THEME 1 : PROTECTION DES DONNEES PERSONNELLES AU BENIN ET GRANDS PRINCIPES DE LA PROTECTION DES DONNEES PERSONNELLES

PROFESSEUR : ZANNOU MARTIAL TIBURCE

ENSEIGNANT-CHERCHEUR À L'UAC

EXPERT DE L'AIEA EN DROIT NUCLÉAIRE

INTRODUCTION À LA PROTECTION DES DONNÉES PERSONNELLES

La question du traitement des données à caractère personnel apparaît comme un enjeu économique majeur. La quantité de données collectées augmente chaque année et sera au cœur de l'économie de demain.

L'évolution des nouvelles technologies permettant de recueillir, de traiter, de stocker, de rechercher et de diffuser des informations ; les traces que leur simple usage génère ; la valeur marchande acquise par les informations ; les fichiers se vendant d'autant plus cher qu'ils sont enrichis et permettant d'établir des profils ; le développement d'Internet, l'internationalisation des échanges concourent à une "libre circulation" des données personnelles, et doivent conduire les citoyens que nous sommes à une vigilance accrue du respect de la vie privée et des libertés individuelles. En cela, la protection des données personnelles est devenue un enjeu quotidien.

A. Sources, fondements et notions

Nous examinerons les sources et enjeux de la protection des données personnelles

1. Les sources

Les bases juridiques de la protection des données personnelles trouvent leurs origines dans les sources nationales et internationales.

Sources nationales

Au Bénin, la protection des données à caractère personnel est réglementée dans:

- *La constitution*
- la loi N° 2009 - 09 du 27 Avril 2009 modifiée par la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin et la loi 2020-35 du 06 janvier 2021.

Ce code du numérique a pour objet de régir :

- les activités qui relèvent des réseaux et services de communications électroniques ;
- les outils électroniques ;
- les services de confiance en l'économie numérique ;
- le commerce électronique ;
- la protection des données à caractère personnel ; et
- la cybercriminalité et la cybersécurité

Le siège de la protection des données est le livre 5ème. Ce livre est le bréviaire et le socle juridique de toutes les activités relatives à la protection des données. Il fixe un cadre légal de protection de la vie privée et professionnelle consécutif à la collecte, au traitement, à la transmission, au stockage et à l'usage des données à caractère personnel.

2. Notions et enjeux de la protection

Protéger les données personnelles, c'est empêcher que ces informations soient mal utilisées ou volées. C'est la protection de la sphère privée, le respect d'un droit fondamental, constitutionnel.

Il convient de savoir quelles sont les données personnelles à protéger. La notion de donnée à caractère personnel en particulier et celle de données en général, est abondamment évoquée dans le code qui y a apporté une clarification conceptuelle. On entend par :

- **Données à caractère personnel** : toute information de quelque nature que ce soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable, ci-après dénommée personne concernée. Est réputée identifiable, une personne qui peut être identifiée, directement ou indirectement notamment par référence à un identifiant, tel un prénom ou un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;

- **Données afférentes à la création de signature**: les données uniques telles que des codes ou des clés cryptographiques privées, que le signataire utilise pour créer une signature électronique sécurisée;

- **Données biométriques** : toutes les données relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique qui permettent son identification unique, telles que des images faciales ou des données dactyloscopiques

- **Données concernant la santé** : toute information concernant l'état physique et mental d'une personne concernée, y compris les données génétiques et la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

- **Données de création de cachet électronique** : les données uniques qui sont utilisées par le créateur du cachet électronique pour créer un cachet électronique ;

- **Données d'identification personnelle** : l'ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale ;

- **Données génétiques** : toute information concernant les caractères génétiques héréditaires ou acquis d'une personne physique qui donnent des indications uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ;

- **Données informatiques** : toute représentation de faits, d'informations, de concepts, de codes ou d'instructions lisibles par une machine, sous une forme qui se prête à un traitement informatique y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

- **Données relatives aux abonnés** : toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

  - le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;
  - l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;
  - toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services ;

