Inde - le Personal Data Protection Bill, 2018 : émergence d'une politique de protection des données personnelles

ASIE

Dans le contexte de l'arrêt Puttaswamy consacrant le droit au respect de la vie privée comme un droit constitutionel fondamental et la réforme du régime de protection des données personnelles en Europe, l'Inde fait face à l'imperative nécessité d'adopter un régime de protection des données personnelles.

Aadhaar, Règlement Général de Protection des Données ("**RGPD**"), transition vers une économie digitale… règlementer la protection des données est devenu un impératif politique pour l'Inde.

Outre le contexte global de renforcement de la protection des données personnelles, Aadhaar (le projet d'identification biometrique) est à l'origine de l'empressement de l'Inde à adopter un tel régime. Dans le cadre de la mise en place d'Aadhaar, l'Inde a en effet procédé à la plus grande collecte de données personnelles de son histoire (et du monde), sans regime de protection des données personnelles en place. Cette collecte, quasi-obligatoire par nature, et le traitement des données en resultant, a mis en lumière les failles du système indien suite à de nombreuses violations. Le systeme Aadhaar (regroupant les données de 1,2 milliards d'individus) a été, et est toujours, vertement contesté, notamment devant les juridictions indiennes, du fait des risques qu'il présente pour le droit au respect de la vie privée. Dans un arrêt de principe K S Puttaswamy v Union of India (2017), la Cour Suprême indienne a ainsi réaffirmé que le droit au respect de la vie privée est un droit fondamental et mis à la charge de l'Etat un devoir positif de protection contre toute atteinte à la vie privée des individus par les acteurs privés et publics.

Cet arrêt a réintroduit de force le dialogue sur la protection des données pesronnelles en Inde, sur fond de RGPD.

Moins d'un an après sa formation, un comité d'experts dit Srikrishna Committee, ayant pour mission de formuler un régime de protection des données, a publié, le 27 juillet dernier, le projet de Personal Data Protection Bill, 2018 ("**PDPB**") largement inspiré du RGPD.

Les principales caractéristiques du PDPB, introduisant le concept de 'privacy by design' au coeur du RGPD, sont les suivantes:

I. CHAMP D'APPLICATION ET APPLICABILITÉ

Le PDPB régit la collecte et le traitement des **données**, définies comme tout information, fait, concept, opinion, instruction pouvant être echangé, interpreté ou traité par des humains ou de manière automatisée. Le PDPB distingue par ailleurs les données personnelles des données sensibles définies de manière limitative.

Le PDPB introduit également en droit indien les concepts de:

- ***data fiduciary***, défini comme toute personne physique ou morale, privée ou publique qui dirige directement ou indirectement le traitement des données personnelles,
- ***data principal***, défini comme la personne physique propriétaire des données personnelles, et
- ***data processor,*** défini comme toute personne physique ou morale, privée ou publique qui participe au traitement des données personnelles pour le compte du data fiduciary (hors salarié du data fiduciary).

Comme le RGPD, le PDPB est extra-territorial et s'applique non seulement aux *data fiduciaries* établis en Inde mais également aux *data fiduciaries* qui fournissent, de manière habituelle, des services ou des biens en Inde ou sont impliqués dans le profilage de *data principals* en Inde.

II. LICÉITÉ DE LA COLLECTE ET DU TRAITEMENT DES DONNÉES PERSONNELLES

Le PDPB liste de manière limitative les conditions de la licéité de la collecte et du traitement des données personnelles (***grounds for processing***), l'obtention préalable du consentement de la personne concernée étant le critère principal. Le gouvernement pourra quant à lui justifier la collecte, sans consentement, de toutes données lorsque la collecte est 'nécessaire' pour les 'fonctions de l'Etat' (le caractère nécessaire de la collecte devant être apprecié au regard des limites de constitutionalité posées par l'arrêt Puttaswamy).

Pour être valide, le consentement doit être: (a) libre, (b) éclairé, (c) spécifique, (d) univoque et (e) susceptible d'être retiré (droit de retrait). Du fait de ces nouveaux critères de validité du consentement, le PDPB met ainsi à la charge de tout *data fiduciary* l'obligation de revoir les procédures d'obtention du consentement pour les mettre en conformité avec le PDPB.

Le PDPB prévoit par ailleurs un régime spécifique aux traitements de données personnelles de mineurs, pour lequel le consentement des personnes dépositaires de l'autorité parentale devra être recueilli après verification de leur âge.

