SEMINAIRE INTERNATIONAL DE FORMATION DES CADRES DES AUTORITES AFRICAINES DE PROTECTION DES DONNEES PERSONNELLES

Ouagadougou, 10 et 11 juillet 2018

Salle de conférences Direction générale des douanes

THEME : Les principes standards de la protection des données personnelles (PDP)

OUEDRAOGO *Ahmed Hissène Ange Marie-Noel,*
SECRETAIRE GENERAL/CIL/ BURKINA FASO

PLAN

INTRODUCTION:

NAISSANCE DU DROIT A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL/DEFINITIONS DE CONCEPTS

I. LES MENACES DU DEVELOPPEMENT DES TIC SUR LES DONNEES A CARACTERE PERSONNEL, LES LIBERTES INDIVIDUELLES ET LA VIE PRIVEE

II. LES PRINCIPES STANDARDS DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

CONCLUSION

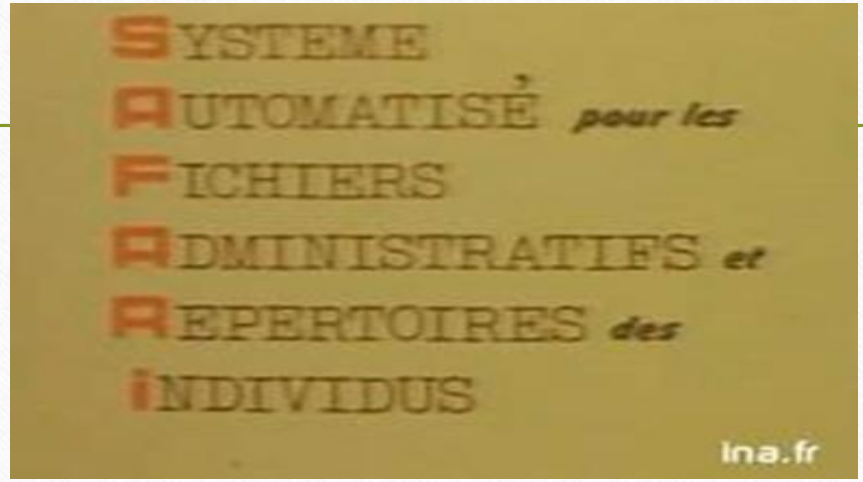
INTRODUCTION

Le Président de la République a chargé, par décret du 8 novembre 1974, une commission instituée auprès du Garde des Sceaux de « proposer au Gouvernement, dans un délai de six mois, des mesures tendant à garantir que le développement de l'informatique dans les secteurs public, semi-public et privé se réalisera dans le respect de la vie privée, des libertés individuelles et des libertés publiques ».

Ainsi était posé un problème que ne peut ignorer aucune société moderne éprise de liberté.

Mais de quoi s’agit-il?

- Il s’agit du projet SAFARI, qui veut dire



- Le 21 mars 1974, **Philippe Boucher** signe dans les pages « Justice » du quotidien « le Monde » un court article intitulé « SAFARI ou la chasse aux français » qui allait éveiller l´opinion publique et propulser la France au devant des nations sur les questions de libertés individuelles.

- En effet en 1974, le ministère de l'intérieur français avait tenté de créer un fichier informatisé au nom évocateur : **S.A.F.A.R.I.**, ce système prévoyait de créer une base de données centralisée de la population, en utilisant le fichier de sécurité sociale comme identifiant commun à tous les fichiers administratifs.
- Le tollé général qu'a suscité l'article de presse montre à quel point les menaces aux libertés individuelles, publiques et aux droits fondamentaux des citoyens étaient réelles.
- Et au-delà de la France, ce débat a été fondateur à l'échelle internationale (Conseil de l'Europe, Nations Unies) dans bien de pays en Europe et ailleurs.

QUELQUES DEFINITIONS

Donnée à caractère personnel

Il s'agit de toute information relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique psychique, économique, culturelle ou sociale.

La donnée personnelle peut donc être: Nom, prénom(s), Adresse, date de naissance, la photographie (l'image), le numéro de téléphone, le numéro d'immatriculation d'un véhicule…

Traitement de données à caractère personnel

Toute forme de manipulation ou ensemble d'opérations que l'on peut faire avec des données personnelles:

- la collecte des données,
- la conservation,
- la consultation,
- la modification,
- la communication,
- la suppression,
- le transfert,
- etc.

Responsable de traitement

Le responsable du traitement est celui qui décide de faire collecter des informations sur des personnes, de leur conservation, de leur communication à d'autres personnes, de leur modification, de leur suppression etc.

Il détermine les objectifs et les moyens de mise en œuvre de ce traitement de données.