- **Données relatives au contenu** : contenu informatif de la communication, c'est-à-dire le sens de la communication, ou le message ou l'information véhiculés par la communication. Il s'agit de tout ce qui est transmis dans le cadre de la communication en dehors des données relatives au trafic ;

- **Données relatives au trafic** : toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent ;

- **Données sensibles** : toutes les données à caractère personnel relatives aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle ou raciale, à la santé, à la génétique, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;

Tout l'enjeu de la protection des personnes est de tenter de donner à l'individu un contrôle sur la collecte et l'exploitation de ses données personnelles, même s'il s'agit d'un combat difficile, compte-tenu de la croissance exponentielle des moyens informatiques de collecte et de traitement mondialisés.

En créant un environnement qui place la protection des données au cœur des entreprises, et protège la capacité des personnes à contrôler leurs données, les entreprises pourront regagner la confiance des clients. Ceci peut être un avantage important pour attirer de nouveaux clients et retenir la clientèle existante.

Sources internationales

On distingue :

♦ La déclaration universelle des droits de l'homme (DUDH) en son article 12 stipule : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes. »

♦ Le Pacte international relatif aux droits civils et politiques (PIDCP), protège, en son art. 17, la vie privée, sans mentionner expressément la protection des données,

♦ La Directive européenne 95/46/CE du 24 Octobre 1995 « met en place un cadre réglementaire visant à établir un équilibre entre un niveau élevé de protection de la vie privée des personnes et la libre circulation des données à caractère personnel.

♦ La convention 108 du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Sources régionales et communautaires

♦ La convention de l'Union Africaine sur la cyber-sécurité et la protection des données personnelles adoptée le 27 juin 2014 au sommet de l'UA à Malabo en Guinée Equatoriale : vise à « renforcer et harmoniser les législations actuelles des Etats membres et à créer un cadre normatif approprié. Seuls huit pays (Bénin, Tchad, Congo, Guinée-Bissau, Mauritanie, Sierra Leone, Sao Tomé-et-Principe et Zambie) signataires et un seul (Sénégal) a ratifié la convention.

♦ CEDEAO : Acte additionnel A/SA.1/01/10 du 16 février 2010 relatif à la protection des données à caractère personnel : invite chaque Etat membre à mettre en place un cadre légal de protection de la vie privée .

♦ UEMOA : Article 3 alinéa 3. 2 de la Directive n°4/2006/CM/UEMOA du 23 mars 2006 relative au service universel et aux obligations de performance du réseau : « les Etats membres s'engagent à mettre en œuvre les dispositions législatives et réglementaires applicables en matière de protection des données à caractère personnel et relatives à la vie privée ».

♦ CEMAC : Directive N° 07/08-UEAC-133-CM-18 fixant le cadre juridique de la protection des droits des utilisateurs des réseaux et des services de communications électroniques au sein de la CEMAC (Communauté Economique et Monétaire de l'Afrique Centrale) -

♦La résolution A/RES/45/95 du 14 décembre 1990 sur les « principes directeurs pour la réglementation des fichiers personnels informatisés »

♦**La convention** de l'Union **Africaine** sur la cyber-sécurité et la **protection des données** à caractère personnel, adoptée le 27 juin 2014 à Malabo, en Guinée Equatoriale

♦L'Acte additionnel de la CEDEAO relatif à la protection des données à caractère personnel, adopté le 16 février 2010, d'application directe dans les Etats membres de la communauté.

A. Champ d’application

Le champ d’application d’une loi est la détermination des limites dans lesquelles cette loi s'applique. Le champ d’application du code (évoqué plus haut) est large mais puisqu’il s’agit de protection des données, nous nous y intéresserons spécifiquement. On distingue le champ d’application matériel et le champ d’application territorial.

1) Le champ d’application matériel et territorial

- **Champ d’application matériel**

Dans le jargon juridique fortement emprunt des expressions latines, l’expression "Ratione materiae" signifie "en raison des dispositions légales ou règlementaires qui règlent la matière »

La notion de compétence matérielle recouvre toutes les classes d’affaires dont un tribunal peut connaître. En d’autres termes, il s’agit de la compétence « s’appréciant en raison de l’objet du litige ». Chaque tribunal peut entendre une classe particulière d’affaires : des affaires liées à des litiges de droit du travail ; des affaires liées à l’interprétation ou à la violation de la constitution ; des affaires touchant au droit civil.

