

**Séminaire sur le cadre juridique des technologies de l'information et de communication
au Sénégal organisé par l'Agence de l'informatique de l'Etat
Dakar 28-29 août 2005**

Communication

**La protection des personnes à l'égard des traitements nationaux et
internationaux de données à caractère personnel
- Les enjeux d'un nouveau droit fondamental -**

Alex TÜRK

Président de la Commission nationale de l'informatique et des libertés, France

Introduction : les difficultés majeures auxquelles nous sommes confrontés

« Informatique et libertés » : cette expression française pour désigner celle internationale, un peu malencontreuse, de « protection des données à caractère personnel », ne constitue pas une contradiction mais une exigence indispensable au fur et à mesure du développement fulgurant des technologies de l'information, tant celui ci devient central dans la vie de chacun : Internet, téléphones portables, administration électronique, biométrie.

Les difficultés majeures auxquelles nous avons à faire face tiennent tant à l'objet de l'informatique et des technologies de l'information et de communication, qu'au sujet, le droit.

**1. L'ambivalence, l'universalité et l'accélération de l'informatique, des
technologies de l'information et de communication**

Le progrès technologique est par son essence ambivalent, universel et en constante accélération.

- L'ambivalence des technologies

Les systèmes d'information véhiculent le meilleur. Ils permettent des gains de productivité fulgurants dans la gestion des organisations, en matière de communication et d'accès à l'information et aux services.

Ils présentent également des risques majeurs.

Par exemple, la biométrie apporte des services considérables pour protéger l'identité mais elle constitue également un énorme danger pour les libertés.

Les fichiers informatiques, si l'on n'y prend pas garde, peuvent être très facilement détournés de leur finalité ou conservés à l'insu des personnes concernées.

Il serait prétentieux de croire qu'on peut séparer ces deux aspects.

L'universalité

Les technologies sont universelles. Les frontières disparaissent, ce qui est positif.

Les ordinateurs personnels sont accessibles au plus grand nombre au quotidien pour des usages de plus en plus diversifiés, professionnels ou personnels.

Grâce aux fonctions de communication intégrées aux ordinateurs et à celles des ordinateurs intégrées dans des équipements de communication, il est possible d'utiliser de multiples applications en tout lieu, au plan national et au plan international.

Le fonctionnement des réseaux génère des traces de tous nos actes : achats à distance, consultation d'information de toute nature y compris politique, localisation du téléphone portable.

Autant d'informations qui touchent à notre droit à la vie privée ou à nos libertés fondamentales notamment de s'informer, de penser, de communiquer, d'aller et venir...

L'accélération des technologies

L'accélération des technologies est constante. A l'usage des grands ordinateurs par centaines s'est ajouté celui des micros-ordinateurs par milliers, ceux de l'Internet et des téléphones portables par millions.

Des puces électroniques sont intégrées de plus en plus aux milliards d'objets distribués et possédés. Demain elles dialogueront entre elles : pour quoi faire ? avec notre accord ou à notre insu ? combien de temps ?

2. Les difficultés tenant au droit et la recherche de solutions

Au regard de l'ambivalence des technologies le droit est univoque, au regard de leur universalité il est étroit, au regard de l'accélération constante dont elles sont le siège il est lent.

Universalité et textes internationaux

Pour répondre au défi de l'universalité, des textes ont été élaborés au plan international en même temps que les premiers textes nationaux: lignes directrices de l'OCDE (1980), convention du Conseil de l'Europe (1981), principes directeurs de l'ONU (1990), directive européenne (1995).

Pour répondre au défi de l'ambivalence et de l'accélération, tous ces textes établissent des principes préventifs des abus.

Elaborés dans la même période on y retrouve un minimum de principes communs.

Le texte de l'ONU et surtout les textes européens sont plus développés. Mais seuls les textes européens sont contraignants.

