Pourquoi une loi portant protection des données personnelles et une autorité de contrôle ?

Le monde entier connait de grandes mutations depuis ces deux dernières décennies. La mutation la plus emblématique, mais en même temps, la plus problématique est incontestablement la révolution du numérique. Problématique dans ce sens que c'est un univers complexe dont même les professionnels n'ont pas encore cerné tous les contours, à fortiori le consommateur non initié.

L'explosion de l'informatique et toutes les applications qu'elle permet a multiplié les moyens de collecte des informations et a accentué la possibilité de contrôle et de surveillance des personnes.

L'intensification de la collecte des données aboutit à une lecture plus aisée par les tiers de la personnalité de l'individu, de ses goûts ou encore de ses croyances, bref une connaissance parfaite de son intimité.

Dès lors, il devient plus facile ensuite d'utiliser ces informations contre lui ou plus simplement d'en tirer profit ; ceux qui vendent l'information sont les nouveaux riches de notre époque. C'est dire que les technologies de l'information et de la communication impactent l'exercice de nos droits et libertés.

Le développement des nouvelles technologies comporte insidieusement les risques de violation des droits fondamentaux de l'homme.

Alors comment prendre en compte les risques et dangers liés à l'utilisation des systèmes d'information ?

Comment protéger la vie privée des personnes dans ce monde envahi par l'internet et les autres TIC ?

Les risques qu'elles font peser sur nos vies privées sont assez graves s'il n'y a pas de garde-fou.

D'où le besoin de légiférer et de mettre en place un mécanisme indépendant de contrôle et de suivi de l'application des principes.

Pour ce faire, il y a lieu d'aborder, dans un premier temps, les risques de base des TIC, dans un second temps l'opportunité d'un mécanisme juridique de protection et enfin, la nécessité d'une Autorité de contrôle.

A. Les risques de base liés au mauvais usage des TIC

Une information relative à une personne, détenue par un tiers, est source de pouvoir ; or, numérisée, elle est beaucoup plus facile à manipuler : possibilité de stockage pendant longtemps par exemple dans une mémoire électronique, facilités de la copier sur une clé

USB, de la modifier par un programme/logiciel, de la divulguer sur un réseau ou de l'utiliser à une autre fin que pour celle pour laquelle on l'a établie.

Cependant, ces informations, dites « nominatives », touchent à l'identité des personnes concernées, à leur vie privée et, selon l'usage qui peut en être fait à l'aide des TIC, elles peuvent impacter l'exercice d'autres libertés ou droits fondamentaux : exemple de la liberté d'aller et venir (le portable est localisé (et par ricochet son détenteur) par l'opérateur de téléphonie pour pouvoir vous acheminer une communication ; il peut ainsi être utilisé le cas échant à d'autres fins).

Dès la fin des années soixante et le début des années soixante-dix, l'utilisation de l'informatique a soulevé très vite des inquiétudes, notamment l'utilisation faite par l'Etat et les administrations, seuls capables à l'époque de rassembler de grandes quantités d'informations sur les citoyens[1]. Le risque, à terme de voir l'Etat surveiller les moindres faits et gestes des individus et ainsi porter atteinte à leur droits et libertés a débouché sur l'adoption de législations protectrices, première garantie d'une protection des personnes à l'ère du numérique.

B. De la nécessité d'adopter une législation sur la protection des données personnelles

Parce que les traitements de données personnelles peuvent porter gravement atteinte à la vie privée des individus, il est nécessaire d'établir des principes préventifs, surtout que les traitements sont de plus en plus automatisés.

Aussi, les législations en la matière doivent énoncer les principes cardinaux pour le traitement des données personnelles, notamment les droits et obligations des personnes concernées. Ces principes, de nature préventive, doivent s'appliquer à tout type de traitement. Il s'agit entre autres principes de :

- **la finalité**: on ne peut collecter des données et les traiter que pour des finalités légitimes bien définies ;
- **la qualité des données** : on ne doit collecter que des données pertinentes et non excessives quant à la finalité définie. Par exemple, le fait de collecter des données sur la profession des parents dans une procédure de recrutement d'agents est disproportionné.
- **la durée de conservation :** on ne peut garder les données que le temps nécessaire à la réalisation de la finalité. Ce principe est particulièrement important à l'égard par exemple de la durée de conservation des données de géolocalisation des utilisateurs de téléphonie mobile.