Sachant que le livre 5ème régit la matière de protection des données personnelles, l'article 380 abonde dans le même sens et précise que les dispositions du livre 5ème s'appliquent notamment à :

- toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation de données à caractère personnel par une personne physique, par l'État, les collectivités locales, les personnes morales de droit public ou de droit privé ;
- tout traitement automatisé en tout ou en partie, ainsi que tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier, à l'exception des traitements visés à l'alinéa 2 ;
- tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté et les intérêts essentiels de l'État, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur.

- ***Champ d'application territorial de la loi***

L'expression latine "ratione loci" signifie " en raison du lieu". Elle est employée dans les affaires dans lesquelles est soulevée un moyen portant sur la compétence géographique d'une juridiction

Aux termes de l'article 381, les dispositions du Livre 5ème s'appliquent au traitement des données à caractère personnel effectué dans le cadre des activités d'un responsable du traitement ou d'un sous-traitant sur le territoire de la République du Bénin, que **le traitement ait lieu ou non en République du Bénin.**

Les dispositions du livre s'appliquent au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de la République du Bénin par un responsable du traitement ou un sous-traitant qui n'est pas établi en République du Bénin, lorsque les activités de traitement sont liées :

1- à l'offre de biens ou de services à ces personnes concernées en République du Bénin, qu'un paiement soit exigé ou non desdites personnes ; ou

2- au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de la République du Bénin ;

3- le traitement est mis en œuvre sur le territoire d'un Etat membre de la CEDEAO.

Les dispositions du présent Livre s'appliquent au traitement de données à caractère personnel par un responsable du traitement qui n'est pas établi en République du Bénin mais dans un lieu où le droit de la République du Bénin s'applique en vertu du droit international public

Les Exclusions

Les dispositions du Livre 5ème ne s'appliquent pas aux traitements de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques lorsque ces données ne sont pas destinées à une communication à des tiers ou à la diffusion.

Ces dispositions ne peuvent restreindre :

1- des modes de production d'informations disponibles en vertu d'une loi pour une partie dans quelque procédure judiciaire que ce soit ;

2- le pouvoir des cours et tribunaux judiciaires de contraindre un témoin à témoigner ou de contraindre à la production de preuves.

II/ CADRE DE LA PROTECTION DES DONNÉES PERSONNELLES AU BÉNIN : HISTORIQUE, SOURCES JURIDIQUES (SPÉCIFIQUES, RÈGLEMENTATION ET CODE ÉTHIQUES DES PROFESSIONS ET ACTIVITÉS DE LA SANTÉ).

Les données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d'une personne physique (y compris la prestation de services de soins de santé) qui révèlent des informations sur l'état de santé de cette personne.

Le respect de l'éthique médicale constitue la meilleure garantie de la qualité des soins et de la liberté du malade ; il témoigne de la recherche d'une certaine forme de sagesse, de « science avec conscience », dans l'exercice de la médecine contemporaine.

Le code d'éthique sert donc de balise et de vecteur de transparence : il établit « les règles du jeu » afin de guider les rapports entre les membres d'un organisme, entre un organisme et des usagers et entre l'organisme et le public.

La cartographie des traitements de données personnelles permet de mesurer concrètement l'impact du règlement sur la protection des données de votre activité. Cela passe par le recensement de façon précise les traitements de données personnelles que vous mettez en œuvre ; et la tenue d'un registre des traitements.

La loi : Benin-Loi-2017-20-Portant-code-du-numerique-en-Republique-du-Benin (livre 5eme titre 2 chapitre II)

- Le traitement de données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, la religion ou les croyances, l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.

