrit, légalement, donné de bonne foi, en toute transparence et pour un but clair et précis.
Comment recueillir ce consentement ? Pour quel usage et quelle durée ? Pour quelle zone géographique ?
Se pose alors la question de l'application cumulative ou distributive du RGPD et de la PIPL lorsque ce même client souhaitera, lors d'un séjour à Paris, acheter un sac de la même marque ou par le biais de la plate-forme e-commerce éditée par l'enseigne. L'enseigne aura-t-elle harmonisé une base client avec le seul consentement recueilli en Chine ? L'enseigne devra-t-elle accomplir des formalités additionnelles dans ses boutiques en France ?
L'opportunité de compartimenter les bases clients afin de résoudre, d'un point de vue opérationnel, ce sujet réglementaire est souvent envisagée mais cela ne répond pas au souhait des enseignes internationales de se doter, au contraire, d'une base de données unique. Le circuit des données devra faire l'objet d'une attention particulière pour résoudre cette équation, notamment aux fins d'informer l'individu du traitement mis en œuvre, et ce via le bon support d'information et d'assurer la conformité du transfert des données hors des frontières où elles ont été collectées. La question de la conservation des données du client sera par ailleurs à soulever, les délais de conservation

et d'archivage des données variant d'un Etat à l'autre.
Ce sujet se retrouvera également dans le cadre de la mobilité de salariés dans le domaine du retail ou du luxe, lorsque ceux-ci sont amenés à travailler dans différents points de ventes à travers le monde et, dans le cas d'espèce, entre la France et la Chine.

## 2. L'échange des données personnelles : des exigences pour les expéditeurs et destinataires ?

### 2.1. Règles applicables en matière de PIPL

La PIPL impose un cadre strict aux transferts de données personnelles hors du territoire chinois. Ainsi, les données ne peuvent être transférées hors de Chine que si le destinataire de données a validé une analyse de sécurité menée par une autorité compétente, si le destinataire a obtenu une certification de protection des données délivrée par une agence professionnelle, si un contrat a été conclu entre l'émetteur et le destinataire des données (sur la base du contrat type élaboré par une autorité compétente) ou si une loi prévoit et autorise ce transfert. Outre le respect de l'une des conditions ci-dessus, l'émetteur du transfert doit également prendre un certain nombre de mesures visant à garantir un niveau aussi protecteur que celui de la PIPL, il doit informer les personnes concernées et obtenir leur consentement.
Ces mesures et conditions traduisent la volonté affirmée de garantir la protection des données hors du territoire chinois.
A travers cette loi, il y a une obligation imposée aux sociétés de garantir la protection de ces données et de s'assurer du bon usage du consentement donné par la personne. Les autorités chinoises exigent désormais que cette protection passe par la mise en place d'un système local en adéquation avec l'activité de la société et le service rendu à la personne.
Le régulateur veut s'assurer que les données sont sous contrôle et un enregistrement de l'encadrement de la protection des données par les sociétés peut être requis par les autorités chinoises.

***Les transferts de données hors UE ne sont pas interdits à condition que les responsables de traitement ou sous-traitants qui les opèrent assurent un niveau de protection des données suffisant et approprié.***

### 2.2. Règles applicables en matière de RGPD

Le RGPD organise les conditions dans lesquelles des données peuvent être transférées hors de l'Union européenne.
Les transferts de données hors UE ne sont pas interdits à condition que les responsables de traitement ou sous-traitants qui les opèrent assurent un niveau de protection des données suffisant et approprié.
La Commission européenne a déjà, par voie de décision d'adéquation, constaté que des pays tiers assuraient un niveau suffisant de protection. Aussi, à titre d'exemple, dans le cadre d'un transfert en Suisse, Argentine ou Japon, aucune formalité supplémentaire ne sera exigée.
A contrario, pour un transfert vers un pays tel que la Chine, le RGPD exige que ce transfert soit encadré par un véhicule juridique. Parmi ces instruments juridiques, les clauses contractuelles types (CCT), éditées par la Commission européenne, peuvent être utilisées.
Concrètement, avant d'être transmise en Chine, les données de partenaires européens ou tout accès d'entreprises situées en Chine à des données hébergées et traitées en Europe, devront faire l'objet d'un accord de transfert.
La Commission, a, à ce titre, récemment modifié les exigences attendues dans le cadre de ces CCT, il est désormais imposé aux cocontractants d'évaluer en pratique si la législation du pays tiers permet de respecter le niveau de protection requis par le droit de l'UE et les garanties fournies par les CCT. Si cette évaluation révèle un niveau de protection insuffisant dans le pays tiers, des mesures complémentaires devront être prévues.

