

L'INDE SE MET A LA PAGE EN MATIERE DE PROTECTION DES DONNEES PERSONNELLES

L'Inde a récemment réformé la Loi sur la technologie de l'information datant de 2000 (« Information Technology Act » - ITA), ajoutant des dispositions très attendues sur la protection des données, la cybercriminalité, la responsabilité des fournisseurs d'accès à internet et l'authentification de la signature électronique. Le Ministère indien des Technologies, de l'Information et de la Communication est actuellement en train de rédiger des dispositions supplémentaires selon les préconisations du NASSCOM (l'organisme de promotion et de développement des nouvelles technologies et des services associés) et du Conseil de sécurité des données (« Data Security Council of India » - DSCI). Dès que le Ministère aura finalisé la réforme, les amendements seront applicables et auront un impact sur tous les pays faisant affaires avec ou en Inde.

L'augmentation générale de la cybercriminalité et les attentats terroristes de Bombay en novembre 2006 ont probablement précipité l'adoption de la réforme de la Loi sur la technologie de l'information (the Information Technology Amendment Act – ITAA). La croissance rapide des secteurs IT et de la sous-traitance en Inde (où le traitement des données est un élément important) a aussi sûrement contribué à l'adoption de l'ITAA. L'ITAA représente un véritable investissement dans les dispositifs de sécurité des données en Inde. En outre, la réforme informe le monde entier que l'Inde reste un endroit sûr pour faire des affaires.

Dispositions clefs de la réforme de la Loi sur la technologie de l'information

L'ITAA va exiger de toutes les entreprises étrangères qui ont un service indien offshore de maintenir « des pratiques et des procédures de sécurité raisonnables » en cas de gestion de « données personnelles sensibles » sur leurs systèmes informatiques (Section 43 A). Les définitions légales de « pratiques de sécurité raisonnables » ou « données personnelles sensibles » sont en train d'être finalisées.

Cependant, comme les préconisations du NASSCOM et du DSCI sont déjà en place, les « pratiques de sécurité raisonnables » vont probablement obliger les organisations à détailler leurs standards et procédures de contrôle de sécurité. En cas de faille de sécurité, l'organisation

devra démontrer la conformité de son dispositif avec les procédures et prouver que les procédures sont proportionnées par rapport aux données qui doivent être protégées.

La définition de l'ITAA des « données personnelles » sera probablement la suivante : *« informations qui permettent d'identifier directement ou indirectement une personne, que ce soit par référence à l'identification d'un numéro ou à des détails physiques, économiques, culturelles, physiologiques ou mentaux »*. Cette définition est en accord avec les directives européennes sur la vie privée. En effet, l'ITAA introduit le concept de « donnée personnelle » dans le droit indien. Alors que la loi d'origine punissait l'extraction non autorisée de données et/ou tout atteinte aux données, elle n'incluait pas cette disposition.

En revanche, la définition des « données personnelles sensibles » de l'ITAA devrait exclure les références aux origines raciales ou ethniques ainsi qu'aux croyances politiques ou religieuses. Cela constitue une nette différence avec les directives européennes.

Il sera donc impératif pour les entreprises qui font affaires avec l'Inde ou en Inde de se familiariser avec la section 43 A de l'ITAA, ainsi qu'avec ses définitions spécifiques pour le vocabulaire clef. Cela aura clairement des répercussions pour l'industrie de sous-traitance indienne et ses partenaires de tous pays.

En outre, l'ITAA étend la responsabilité de l'utilisation des données personnelles des particuliers aux personnes morales. Le manquement d'une entreprise à la sécurité des données personnelles entraîne un droit d'agir en justice à tout individu qui a vu ses données personnelles sensibles compromises.

L'ITAA constitue une étape majeure dans la mise en place de lois efficaces pour la protection des données aussi bien pour les entreprises indiennes que leurs partenaires étrangers. Cependant, de nombreux détails doivent encore être précisés par les ministères et leur organisme de conseil, le DSCI, avant que l'on puisse déterminer l'impact réel de cette loi.

Par ailleurs, l'ITAA élargit également le champ de la cybercriminalité en y incluant le cyberterrorisme, élève certaines peines pour la cybercriminalité et insère des exigences accrues de coopération, de rétention et d'accès aux données pour les intermédiaires comme les fournisseurs d'accès à internet et les partenaires réseaux ou télécoms.

Conseil aux entreprises

Aux vues des modifications apportées par l'ITAA, il est plus prudent, pour une entreprise qui exerce une activité en Inde ou avec l'Inde, de revoir ses contrats conclus avec ses partenaires indiens afin de s'assurer que ces derniers abordent correctement la question de la protection des données. Il conviendrait également de modifier les contrats à long terme contenant des dispositions relatives à la sécurité des données qui ne sont plus d'actualité ou qui ne sont pas en accord avec les modifications de l'ITAA.

Vous trouverez ci-dessous quelques conseils à prendre en compte lors de l'évaluation de vos contrats de sous-traitance en cours avec des partenaires indiens :

- Etudiez les pratiques et procédures de sécurité des données de votre partenaire indien et assurez-vous qu'elles ne présentent pas de faille ou déficience.
- Assurez-vous que votre contrat de sous-traitance exige expressément de votre prestataire de service indien qu'il se conforme à l'ITAA et à toute

autre loi applicable concernant la protection des données.

- Aussi longtemps que le Gouvernement indien n'aura pas précisé les procédures de sécurité appropriées, votre contrat de sous-traitance devrait également exiger de votre société qu'elle se conforme aux normes de sécurité reconnues dans le secteur de l'industrie (par exemple : Norme de sécurité informatique des données de l'industrie des cartes de paiement).

- Votre contrat de sous-traitance doit aborder la définition de « faille de sécurité ».

- Votre contrat doit inclure un droit d'audit exhaustif pour que vous puissiez vérifier que votre partenaire remplit entièrement ses obligations.

- Votre contrat doit prévoir des recours contractuels en cas de non-conformité, y compris des indemnités, un droit de résiliation etc.

- Votre contrat doit enfin aménager la responsabilité des partenaires en cas de dommage direct ou indirect suite à des failles de sécurité.

En conséquence, en attendant que l'Inde adopte formellement l'ITAA par sa publication dans la gazette Officielle, précisant ainsi les définitions de « donnée personnelle sensible » et de « pratiques et procédures de sécurité raisonnables », voici un point de plus qu'il sera indispensable d'étudier avec attention avant de se lancer pour les entreprises qui envisagent de sous-traiter tout ou partie de leurs activités à un partenaire indien.

Une analyse d'Annabelle RICHARD, Avocat à la Cour et Attorney at Law (New York Bar) et d'Arya SHEKAR, juriste au sein du Département Technologies Médias et Télécommunications du cabinet Ichay & Mullenex Avocats.

Le cabinet Ichay & Mullenex Avocats s'est spécialisé dans la gestion des problématiques juridiques liées à l'activité des entreprises de nouvelles technologies. Il conseille ainsi de nombreux acteurs du e-commerce, de l'informatique, des médias, des télécoms et de la recherche dans la gestion de leurs affaires au quotidien, pour leurs projets de croissance interne ou externe et leur développement à l'international. L'ensemble des avocats du cabinet IMA a reçu une double formation en complétant leur formation française soit par une formation à l'étranger soit par une formation en école de commerce. Chacun d'entre eux est tourné vers la nouvelle économie et la mondialisation des échanges accompagnant leurs clients avec une vision pragmatique de la vie des affaires.

5, rue de Monceau 75008 Paris - France
Tel : +33 1 42 89 19 80
Fax : + 33 1 42 89 14 99
www.ichay-mullenex.fr