A ce jour, cinquante Etats dans le monde se sont dotés de législations dans ce domaine, la plupart au Nord, certains au Sud en particulier sur ce continent le Burkina Faso dont il convient de saluer le caractère précurseur.

La méthode au plan national

Au plan national trois voies ont été tentées, les deux premières ne sont pas satisfaisantes :

- la voie de la déontologie des professionnels de l'informatique. Parce que ces derniers sont des salariés, un régime de protection ne peut reposer sur eux seuls ;
- celle des législations spécifiques au fur et à mesure de l'apparition de scandales dans tel ou tel secteur d'activités, approche adoptée par les Etats-Unis d'Amérique. Elle n'est pas satisfaisante du fait des caractéristiques des techniques (ambivalence, universalité, accélération) ;
- enfin, celle de l'approche globale, ancrée dans les droits de l'Homme et posant des principes généraux, le cas échéant complétés par des dispositions spécifiques.

C'est cette dernière voie qui est la plus adaptée et la plus efficace. Elle repose sur quatre axes essentiels :

- la reconnaissance du droit à la protection des données personnelles comme droit fondamental,
- la mise en place de normes en droit positif,
- l'institutionnalisation d'une autorité de contrôle indépendante,
- la recherche de solutions pour les flux transfrontières.

I- La reconnaissance du droit à la protection des données à caractère personnel comme droit fondamental

La reconnaissance dans les textes et par les personnes de leur droit à la protection des données comme droit fondamental autonome n'est pas générale, même en Europe.

Le projet de traité pour une constitution de l'Union européenne l'avait prévue dans sa première partie sur les institutions et dans la seconde sur la charte des droits fondamentaux. Cette dernière demeure en tant qu'engagement.

En France, bien que le droit des personnes à l'égard du traitement des données personnelles ait valeur constitutionnelle au titre de la protection de la vie privée ou de la protection des libertés fondamentales, un cinquième seulement des Français connaissent leurs droits selon une enquête que nous avons réalisée il y a un an. Même dans les pays dotés d'une législation, un effort pédagogique très important est nécessaire.

Un certain nombre de pays dans le monde ont adopté des textes assurant une protection de même niveau qu'en France. En Europe, une directive adoptée en 1995 y tend. Le défi demeure important avant que tous reconnaissent ce droit nouveau comme droit fondamental.

On notera avec intérêt la déclaration adoptée à l'issue du Xème Sommet des chefs d'Etats et de gouvernement de la Francophonie réunis à Ouagadougou en novembre dernier qui vise

expressément le développement du droit des personnes, de leurs libertés et droits fondamentaux dans l'utilisation des fichiers et traitements de données à caractère personnel.

On notera également la déclaration de Cotonou adoptée à l'issue de la III^{ème} conférence ministérielle sur la culture de juin 2001 qui promeut une conception différente de celle des Etats-Unis d'Amérique, du droit d'auteur, de la propriété intellectuelle et des biens culturels qui ne sont pas des marchandises comme les autres.

Cette approche commune qui entretient des liens étroits avec la dignité humaine, les libertés fondamentales et les droits de l'homme constitue un point d'appui. La question se pose de l'opportunité d'insérer dans le corpus de Bamako une référence expresse à la protection des personnes à l'égard des données personnelles ce qui établirait une base juridique stable.

Il s'agit de promouvoir au sein de la Francophonie des valeurs communes qu'il convient de respecter tout en tenant compte de la diversité des systèmes juridiques.

Or ces valeurs ne semblent pas, en ce qui concerne la protection des personnes à l'égard du traitement de leur données, suffisamment explicitées dans la déclaration de principes du Sommet mondial sur la société de l'information publiée en mai 2004 qui privilégie une approche fondée sur la confiance et la sécurité des données ce qui paraît insuffisant (point 35).

Pour les pays non encore dotés d'une législation, l'opportunité est grande de sauter une étape : mettre en place à la fois le droit fondamental à la protection des données à caractère personnel et la législation qui le régit.

