Séquence 3 : Les données à caractère personnelle

Chapitre I : Les principes applicables au traitement des données à caractère personnel

Dans le souci d'harmoniser un cadre normatif universel afin de sauvegarder les droits et libertés fondamentaux de l'homme dans les applications informatisées, la communauté internationale, sous l'égide des Nations Unies, a adopté le 14 décembre 1990 par la résolution 45/95 du 10 décembre 1990, les Principes Directeurs pour le règlement des fichiers informatisés contenant des données à caractère personnel. Ces principes directeurs constituent en réalité les garanties minimales applicables à tous les fichiers informatisés publics et privés que chaque Etat doit prévoir dans sa législation interne. Ce fut le cas avec la loi n°2008-12 à travers ses articles 33 et suivants.

Dans le cadre de ce chapitre, notre préoccupation porte sur deux axes majeurs, notamment les principes relatifs à l'objet du traitement (Section 1) et les principes propres aux parties (Section 2).

SECTION I : LES PRINCIPES RELATIFS A L'OBJET DU TRAITEMENT

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.

- **Le principe de finalité** :

Aux termes de l'article 35 de la loi n°2008-12 « *les données doivent être collectées pour des finalités déterminées explicités et ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités* ».

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 fausse. 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.

Par ailleurs, le fichier de gestion administrative et pédagogique des étudiants ne peut être utilisé à des fins commerciales ou politiques.

Le principe de finalité est rappelé dans la loi d'orientation sur la société de l'information précisément à son article 9 aliéna 3 qui précise que « *tous les acteurs de la société de*

l'informatique doivent prendre des mesures appropriées, notamment préventives utiles pour promouvoir la paix et pour empêcher les utilisations abusives des TIC, par exemple la collecte de données à l'insu des personnes concernées ou le détournement de la finalité de données personnelles qui ont été légalement collectées ».

- **Le principe de proportionnalité** :

Le principe de proportionnalité trouve son siège dans l'article 35 alinéa 2, formulé en ces termes « *les données doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement* ».

Le principe de proportionnalité inclus dans les lignes directrices de l'ONU dans le principe de finalité, ou selon l'OCDE, de minimisation de la collecte et de la conservation de données limitées 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 générale cette question est sans rapport avec les qualifications requises par le poste à pouvoir. Des lors de telles données ne peuvent être collectées**.**

- **Le principe du consentement** :

L'article 33 de la loi 2008-12 pose le principe du consentement préalable en ces termes « *le traitement des données à caractère personnel est considéré comme légitime si la personne donne son consentement* ». Autrement dit selon cette disposition afin que le traitement ne soit pas entaché d'illégalité, il faut nécessairement le consentement préalable de la personne concernée. Les valeurs qui sous-tendent la démocratie et l'Etat de droit exigent que le citoyen dans sa vie privée bénéficie le maximum de protection par la loi.

Le responsable de traitement conformément à ladite loi est tenu d'informer la personne concernée pour qu'elle puisse donner son accord sur l'utilisation de ses informations personnelles dans le cadre d'un traitement.

En cas d'incapacité, la personne concernée peut être représentée par son avocat ou un membre de sa famille. Cette disposition montre l'importance que le législateur sénégalais accorde au respect de la vie privée de la personne. Le consentement préalable est donc, une condition sine qua none.

Toutefois, il peut être dérogé à cette exigence du consentement lorsque le traitement est nécessaire :

- Au respect d'une obligation légale auquel le responsable est soumis;
- A l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;
- A l'exécution d'un contrat auquel, la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ;

- A la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

Ces cas dérogatoires du consentement sont justifiés. Soient ils mettent en avant l'intérêt général (obligation légale du traitement) soit ils visent à protéger l'intérêt de la personne concernée.

- **Le principe de loyauté et la transparence** :

La collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse conformément à l'article 34 de la loi n°2008-12 du 25 janvier 2008.

Qu'est-ce à dire ? Sinon que 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.

- **Les principes applicables au traitement des données sensibles** :

En vertu de l'article 40 de la loi n°2008-12 « *Il est interdit de procéder à la collecte, et à tout traitement qui révèlent l'origine raciale, ethnique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, ou plus généralement celles relatives à l'état de santé de la personne concernée* ».

Cette disposition met l'accent sur l'interdiction de traiter ces données dites « données sensibles », celles-ci touchent directement à l'intimité la plus profonde de notre personne. Le principe de non-discrimination en est le sous bassement de cet article 40, principe prévu dans les instruments internationaux. Le principe 5 des Nations Unis affirme cette règle fondamentale du droit international des droits de l'homme : à savoir le principe de non-discrimination qui interdit la collecte et le traitement d'information pouvant engendrer une discrimination illégitime ou arbitraire notamment les informations sur l'origine raciale ou ethnique, la couleur, l'orientation sexuelle, les opinions politiques, les convictions religieuses et philosophiques mais aussi l'appartenance à une association ou un syndicat. C'est pourquoi, il est expressément prévu que les dérogations à ce principe ne pourront être autorisées par la loi que dans les limites de la charte Internationale des Droits de l'homme et les autres instruments pertinents dans le domaine de la protection des Droits de l'Homme et de la lutte contre les discriminations.

- **Les principes régissant les données médicales, les données relatives aux infractions, aux condamnations pénales et aux mesures de sûreté**

Ces catégories font parties des données dites données sensibles mais, elles ont leur particularité.

Selon l'article 42 LDCP « *le traitement des données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être mis en œuvre que par :*

- *les juridictions, les autorités publiques et les personnes morales gérant un service public agissant dans le cadre de leurs attributions légales.*
- *les auxiliaires de justice pour les stricts besoins de l'exercice des missions qui leur sont confiées par la loi ».*

Par ailleurs, l'article 43 dispose que *le TDCP à des fins de santé n'est légitime que lorsque la personne concernée a donné son consentement.*

Il ressort de ces deux dispositions que le caractère intime de ces catégories de données exige qu'elles soient collectées et traitées par des personnes dotées de compétences spécifiques dans les matières concernées en l'occurrence en matière criminelle ou médicale.

En aucun cas on ne doit se servir de ces fichiers contenant le casier judiciaire d'un ou des anciens détenus pour surveiller leur moindre geste dans leur vie quotidienne. Le but de prévention, et l'envie de surprendre « en flagrance » délit ne doivent pas favoriser l'avènement d'une société déshumanisée ou le désir de prévenir transforme l'homme en une machine prédestinée ayant renoncée à tout libre arbitre.

S'agissant du traitement des données médicales, le consentement de la personne est le garde-fou de tout abus. L'état de santé d'un patient ne peut être connu que par le médecin qui est tenu par les règles du secret professionnel.