Contribution au GSR 2012 : **Protection des Données Personnelles : Impossible dans le Cloud ?**

Les conclusions de l'étude que nous avons réalisée à l'UIT sur le **Cloud Computing** en Afrique (et qui sont à mon avis applicables à la majorité des pays en développement) nous appelles à agir le plutôt possible pour opérer les mises à niveau nécessaires sur les cadres règlementaires régissant les TICs afin de pouvoir réaliser le compromis adéquat entre les deux impératifs vitaux suivants, à la faveur d'un développement équilibré de l'usage des services des TICs, notamment après l'avènement et l'expansion rapide de la technologie Cloud Computing qui ne reconnait pas les frontières physiques.

1er impératif : Assoir un environnement d'affaires propice au développement de la technologie et de l'usage du **Cloud Computing** en limitant les barrières réglementaires afin de donner le maximum de chances aux entreprises de profiter des avantages économiques qu'apporte cette technologie (modularité des ressources hard et soft, disponibilité, facturation à l'usage …etc.) qui impacte directement la compétitivité de ces entreprises et leur positionnement dans le marché mondial.

En effet, outre l'ouverture directe sur le marché international, l'adoption de la technologie **Cloud Computing**, donne la possibilité aux entreprises de se passer des investissements lourds dans des ressources informatiques qui, de plus, nécessitent une gestion interne lourde et coûteuse.

2ème impératif : Assurer la libre circulation des données tout en protégeant les libertés et les droits fondamentaux des personnes et de leur vie privée.

Pour pouvoir réaliser cet équilibre ''juridique' entre ces deux impératifs, il est nécessaires d'identifier les aspects réglementaires qui entre en jeux dans cet exercice.
Les retours d'expériences que nous avons pu avoir à l'occasion de l'étude mentionnée ci-dessus et à l'occasion du Workshop sur le **Cloud Computing** organisé à Tunis par Tunisie Telecom et l'UIT en Juin 2012, nous permettent d'énumérer un certain nombre d'aspects touchant à la protection et à la souveraineté des données.
Les exemples considérés dans ce qui suit se réfèrent à l'expérience tunisienne dans ce domaine (loi organique n°2004-63 du 27 juillet 2004 portant sur la protection des données personnelles) telle que présentée par Mme HÉLA BEN MILED, magistrat, membre de l'Instance Nationale de Protection des Données Personnelles, à l'occasion du Workshop ci-dessus mentionné. Nous avons alors énuméré les aspects réglementaires fondamentaux qui doivent être bien cernés dans toute réglementation portant sur la protection des données personnelles. A savoir :

1. La Définition précise de ce qu'on convient d'appeler Données Personnelles. Par exemple : nom, prénom, date de naissance, adresse postale, adresse électronique, adresse IP d'un ordinateur, numéro de téléphone, numéro de carte de paiement, plaque d'immatriculation d'un véhicule, empreinte digitale, ADN, photo, numéro de sécurité sociale…etc.
2. La précision des cas et des situations pour les quels le traitement des Données Personnelles est autorisé (ou interdit). Ex : consentement, données ayant un aspect manifestement public, données nécessaires à des fins historiques ou scientifiques, données nécessaires à la sauvegarde des intérêts vitaux de la personne concernée…etc.

3. L'obligation de loyauté : cet aspect englobe aussi bien l'obligation d'information des personnes concernées et de leur permettre de s'opposer ainsi que l'obligation de mise à jour des données (les données doivent être toujours exactes).
4. L'obligation de sécurité et de confidentialité : Le responsable du traitement doit assurer la sécurité des informations traitées et empêcher les tiers de procéder à leur modification ou altération. De même le responsable du traitement doit adopter toutes les mesures nécessaires pour empêcher des personnes non autorisées d'avoir accès aux données, les lire ou les copier.
5. L'obligation d'Information : Le responsable du traitement doit informer au préalable et avant de commencer le traitement et par écrit les personnes concernées de la nature des données à collecter, des finalités du traitement dont leurs données personnelles peuvent faire l'objet, de leur droit d'accès, du caractère obligatoire ou facultatif de leur réponse, des conséquences du défaut de réponse, de leur droit de revenir à tout moment sur l'acceptation du traitement, de leur droit de s'opposer au traitement de leurs données, du pays le cas échéant vers lequel seront transférées leurs données personnelles.

A ces aspects d'ordre général, s'ajoutent des questions propres à l'introduction des services Cloud Computing, du genre :

1. Dans quel pays (ou quelle région) se trouve le fournisseur des services Cloud Computing ?
2. Est-ce que l'infrastructure utilisée (Data Centres) est située dans le même pays?
3. Est-ce que le fournisseur des services Cloud Computing est autorisé à utiliser une infrastructure localisée en dehors du pays du contrat?
4. Où est ce que les données vont être physiquement hébergées?
5. Est-ce que la juridiction compétente pour le contrat de services est la même que celle applicable pour la protection des données?
6. Est-ce que certains des services Cloud Computing offerts sont sous-traités localement ou ailleurs?
7. Quel va être le sort des données stockées dans le Cloud Computing à la fin du contrat?
8. A la fin de l'utilisation des ressources louées dans le Cloud Computing, quelle garantie pour la suppression totale des données avant la réaffectation de ces ressources ?
9. Est-ce que le client va avoir la possibilité de contrôler et de suivre le lieu de stockage physique de toutes ses données ?
10. Est-ce qu'il y a des garanties, pour les clients du Cloud Computing, que leurs ressources (serveurs hébergés) sont parfaitement isolées et non partagées ?
11. A la fin de l'utilisation des ressources louées dans le Cloud Computing, quelle garantie pour la suppression totale des données avant la réaffectation de ces ressources à d'autres utilisateurs ?

Afin d'assurer une évolution vers une réglementation capable de répondre à ce type de questionnement, il est recommandé aux pays d'adopter le plus tôt possible une nouvelle approche réglementaire qui tient compte du nouveau contexte découlant de l'utilisation des nouvelles technologies, telle que le Cloud Computing, et de considérer leur impact sur la sécurité et la confidentialité des données personnelles.
Une telle approche doit inévitablement sur la mise en place d'une coopération internationale et sur des accords mondiaux dans ce domaine afin d'éviter d'avoir des cadres législatifs et réglementaires incohérents ou contradictoires et aussi que les utilisateurs n'aient pas à se plier aux spécificités législatives de chaque Etat.
Il est aussi important d'avoir une bonne collaboration entre tous les acteurs: régulateurs, décideurs, operateurs, académies et industries.