- L'interdiction de traiter des données à caractère personnel visées à l’alinéa 1 du présent article ne s'applique pas dans les cas suivants :

- le traitement est nécessaire aux fins de médecine préventive ou la médecine du travail, de diagnostics médicaux, de l'administration de soins ou de traitements soit à la personne concernée, soit à un parent, ou de la gestion de services de santé agissant dans l'intérêt de la personne concernée et le traitement est effectué sous la surveillance d'un professionnel des soins de santé ;

- le traitement est nécessaire pour des motifs d’intérêt public dans le domaine de la santé publique, tel que la protection contre les menaces transfrontalières graves pesant sur la santé, aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux sur la base du droit en vigueur, qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel ;

- le traitement est nécessaire à la réalisation d'une finalité fixée par ou en vertu des dispositions du présent Livre, en vue de l'application de la sécurité sociale ;

- le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l’article 396.

- Les données à caractère personnel visées à l’alinéa 1 peuvent faire l'objet d'un traitement aux fins prévues à l’alinéa 2, point viii, si ces données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit en République du Bénin ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit du Bénin ou aux règles arrêtées par les organismes nationaux compétents.

III/LES PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES PERSONNELLES AU BÉNIN

La transformation numérique modifie notre façon de travailler. De plus en plus, les équipes de marketing incitent les clients à interagir avec l'entreprise par la voie numérique au travers des médias sociaux et des applications mobiles, en plus des canaux de communication plus traditionnels comme Internet et la messagerie électronique. À mesure que la quantité d'informations partagées par les clients via les nouveaux canaux numériques augmente et que les applications d'entreprise qui traitent des données personnelles se déplacent vers le cloud, le risque de vol ou de fuite de ces données s'accroît. L'un des objectifs premiers du code du numérique est de réduire ce risque.

Avant de prendre des mesures pour parvenir à une totale conformité, les entreprises doivent faire en sorte de parfaitement comprendre les exigences qu'il fixe. Fondé sur les principes généralement reconnus en matière de protection de la vie privée, le code du numérique énonce dix principes fondamentaux :

A/ ***Les principes de licéité et de loyauté des traitements***

Aux termes de l'article 383, les données à caractère personnel doivent être :

1- traitées légitimement ;

2- collectées, enregistrées, traitées, stockées et transmises de manière licite, loyale, transparente et non frauduleuse ;

3- adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ;

B/ Le principe de transparence

Aux termes de l'article 384, le principe de transparence implique une information obligatoire et claire ainsi qu'intelligible de la part du responsable du traitement portant sur les données à caractère personnel.

C/ Le principe de la limitation de la finalité

- La finalité du traitement est l'objectif principal de l'utilisation de données personnelles. Les données sont collectées pour un but bien déterminé et légitime et ne sont pas traitées ultérieurement de façon incompatible avec cet objectif initial.
- La finalité du traitement fait partie des principes essentiels de la règlementation. Tout traitement de données se réalise en fonction d'une finalité déterminée, explicite et légitime.
- La finalité d'un traitement de données personnelles est le pourquoi, l'objectif de l'action qui a été mise en place sur des données personnelles.

Sens et types de finalités

Cet objectif doit être rédigé de façon très précise : on parle de finalité déterminée et explicite.

La finalité doit être déterminée, légitime et explicite :

L'objectif doit être légitime, c'est-à-dire respecter le cadre légal en vigueur et ne doit pas être modifié par la suite (on parle alors de détournement de finalité).

Enfin il est à noter le principe de La proportionnalité du traitement.

Le principe de la proportionnalité du traitement suppose que les données à caractère personnel qui ont été collectées sont bien en adéquation avec la finalité du traitement.

La proportionnalité est le lien permanent entre collecte et finalité.

D/ Le principe de la minimisation des données

Les organisations ne peuvent traiter les données personnelles que si cela est nécessaire aux finalités spécifiques pour lesquelles elles ont été collectées. Cela représente deux principaux avantages. Premièrement, en cas de violation de données, toute partie non-autorisée ayant accès aux données ne pourront voir qu'une quantité limitée de données. Deuxièmement, la minimisation des données permet de préserver l'exactitude des données et d'assurer leur mise à jour.