Il peut être une personne physique ou une personne morale (une administration quelconque ou une entreprise).

Personne concernée

La personne concernée est la personne dont les données font l'objet de traitement.

I. LES MENACES DU DEVELOPPEMENT DES TIC SUR LES LIBERTES INDIVIDUELLES ET LA VIE PRIVEE

- Les menaces que font reposer les TIC sur les libertés individuelles, la vie privée sont de plusieurs ordres, et sans être exhaustif, on peut retenir:

La perte de contrôle des données

L'individu doit être maître de ses données alors que les capacités de stockage des données et les possibilités de calculs qu'offrent les TIC font que les données finissent par nous échapper.

Les risques liés aux Interconnexion des fichiers

- L'interconnexion des fichiers suppose la mise en relation et la centralisation de données de sources différentes sur les personnes et permettant aux responsables de traitements d'avoir accès à une quantité inimaginable d'informations avec tout ce que cela comporte comme risques d'abus. La vie privée se retrouve exposée.

Le déséquilibre des pouvoirs au profit des détenteurs des responsables de traitement

- D'ordinaire, une information relative à une personne, détenue par un tiers, est source de pouvoirs, or, numérisée elle est beaucoup plus facile à manipuler : on peut la stocker longtemps par exemple dans une mémoire électronique, la copier sur une clé USB, la modifier par programme/logiciel, la transmettre à d'autres ou l'utiliser à une autre fin que celle pour laquelle on l'a collectée.

- Ces informations personnelles touchent à notre identité, à notre vie privée et, selon les usages des TIC, elles peuvent aussi toucher à l'exercice d'autres libertés ou droits fondamentaux :
- Exemple de la liberté d'aller et venir (votre portable, et donc vous même, est localisé par l'opérateur de téléphonie pour pouvoir vous acheminer une communication et peut ainsi être utilisée le cas échant à d'autres fins), la liberté d'information (les requêtes d'information sur un moteur de recherche), la liberté d'association (fichier des adhérents à un parti politique) etc.

- Aussi la nécessité d'encadrer le développement de l'informatique dans le respect des droits de l'homme, de la vie privée et la dignité humaine s'est vite imposée. Et le débat suscité n'avait d'autres objectifs que de barrer la voie aux possibles atteintes arbitraires aux libertés individuelles et collectives.
- Les principes érigés à cet effet vont devenir universels et on les retrouve dans les textes de portée internationale et les lois nationales.
- Parmi les textes internationaux, on peut citer notamment:

La Déclaration Universelle des droits de l'homme (Art. 12)

- Les Principes directeurs pour la réglementation des fichiers informatisés contenant des DCP (ONU – Résolution 45/95 du 14 décembre 1990)

- La Convention 108 du CE du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des DCP
- Le Règlement général sur la protection des données (RGPD) de l'Union européenne (entrée en vigueur le 25 mai 2018)
- L'Acte additionnel A/SA.1/01/10 de la CEDEAO du 16 février 2010 relatif à la protection des données à caractère personnel
- La Convention sur la Cybersécurité et la protection des données à caractère personnel de l'Union Africaine de juin 2014

II. LES GRANDS PRINCIPES DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

- Les principes de la PDP sont élaborés dans le souci de protéger l'individu d'un usage pervers ou déviant de ses données surtout à l'ère du tout informatique.

- Ces principes sont les suivants:

Le principe de consentement et de légitimité

- Les données à caractère personnel (DCP) doivent être obtenues et traitées loyalement et licitement.

- Le traitement des DCP est considéré comme légitime si la personne dont on collecte et traite les données donne son consentement sauf si la loi nous autorise à le faire sans son consentement (dérogation).

Le principe de finalité

- La finalité, c'est l'objectif principal qui a guidé à la mise œuvre du traitement.
- Les informations qui concernent les personnes ne peuvent être recueillies et traitées que pour un usage déterminé et légitime.
- Les données ne doivent donc plus être utilisées de manière incompatible avec l'objectif déclaré.

Le principe de proportionnalité

- En vertu de ce principe les données doivent être adéquates, pertinentes, exactes et non excessives par rapport aux finalités pour lesquelles elles sont collectées.
- Et les données doivent être mises à jour régulièrement.

Le principe d'une durée limitée de conservation

- Les informations ne peuvent être conservées pour une durée illimitée. Elles doivent être conservées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées.
- La durée de conservation peut être déterminée en fonction de l'objet de chaque fichier (sauf si la loi la définit).
- Cependant, on occulte pas les besoins de conservation de longue durée pour des raisons historiques, d'archivage ou de statistiques.

Le principe de sécurité des données

- Des mesures de sécurité appropriées doivent être prises pour la protection des DCP enregistrées dans des fichiers automatisés contre la destruction accidentelle ou non autorisée, ou la perte accidentelle, ainsi que contre l'accès, la modification ou la diffusion non autorisés.