II- La mise en place de normes en droit positif

Il s'agit d'établir des principes de fond dont la combinaison vise à prévenir les abus en fonction des risques spécifiques présentés par les technologies et par là à encadrer le développement technologique, ce qui n'est pas le limiter.

Ces principes conduisent à des obligations pour ceux qui créent des traitements de données et à des droits pour les personnes.

Les principes

- **Le principe de finalité** : la finalité d'un traitement doit être justifiée et explicite. Il est interdit d'utiliser les données à d'autres fins que celles pour lesquelles elles ont été collectées, sauf consentement de la personne concernée. Ainsi par exemple il serait contraire au principe de finalité de collecter des données dans le cadre des opérations de recensement à des fins statistiques pour ensuite utiliser ces données à des fins policières. D'ailleurs si tel était le cas il est certain que la population tenterait d'échapper à l'obligation de répondre ou répondrait de manière fautive. On ne peut impunément collecter des données sur la vie privée des personnes aux fins d'une connaissance utile à toute la nation et vouloir ensuite l'utiliser contre elles.

- **Le principe de proportionnalité**, inclus dans les lignes directrice de l'ONU dans le principe de finalité, ou, selon l'OCDE, de minimisation de la collecte et de la conservation de données limitée à celles pertinentes au regard de la finalité légitime poursuivie. Serait-il normal, en effet, au moment de l'embauche d'un salarié de demander au candidat la profession de son père ou de ses frères et sœurs ? En général cette question est sans rapport avec les qualifications requises pour le poste à pourvoir. Dès lors de telles données ne peuvent être collectées.
- **Le principe de limitation de la durée de conservation des informations** : Les informations personnelles ne peuvent être conservées en mémoire éternellement car chacun a le droit à l'oubli. Il faut fixer une date de péremption en fonction de l'objectif assigné au fichier. Ce principe **est majeur notamment dans le domaine de la sécurité publique**, par exemple dans le cadre de la prévention de la **cybercriminalité**, sujet d'un atelier particulier au cours de ce séminaire. Ainsi, les États cherchent à créer l'obligation pour les fournisseurs de services de communication de conserver toutes les données de connexion de leurs clients. Afin d'éviter la société de surveillance, proscrite selon la jurisprudence de la Cour européenne des droits de l'homme, à laquelle une telle obligation pourrait conduire, il convient de cantonner cette durée de conservation à un strict minimum.
- **Le principe de loyauté et la transparence** : Les données personnelles ne doivent pas être obtenues ou traitées à l'aide de moyens illicites ou déloyaux. La transparence doit être assurée de deux manières
 - obligation de celui qui collecte des données d'informer de manière loyale les personnes concernées de la finalité poursuivie par la collecte de données, des destinataires des données, du caractère facultatif ou obligatoire des informations demandées ainsi que des conséquences éventuelles d'un défaut de réponse ;
 - obligation de déclarer les traitements avant leur mise en œuvre à l'autorité de contrôle qui en assure la publicité. A l'expérience, il apparaît que certaines catégories de traitement peuvent être dispensées d'une telle obligation
- **Le principe d'exactitude et de sécurité**. Les responsables de traitements de données doivent mettre en œuvre toutes les mesures techniques et d'organisation appropriées pour protéger les données. Ces mesures doivent viser à la mise à jour des données, à prévenir la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé aux données. On mesure l'importance de ce principe, par exemple, lorsqu'il s'agit de l'accès par Internet des médecins aux fichiers de leurs patients atteints du sida.
- **Principe du respect des droits de la personne**
 - **Droit d'information** : Toute personne peut s'adresser directement à un organisme pour savoir si elle est fichée ou pas.
 - **Droit d'accès** : Toute personne peut, gratuitement et sur simple demande, adresser à l'organisme considéré **une demande d'accès à l'intégralité des**

informations la concernant sous une forme compréhensible (les codes doivent être explicités) et en obtenir copie moyennant le paiement, le cas échéant, des seuls frais de reproduction.