E/ Le principe d'exactitude des données

Le principe d'exactitude est étroitement lié à celui de transparence. Il prescrit à l'alinéa 5 de l'article 383 que les données doivent être exactes et, si nécessaire, mises à jour. Toutes les mesures raisonnables doivent être prises afin que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées ;

F/ Le principe de conservation limitée des données

Les données ne peuvent être conservées que pour une durée prédéfinie et limitée ; la finalité du traitement détermine la durée de conservation. A l'issue du traitement, les données sont soit anonymisées soit conservées pour une réutilisation ultérieure à des fins de recherche scientifique uniquement.

L'alinéa 6 de l'article 383 prévoit que les données soient << conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitées.>>

G/ Le principe de la responsabilité

Le principe de responsabilité est un principe commun pour les organisations dans de nombreuses disciplines ; le principe comprend le fait que les organisations répondent aux attentes, par exemple dans la fourniture de leurs produits et leur comportement à l'égard de ceux avec lesquels elles interagissent.

Le règlement général sur la protection des données intègre la responsabilité du responsable du traitement en tant que principe exigeant des organisations qu'elles mettent en place des mesures techniques et organisationnelles appropriées et qu'elles soient en mesure de démontrer ce qu'elles ont fait et son efficacité sur demande.

Les organisations, et non les autorités chargées de la protection des données, doivent démontrer qu'elles se conforment à la loi. Ces mesures incluent: des documents adéquats concernant ce sur quoi porte le traitement des données à caractère personnel ainsi que la façon dont le traitement est effectué, sa finalité et sa durée; des processus et procédures documentés visant à aborder les questions en matière de protection des données à un stade précoce lors de la création des systèmes d'information ou de la réponse à une violation des données; la présence d'un délégué à la protection des données à intégrer dans la planification et les activités de l'organisation, etc.

H/ Le principe de sécurité des données

L’alinéa 7 de l'article 383 prévoit que les données doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées.

I/ La protection des données de santé

Les données de santé sont des données personnelles et particulièrement sensibles et il est donc important d’assurer une protection forte de ces données afin d’assurer la sécurité de la vie privée des personnes concernées par ces données. Dans le cas plus particulier des données de santé, cette protection se doit d’être renforcée. Ces dernières années, le développement des TIC a facilité la collecte, l’archivage et le partage des données informatisées. Le législateur a rapidement réalisé qu’une cadre juridique strict devait être mis en place.

Le développement du numérique dans le domaine de la santé a profondément modifié la question de la protection des informations relatives aux patients en permettant de conserver des masses de données importantes, d'y avoir accès plus facilement et de les transmettre plus largement. L'accès à toutes ces données présente un intérêt majeur pour les tiers dits « intéressés ». Afin de préserver les droits et libertés fondamentaux, le traitement des données à caractère personnel a rapidement été encadré.

Du fait de leur lien étroit avec la personne concernée, les données de santé font l'objet d'une protection renforcée par rapport aux autres données à caractère personnel.

- **L'intermédiation d'un professionnel soumis au secret médical**
- **L'information du patient : Lors du recueil des données, il est primordial d'annoncer au patient quel sera le traitement destiné à ses données, qu'elles soient enregistrées dans un logiciel ou dans un dossier papier. L'information doit être précise, courte, transparente, facile à comprendre et aisément accessible.**

Elle doit être vulgarisée pour être comprise par tous. L'information doit être adaptée en fonction du patient, de sa pathologie, de la finalité de la collecte de ses données, de son âge, etc. afin d'être la plus transparente possible.

• La sécurisation des données : il est nécessaire d'assurer la protection des données de santé des patients. A ce titre, la protection des données contre des accès illicites ou non-autorisés, la destruction d'origine accidentelle, la perte, etc. doit être prévue grâce à la mise en place de mesure de sécurités adaptées telles qu'un mot de passe personnel, l'utilisation d'un système de chiffrement fiable, etc. De plus, si les données médicales sont hébergées via un hébergeur de données santé certifiée, il est essentiel de vérifier le niveau de sécurité garanti par ce dernier en concluant un contrat avec le prestataire.

MERCI POUR VOTRE ATTENTION