## 3. Quelle est l'approche à adopter face à ces chevauchements de réglementations ?

Avant même d'initier des actions, encore faut-il savoir à quelle réglementation sont soumis les traitements mis en œuvre pour ensuite savoir comment se conformer !
Le RGPD a néanmoins été le modèle de chacune de ces réglementations et l'influence de cette dernière sur la PIPL demeure évidente à la lecture des textes. L'extraterritorialité est cependant soumise en Chine à davantage de contraintes administratives.
Il est difficile de faire l'économie d'un audit des traitements et flux de données mis en œuvre par les sociétés lorsque ces dernières souhaitent s'assurer d'une mise en conformité. En effet, cette cartographie permet d'identifier les différentes réglementations applicables et de coordonner les process de conformité à déployer selon les territoires et entre les différentes entités concernées. La proximité entre ces réglementations permet, souvent, de mutualiser certaines actions, ce qui peut constituer un gain de temps important.
Cet audit va permettre ensuite de définir une stratégie de gouvernance de la data qui pourra être déployée au sein de la société ou, le cas échéant, du groupe tout en limitant les impacts administratifs contraignants que cela pourrait avoir sur les équipes opérationnelles. Cet audit permettra également de prioriser les mises en conformité selon les départements (RH, commercial ou achat) et/ou selon les branches d'activités les plus sensibles d'un point de vue de la protection des données à caractère personnel.

## 4. Actualité juridique

Le 29 avril 2022, Le Comité technique national de normalisation de la sécurité de l'information de Chine (« TC260 ») a publié pour avis consultatif un projet de directive[4], abordant de

manière plus précise la réglementation des transferts internationaux de données personnelles provenant de Chine.
Deux scénarios sont adressés dans cette directive : les transferts intragroupes vers une société en dehors de Chine et les utilisations offshore de données personnelles rentrant dans le champ d'application de la PIPL.
Cette directive ne répond pas encore à toutes les interrogations mais démontre d'ores et déjà une volonté de contraindre à la mise en place d'un dispositif juridique lourd dans toutes les sociétés d'un même groupe dès lors qu'elles entrent dans le champ d'application de la PIPL.
De même, en matière de protection et de gouvernance des données, l'Union européenne continue de compléter son arsenal réglementaire. Ainsi, il devrait être adopté prochainement le Data Act dont le périmètre sera plus large que le RGPD puisqu'il ne se limitera pas aux données à caractère personnel. Il visera à gouverner la collecte, la transmission et le partage de toutes les données générées par des produits connectés, dénommés IOT. Les IOT sont définis comme des « biens corporels meubles (y compris s'ils sont incorporés dans un bien immeuble) qui obtiennent, génèrent ou recueillent des données qu'ils peuvent transmettre via un réseau public, et dont la fonction première n'est pas le stockage et le traitement de données ». Aussi, les données personnelles et non personnelles générées par les IOT seront soumises à des règles de transmissions particulières. L'objectif est de renforcer la sécurité des données issues de ces produits tout en facilitant leur transmission entre notamment le fabricant de produits IOT, l'utilisateur, les prestataires de services qui permettent l'accès aux données et les organismes publics. Ce règlement devrait s'appliquer aux produits de l'IOT et aux services connexes qui sont « mis sur le marché dans l'Union [européenne] », ainsi qu'aux prestataires de services de traitement des données « offrant ces services à des clients dans l'Union européenne. Aussi, celui-ci devra être pris en considération par tout équipementier fabriquant en Chine à destination des marchés européens ». ■

***Le 29 avril 2022, Le Comité technique national de normalisation de la sécurité de l'information de Chine (« TC260 ») a publié pour avis consultatif un projet de directive, abordant de manière plus précise la réglementation des transferts internationaux de données personnelles provenant de Chine.***

*1. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).*
*2. Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.*
*3. Personal Information Protection Law en date du 1er novembre 2021.*
*4. Draft Guidance on Network Security Standardized Practice – Technical Specification for Certification of Personal Information Cross-Border Processing Activities.*