- **Droit de rectification et de radiation :** Toute personne peut demander directement à un organisme détenant des informations sur elle que celles-ci soient **rectifiées** (si elles sont inexactes), **complétées** ou **clarifiées** (si elles sont incomplètes ou équivoques), **mises à jour** (si elles sont périmées) ou **effacées** (si ces informations ne pouvaient pas être régulièrement collectées).
- **Droit d'opposition :** Toute personne **peut s'opposer** à ce qu'il soit fait usage des informations la concernant à des fins publicitaires ou de prospection commerciale ou que les informations la concernant soient cédées à des tiers à de telles fins. Les personnes concernées doivent être mises en mesure d'exercer leur **droit d'opposition à la cession** de leurs données à des tiers dès la collecte des données. L'utilisation d'automates d'appels téléphoniques, de fax ou dans le commerce électronique, sujet d'un atelier particulier au cours de ce séminaire de messages électroniques à des fins publicitaires est interdite si les personnes n'y ont pas préalablement **consenti**.
- Certaines **données dites « sensibles »** touchent directement à l'intimité la plus profonde de notre personne - les données médicales - ou à nos libertés fondamentales, celles qui révèlent nos origines raciales, nos opinions politiques, nos convictions religieuses ou philosophiques, l'appartenance syndicale. Le principe en cette dernière matière est celui de la non discrimination, comme l'exprime l'un des principes directeurs de l'ONU. Dès lors, la collecte et la conservation des **données sensibles** font l'objet de garanties supplémentaires qui reposent notamment sur le consentement des personnes.
- Dans certains pays, notamment en France, la facilité avec laquelle on peut potentiellement effectuer **des tris, des interconnexions, établir des profils (autre risque de discrimination)** avec l'informatique, a conduit à des principes et droits complémentaires qui sont repris depuis 1995 dans la législation européenne sur la protection des données à caractère personnel.

III- L'institutionnalisation d'une autorité de contrôle indépendante

Outre, bien sûr, la possibilité qu'offrent les lois de protection des données, du recours à la justice en cas de dommages subis par la personne ou pour manquement aux obligations, le droit de la protection des données a fait émerger très tôt le besoin d'un mécanisme de mise en oeuvre spécifique sous la forme **d'une autorité administrative indépendante**, laquelle est prévue dans les principes directeurs de l'ONU, et est aujourd'hui consacrée par la Directive européenne et par la convention du Conseil de l'Europe.

Les réflexions qui ont conduit à prévoir une telle autorité sont les suivantes :

- La nécessité de la **transparence des traitements**, notamment ceux de l'administration, et d'en effectuer une évaluation du point de vue des droits fondamentaux avant leur mise en œuvre.
- La nécessité d'un organisme doté de **pouvoirs d'investigation et d'intervention**, en raison du besoin de réaction rapide en cas de plaintes, les fichiers pouvant concerner beaucoup de personnes, également doté au minimum d'un **pouvoir de médiation, voire d'injonction et de sanction**. Cet organisme, **distinct de la justice**, se doit donc de présenter des **garanties d'indépendance** face aux pressions économiques et politiques, à l'image de la justice elle-même.
- Enfin, une dernière idée, qui, à l'expérience, se révèle fondamentale, est la nécessité de disposer d'un organisme doté d'une capacité d'adaptation pour faire face à l'évolution des technologies et des pratiques.

L'expérience montre que **les enjeux institutionnels** tournent autour des trois points suivants, proposés à la réflexion : l'indépendance de l'autorité, son pluralisme, ses moyens d'action.

1. L'indépendance de l'autorité

L'indépendance de l'autorité est à l'évidence la clé du dispositif. En France elle a constitué un des points majeurs de discussion entre le Parlement et le Gouvernement français lors du débat parlementaire.

L'indépendance ne se décrète pas, elle se conquiert. Cependant certaines caractéristiques organiques sont nécessaires à son assise.