Les *data fiduciaries* doivent enfin limiter la collecte des données personelles aux données nécessaires au regard des finalités pour lesquelles elles sont traitées et la durée de conservation de ces données doit être limitée à une période strictement nécessaire à

la réalisation des objectifs pour lesquels les données ont été collectées. En application de ce principe de minimisation, les données collectées ne pourront pas etre utilisées pour d'autres finalités que celles pour lesquelles elles ont été collectées.

III. DROITS DES *DATA PRINCIPALS*

Le PDPB consacrent de nouveaux droits sensiblement similaire à ceux confirmés ou consacrés par le RGPD, notamment le droit d'accès, droit de rectification, droit à la portabilité des données personnelles, droit à l'oubli.

IV. OBLIGATIONS DES *DATA FIDUCIARIES*

Le PDPB met à la charge des *data fiduciaries* certaines obligations, notamment l'obligation de délivrer aux individus une information concise, transparente, intelligible et dans une forme aisément accessible en utilisant un langage clair, de prendre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté, de respecter le principe de minimisation, de preserver la qualite des données, etc.

Dans ce cadre, les sociétés devront prendre des mesures techniques et organisationnelles (ou revoir les mesures existantes) pour se mettre en conformité avec le PDPB (*privacy by design*). La protection des données personnelles devra être intégrée dès la conception des systèmes et des technologies mis en place.

Le PDPB introduit également la notion de '*significant data fiduciaries*' (du fait du volume ou de la nature des données traitées). Ces *significant data fiduciaries* devront s'enregistrer auprès de l'autorite indienne de protection de données ("**AIPD**"), nommer un délégué à la protection des données, réaliser une étude d'impact et analyse de risque et se soumettre à un audit annuel des systêmes en place par un auditeur indépendant.

Le PDPB met enfin à la charge des *data fiduciaries* l'obligation de stocker en Inde les données personnelles régies par le PDPB (soit complètement soit sur un serveur-miroir). En pratique, cette obligation de différencier les données et de les stocker en Inde risque d'être fastidieuse et coûteuse à mettre en place pour les PME et ETI, particulièrement celles identifiées par le Gouvernement comme collectant des données personnelles essentielles (*critical personal data*) devant être stockées uniquement en Inde. Le PDPB pose par ailleurs de nombreuses restrictions aux transferts de données à l'étranger.

V. AUTORITÉ DE CONTRÔLE ET SANCTIONS

Le PDPB crée une autorité indépendante de contrôle, l'AIPD, dotée de pouvoirs réglementaires, de contrôle et de sanction élargis. Essentielle à la mise en place du système de protection des données, l'autorité souffre toutefois, à ce stade du projet de loi, d'un certain manque d'indépendance et d'un excès de délégation de pouvoir réglementaire, qui pourraient *in fine* nuire au régime de protection devant être mis en place.

Le PDPB met en place un mécanisme de notification des violations. Les *data fiduciaries* ont ainsi la responsabilité de notifier l'AIPD de toute violation de données personnelles pouvant nuire à la personne dont les données ont été violées dans un delai devant être prescrit par l'AIPD.

L'AIPD peut imposer des amendes importantes à toute personne qui contreviendrait au PDPB, en ce compris l'Etat. Toutefois, la marge de manoeuvre donnée à l'Etat sous couvert de 'nécessité et d'intérêts stratégiques de l'Etat' risque en pratique de les exempter de toute responsabilité.

Comme le RGPD, le PDPB se caractérise par la sévérité des amendes pouvant etre prononcées par l'AIPD. Le défaut de notification de l'AIPD en cas de violation est ainsi passible d'une amende d'un montant maximum de 50 millions de roupies ou 2% du chiffre d'affaires mondial de l'année précédente. La collecte et le traitement de données personnelles en violation du PDPB ont passibles d'une amende d'un montant maximum de 150 millions de roupies ou 4% du chiffre d'affaires mondial de l'année précédente.

Le PDPB liste également des infractions pénales non soumises à caution (*cognizable and non bailable*) passibles d'une amende d'un montant maximum de 200.000 roupies ou 3 ans d'emprisonnement.

VI. CONCLUSION

La volonté du Gouvernement indien de mettre en place un régime de protection des données personnelles conforme aux standards mondiaux doit etre saluée. Toutefois, et bien que fortement inspiré du GRPD, le PDPB présente plusieurs lacunes qui pourraient avoir un impact négatif sur les droits au respect de la vie privée et à l'information. Le Gouvernement devra adresser ces lacunes avant de soumettre le projet de loi au parlement.

Plus d'infos juridiques sur l'Asie :

> Chine - Réforme de l'impôt sur le revenu des personnes physiques

Pour toute information complémentaire, merci de contacter :

asie@dsavocats.com