[1] Confère le débat en France le projet de mise en place d'un système automatisé pour les fichiers administratifs et le répertoire des individus (Le Monde « Safari ou la chasse aux français », 1974)

- **la sécurité et la confidentialité des données** : il convient de traiter les données avec les mesures de sécurité aussi bien techniques que organisationnelles appropriées (code d'accès à la base de données par exemple) ;
- **la transparence à l'égard des personnes concernées** : respecter les droits des personnes dont les données sont traitées (droit à l'information sur la finalité poursuivie, sur les destinataires, droit d'accès aux données qui sont conservées, droit d'opposition, droit de correction en cas d'erreur, droit de suppression)

Il y a aussi que de nos jours, la protection des données personnelles est devenue une exigence démocratique. Elle participe à la consolidation de l'état de droit, en ce sens que les libertés individuelles et collectives dans un monde où le numérique a envahi tous les aspects de la vie de l'homme, doivent être protégées.

Encore bien plus, d'un point de vue économique, il y a un avantage certain pour les pays, surtout les pays qui cherchent à s'attirer des investisseurs, à se doter d'une législation sur les données personnelles. L'existence d'un cadre juridique à la protection des données personnelles contribue à améliorer le climat des affaires et assurer un espace juridique sécurisé pour les investisseurs et pour les citoyens-clients ; elle crée la confiance, permet une circulation aisée des données et est de nature à fluidifier les échanges économiques

Une chose est d'avoir adopté une législation, une autre chose est qu'elle soit mise en œuvre.

D'où la nécessité de créer une Autorité de contrôle, indépendante, dont la mission générale sera de promouvoir l'application des principes et de veiller au respect de la législation.

C. De la nécessité d'un mécanisme institutionnel de protection des données

Trois postulats peuvent être pris en compte :

- Le premier postulat est que les traitements de données nominatives sont peu « visibles » (dans les ordinateurs, les réseaux...) et peuvent être complexes et difficilement compréhensibles par les personnes concernées de par leur expérience.

- Le deuxième postulat est que les fichiers peuvent contenir des milliers de données, voire des millions de personnes, ce qui rend incontournable la création d'une Autorité de protection.

- Le troisième postulat est que les responsables de traitements qui détiennent des données nominatives ne peuvent demeurer, en toutes circonstances, juges et parties de l'application et de l'interprétation des principes édictés.

Il faut donc un mécanisme institutionnel d'interprétation et de contrôle car les principes prescrits en matière de protection des données sont généraux. Laisser mains libres les responsables de traitement n'assure aucune sécurité juridique, particulièrement dans les cas à risque (fichiers détenus par les administrations dans des registres, grandes bases de données médicales, etc...).

L'adoption seule d'une législation sur la protection des données personnelles ne saurait palier tous les risques liés aux traitements, au vu de l'évolution rapide des technologies.

Ce qui explique la création d'Autorités de protection pour veiller à ce que les applications de l'informatique ne portent atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles des citoyens.

Elles doivent être dotées de pouvoirs réglementaires et de sanctions, de pouvoir de recommandation et de contrôle sur tous les fichiers nominatifs.

Pour se faire, la mise en place des Autorités de contrôle doit présenter un certain nombre de garanties d'indépendance ; ces autorités doivent avoir une mission bien précise pour leur permettre d'atteindre leurs objectifs.

a) Des missions d'une autorité de contrôle ou de protection

Les missions d'une autorité de protection sont :

- d'informer les personnes de leurs droits et obligations, car la matière même est nouvelle avec le développement de l'informatique ;
- de donner des conseils les obligations des responsables de traitement (recommandations) ;
- d'assurer une veille technologique, c'est-à-dire suivre l'évolution des technologies et des pratiques en vue de saisir les pouvoirs publics d'un besoin de dispositions à prendre, de répondre aux demandes d'études et d'avis techniques aussi bien des juridictions que des pouvoirs publics ;
- de mener des missions de contrôle auprès des responsables de traitements de données ;
- de sanctionner en cas de non-respect des dispositions de la Loi et/ou de saisir la justice en cas d'infraction pénale ;
- etc.

b) La nécessité d'un organe indépendant

L'indépendance qui caractérise l'Autorité de contrôle se manifeste par :

- **la composition pluraliste :** dans la plupart des pays, les Autorités de protection comprennent des membres des hautes cours de justice, des parlementaires, des professionnels des TIC, de la société civile dans sa composante droits humains.

- **le mode de désignation des membres :** la désignation pourrait se fait par les structures d'origine de chaque membre, le plus souvent par élection.

- **les immunités dans l'exercice de leurs fonctions ;**

- **l'engagement solennel des membres** : les membres avant d'entrer en fonction prêtent serment ;

- **l'obligation de rendre compte : rapport annuel d'activités.**

CONCLUSION

Le développement fulgurant des technologies a accru les possibilités d'atteinte à la vie privée des individus. Il importe donc aux Etats de s'assumer en mettant en place un arsenal juridique et institutionnel protecteur des citoyens et garant des droits et libertés des citoyens dans le monde numérique.

Marguerite OUEDRAOGO BONANE
Présidente de la Commission de l'Informatique
et des Libertés (CIL) Burkina Faso