En cette matière, différents aspects sont à prendre en considération :

- l'affirmation dans la loi que l'autorité ne doit recevoir d'ordre de personne ;
- l'inamovibilité, la durée du mandat et l'impunité de ses membres ;
- la procédure (appel à candidatures ou non) et le mode de désignation de ses membres, par le parlement, le gouvernement, des corps constitués, la société civile ;
- l'indépendance financière de l'autorité (absence de contrôle a priori par l'exécutif mais contrôle a posteriori de la régularité des opérations, comme pour tout organisme public).

2. Le pluralisme et la collégialité de l'institution

Sans être un parlement, ni une juridiction, ni une société de conseil, l'autorité doit bénéficier grandement du pluralisme de sa composition : hommes politiques, magistrats, société civile.

Le pluralisme permet notamment la confrontation des idées dans une matière souvent prospective.

La collégialité garantit une prise de décision indépendante.

3. Les moyens d'action et les missions de l'autorité de contrôle :

Ce qui devrait guider la réflexion sur les missions et moyens d'action de l'autorité est ici l'effectivité recherchée de la protection dans un contexte marqué par la nouveauté, la rapidité d'évolution et l'impact des traitements de données sur un nombre potentiellement très important de personnes.

Ainsi, la grille suivante des tâches qui peuvent être confiées à l'autorité indépendante et des pouvoirs qui peuvent lui être conférés est proposée à la réflexion :

- **informer** les citoyens de leurs nouveaux droits et obligations (diffusion de documents, site Internet, participation à des conférences, réponse aux demandes de conseil) ;
- **tenir le registre des traitements déclarés** ;
- **rendre des avis** préalablement à leur mise en œuvre, sur les traitements qui comportent des risques particuliers, notamment dans le secteur public, voire être dotée d'un certain pouvoir réglementaire dans des matières sensibles ;
- **instruire les plaintes de particuliers** ;
- **effectuer des contrôles sur place** ;
- outre le pouvoir de **médiation** qui permet en général de résoudre la plus grande quantité des problèmes, il peut y avoir avantage à conférer à l'autorité le pouvoir d'adresser des avertissements, le **pouvoir d'injonction** et le pouvoir de **prononcer des sanctions pécuniaires** ;
- assurer la **veille et une mission de prospective**, technique et juridique, afin de faire émerger les questions nouvelles, animer le débat public à partir d'analyses tirées de l'expérience, proposer des voies d'arbitrage, publier des **recommandations** ou suggérer des adaptations législatives si nécessaire ;
- au plan international, **coopérer avec ses homologues**. Institutionnalisée au plan européen, la coopération s'est également « naturellement » développée au plan mondial grâce notamment à une conférence internationale organisée chaque année et aux contacts quotidiens. Une réflexion est menée actuellement pour développer un réseau des autorités francophones.
- disposer de la **liberté d'expression** pour rendre publiques ses observations, notamment dans le cadre d'un rapport annuel mais également à tout moment où elle l'estime nécessaire dans les relations internationales.

Le développement massif des traitements a conduit certains législateurs, dont le législateur français, à compléter le dispositif public par un autre, optionnel, de nature privé mais en relation avec l'autorité de contrôle publique qui est celui de l'institutionnalisation de « correspondants informatique et libertés » dans les entreprises et dans les collectivités locales.

IV- Comment traiter la question des flux de données transfrontaliers pour assurer au mieux la poursuite de la protection ?

Il y a des « paradis fiscaux ». Il peut y avoir aussi des « paradis des données », c'est-à-dire des pays dans lesquels des opérateurs sans scrupules pourraient trouver intérêt à l'absence de toute règle de protection des informations personnelles.

1. La nécessaire poursuite de la protection et la double fracture juridique au plan mondial

La mondialisation des échanges est accompagnée de flux de données personnelles.

Il s'agit de la gestion au sein des multinationales de leurs clients et de leurs personnels, mais également de l'insertion dans le marché international des pays émergents par des activités, par exemple, de centre appels opérant avec des fichiers de clientèle externalisés de grands groupes commerciaux établis à l'extérieur.