Le principe de confidentialité

- Tout responsable de traitement doit prendre les mesures nécessaires pour garantir la confidentialité des informations et éviter leur divulgation à des tiers non autorisés.
- le responsable du traitement doit veiller à ce que toute forme de manipulation ou de consultation soit exclusivement effectuée par des personnes habilitées qui agissent sous son autorité et sur ses instructions.

LE PRINCIPE DE L'INTERDICTION DE TRAITER DES DONNÉES DITES « SENSIBLES »

- Hormis les cas ou la **loi l'autorise** et en dehors du **consentement de la personne concernée**, il y a le principe **interdisant** la collecte et le traitement de données qui révèle:

- **l'origine raciale, ethnique ou régionale;**
- **les opinions politiques;**
- **les convictions religieuses ou philosophiques;**
- **l'appartenance syndicale;**
- **la vie ou les préférences sexuelles;**
- **les données génétiques;**
- **Les données relatives à la de santé des personnes;**
- **Les données à caractère personnel concernant les condamnations**

Le principe du respect des droits des personnes

- Les lois « informatique et libertés » accordent des garanties complémentaires pour les personnes concernées, et tout responsable de traitement doit s'y soumettre.
- Il s'agit notamment les droits suivants:

Le droit à l'information

Toute personne a le droit de savoir si elle est fichée et dans quels fichiers elle est recensée.

Ce droit de regard sur ses propres données personnelles vise aussi bien la collecte des informations que leur utilisation.

Le droit d'être informé est essentiel car il conditionne l'exercice des autres droits tels que le droit d'accès ou le droit d'opposition.

Les personnes concernées doivent être informées de la finalité du traitement, du caractère obligatoire ou facultatif de certaines informations demandées, des éventuels destinataires sous certaines conditions.

Le droit d'accès

- Ce droit postule que les personnes concernées ont le droit de connaître les données conservées et traitées qui les concernent auprès de toute personne ou organisme responsable de traitement.

On distingue:

- **- le droit d'accès direct**
- **- le droit d'accès indirect**

L'accès est direct si la personne concernée peut saisir directement le responsable du traitement.

L'accès aux données est indirect lorsque la personne concernée doit passer par l'autorité de protection des données pour exercer son « droit de curiosité ».

Le droit de rectification et de suppression

Ce droit est la conséquence du droit d'accès.

Il permet aux citoyens d'exiger du responsable la correction, la mise à jour, ou la suppression des données personnelles la concernant et qui sont inexactes, incomplètes, équivoques, périmées ou même celles dont la collecte, l'utilisation, la communication et la conservation sont interdites par la loi.

Le droit d'opposition

- Par ce droit, toute personne concernée peut, pour des raisons légitimes (risque d'atteinte à leur vie privée, manque de confidentialité, risque de divulgation), s'opposer à ce que des données la concernant fassent l'objet de manipulation.
- Sauf si le traitement de données présente un caractère obligatoire.

Le principe du respect des formalités préalables

Les traitements de DCP avant leur mise en œuvre doivent satisfaire aux formalités préalables en fonction du type de traitement.

Ainsi, les lois portant protection des données à caractère personnel établissent généralement trois **(03) régimes**:

- le régime de la **déclaration**;
- le régime de la **demande d'avis**;
- Le régime de la **demande d'autorisation**.

Le principe de sanction

- Toutes les lois portant protection des personnes à l'égard du traitement de leurs données à caractère personnel sont assorties de sanctions en cas de violation des principes et droits édictés.

- La violation de chaque principe fait l'objet d'une sanction spécifique. Il en est de même des droits.

Le principe de la création d'une Autorité de protection indépendante

- La mise en œuvre des principes repose sur l'existence d'une Autorité de protection des données indépendante dont les **missions de base peuvent être:**

  - Informer les personnes de leurs nouvelles obligations et de leurs nouveaux droits;
  - Conseiller sur la façon de remplir des obligations (recommandations);
  - Suivre l'évolution des technologies pour anticiper sur la réglementation;
  - Contrôler les traitements de données;
  - instruire réclamations et les plaintes ;
  - sanctionner pécuniairement et/ou saisir la justice en cas d'infraction pénale ;
  - coopérer avec ses homologues étrangers, notamment en cas de plainte concernant un traitements transfrontalier

Conclusion

- Les principes de la protection des DCP sont érigés pour éviter une informatisation incontrôlée des administrations, des organisations privées qui menacerait la vie privée et les libertés individuelles tout en accompagnant et encourageant l'innovation technologique.

Je vous remercie pour votre aimable attention.