Il peut s'agir également d'Etats exigeant de disposer, par exemple, des dossiers de réservation de tous les passagers à destination de leur territoire.

Il ne servirait à rien d'établir des règles au plan national si à la faveur de tels transferts internationaux les données soumises à une protection dans leur pays d'origine étaient laissées libres d'usage dans le pays de destination.

Or, si une fracture numérique sépare encore trop les pays du Nord et ceux du Sud, la même que depuis de longues années le Président de la République du Sénégal s'attèle à réduire par des initiatives prises au plan international, une même fracture existe encore trop également au plan juridique.

Cependant la fracture se double au plan juridique, d'une autre fracture Est-Ouest qui complexifie largement le paysage.

En matière de transmission de données, bien logiquement le monde européen prévoit la poursuite de la protection à l'égard des traitement ainsi effectués hors des frontières, le monde américain le refuse ou l'ignore.

Il est particulièrement difficile de mettre en place une boîte de transformation pour animer l'articulation entre les deux systèmes.

Néanmoins, la stratégie juridique poursuivie dans le cadre de l'Union européenne paraît constituer une voie pragmatique intéressante au regard de certains résultats déjà atteints très positifs.

2. La recherche de solutions

Au plan national

Le principe, initié de manière pragmatique par la CNIL en France, a été repris au plan européen. Il consiste à prévoir un mécanisme de **reconnaissance de la protection adéquate dans les pays étrangers**. Celui-ci s'appliquera aux pays qui sont dotés d'une législation d'effet similaire à la loi nationale du pays d'origine et d'une autorité indépendante.

Lorsque le pays destinataire n'est pas doté d'un tel régime de protection, il peut être fait recours, sous le contrôle de l'autorité indépendante du pays d'origine, à des **solutions** contractuelles entre opérateurs, ou à **des règles effectivement appliquées au sein de l'entité destinataire**. Lorsqu'il s'agit de coopération inter-étatique qui suppose des flux réguliers de données, des conventions doivent être négociées pour assurer la poursuite de cette protection.

La pratique montre qu'**une telle approche est très dynamique**. Elle a incité dans le passé récent des Etats à adopter un cadre national de protection en vue de bénéficier de la reconnaissance d'un niveau de protection adéquat. Tel a été le cas notamment, **sous l'effet des dispositions de la directive européenne, du Canada et de l'Australie qui ont étendu le régime de protection applicable, à l'origine au seul secteur public, au secteur privé. Elle incite également les pays émergents à adopter un tel cadre pour apporter des garanties tant à leur nationaux que dans le cadre des activités de prestations de traitement de l'information de leurs opérateurs à destination de clients étrangers.**

Lorsque l'entreprise destinataire n'est pas soumise à une loi de protection, elle ne refuse pas de signer **un contrat** ou d'adopter **des règles internes** contraignantes **pour assurer une telle protection** aux salariés ou aux clients concernés, étant entendu qu'elle s'engage à coopérer avec l'autorité indépendante du pays d'origine des données. Cette approche est à rapprocher aujourd'hui de la démarche initiée par l'ONU en direction des entreprises en matière de codes d'éthique.

Au sein et par la Francophonie

Le développement des traitements à caractère transnational d'une part, et, d'autre part, le partage des valeurs communes qu'il convient de respecter tout en tenant compte de la diversité des systèmes juridiques nous conduisent à la conviction qu'au sein de la Francophonie nous avons mutuellement besoin des uns et des autres.

Il s'agit non seulement de développer et consolider le droit fondamental des personnes à la protection des données personnelles en vue notamment du développement des échanges harmonieux et respectueux des valeurs et de l'accompagnement des mesures de consolidation de l'Etat par l'informatisation, mais également pour poursuivre la promotion au plan mondial de solutions fondées sur la réflexion sur la diversité des systèmes juridiques.