NOTIONS ET PRINCIPES FONDAMENTAUX DE LA PROTECTION DES DONNÉES PERSONNELLES

Cotonou le 05.05.22

Par Ambroise Dj. ZINSOU
Consultant formateur indépendant
Management Télécoms & TIC et Protection des données personnelles et de la vie privée

SOMMAIRE

I. Notions de données personnelles
II. Principes fondamentaux de protection des données personnelles

I. NOTIONS DE DONNÉES PERSONNELLES

1.1. **Définition**

Bien qu'il existe une loi qui traite des données personnelles au Bénin [**loi N° 2017-20 du 20 avril 2018 portant Code du Numérique en République du Bénin-Livre V^{ème}**] de nombreuses personnes ignorent encore ce que cela signifie réellement. Il n'y a pas de liste définitive expliquant quelles données sont qualifiées comme étant personnelles ou non, il s'agit donc de bien interpréter la définition du code.

Elle est définie comme « 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 »

I. NOTIONS DE DONNÉES PERSONNELLES

Cette définition est très large. En effet, dans certaines circonstances, l'adresse IP d'une personne, la couleur de ses cheveux, l'emploi, les opinions politiques peuvent être considérés comme étant des données personnelles.

Par contre le nom d'une personne seule n'est pas forcément considéré comme une donnée personnelle permettant de l'identifier puisque de nombreux individus peuvent porter le même nom. Cependant, si le nom est associé à d'autres informations (telles que l'adresse, le lieu de travail, le numéro de téléphone), cela peut suffire à identifier un individu.

Cependant, le fait de ne pas connaitre le nom d'un individu ne signifie pas qu'on ne peut pas l'identifier. En effet, il est identifiable en croisant d'autres informations le concernant

I. NOTIONS DE DONNÉES PERSONNELLES

1.2. Liste des données pouvant être considérées comme personnelles

- Les informations qui suivent peuvent être considérées comme personnelles, qu'elles soient seules ou associées à d'autres données :

- Nom et prénom, pseudonyme, date et lieu de naissance ;
- Photos, enregistrements sonores de voix ;
- Numéro de téléphone fixe ou portable, adresse postale, adresse e-mail ;
- Identifiant de connexion informatique ou identifiant de cookie ;
- Empreinte digitale, réseau veineux ou palmaire de la main, empreinte rétinienne ;
- Numéro de plaque d'immatriculation, numéro de sécurité sociale, numéro d'une pièce d'identité ;
- Données d'usage d'une application, des commentaires, etc.

I. NOTIONS DE DONNÉES PERSONNELLES

1. 3. **Identification des personnes à partir des données personnelles**

L'identification des personnes physiques peut se réaliser à partir :

- ❑ D'une seule donnée (exemple : nom et prénoms) ;
- ❑ Du croisement d'un ensemble de données [exemple : une femme vivant à telle adresse, née tel jour et membre de telle association].

1.4. Données personnelles sensibles [CDN page 26]

Sont considérées comme données personnelles 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** »

I. NOTIONS DE DONNÉES PERSONNELLES

Toutefois, le code dispose que 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 ne s'applique pas dans les cas cités à l'article 394 [points 1 à 15] du Code du numérique

II. PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES PERSONNELLES

Les grands principes de protection des données sont réaffirmés par le Livre Vème du CDN [art. 379, 383 à 391]. Chaque traitement de données à caractère personnel doit être analysé à la lumière de ces principes dès la phase de conception du projet, puis tout au long de sa vie. Cette analyse doit être documentée afin de répondre aux exigences de conformité et de responsabilité dictées par la loi N° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.

Les dispositions du Livre Vème du Code 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.

2.1. Principe de Responsabilité [Art. 387 du CDN]

Le principe de **Responsabilité** [l'*accountability* pour les anglo-saxons] est **une innovation majeure**.

Il porte sur une nouvelle façon d'appréhender la protection des données personnelles et le basculement d'un régime de formalités préalables statiques à un régime de conformité globale dynamique

II. PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES PERSONNELLES

Le principe de Responsabilité impose au responsable de traitement d'être en mesure de démontrer à tout moment lors d'un contrôle que les traitements mis en respectent l'ensemble des principes de protection des données personnelles définis par le Code [**Art.387 du CDN**] [. Pour ce faire, il se doit de documenter l'ensemble des démarches entreprises et produire la documentation en cas de contrôle. Le simple fait de ne pas être en mesure de produire la documentation qui atteste de la conformité est passible de sanctions alors même qu'il n'y a pas eu violation des données personnelles.

Ce principe se traduit notamment par :

- La définition d'une politique de protection des données et de sécurité des systèmes d'information ;
- L'obligation de mener l'analyse d'impact pour les traitements qui présentent des risques élevés ;
- La tenue d'un registre des activités de traitement ;
- La déclaration des violations de données personnelles si elle existe ;
- La prise en compte des principes de Privacy by design et Privacy by default. [art. 424 de CDN]

II. PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES PERSONNELLES

2.2. Les autres principes de protection des données personnelles.

Le responsable de traitement doit respecter les grands principes et doit être en mesure de les démontrer.

Ces principes sont :

- Licéité du traitement : une base légale explicitée.[**Art. 383 du CDN**]
- transparence du traitement respect des droits de la personne ; [**Art.384 du CDN**]
- Confidentialité et Sécurité des données : confidentialité disponibilité [**Art.385 du CDN**].
- Principe du consentement et de légitimité [**Art. 389 du CDN**];

II. PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES PERSONNELLES

2.2.1. Conditions générale **de licéité des traitements de données à caractère personnel [Art. 383.1 à .8 du CDN]**

i. Exigence du code :

Le Code exige que les données soient **« collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités …..»**.

La finalité correspond à l'objectif de traitement [ex : gestion des recrutements, de la paie, protection des biens et des personnes…].

Une même collecte peut répondre à plusieurs objectifs distincts (ex : soins/recherche).

Dans ce cas, les finalités doivent être :

- déterminées préalablement, ce qui exclut toute collecte de données au hasard ou à des fins préventives ;**explicites,** c'est-à-dire portées à la connaissance de la personne concernée de manière compréhensible et suffisamment claire ;
- **légitimes** au regard de la nature et à l'activité de l'organisme mettant en œuvre le traitement.

II. PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES PERSONNELLES

Les données à caractère personnel collectées doivent être :

- **Adéquates, pertinentes** et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées [**minimisation des données**];
- Exactes et, si nécessaire, mises à jour;
- 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.

ii. Compatibilité de la finalité de recherche scientifique avec une finalité initiale différente

Les informations recueillies pour une finalité peuvent être réutilisées pour poursuivre un autre objectif à condition que cet objectif soit compatible avec la finalité initiale.

Le Code du numérique pose une présomption de compatibilité des traitements ultérieurs avec les finalités initiales pour trois catégories de traitements [Art. 383.6 et 396 du CDN] :

- Les traitements à des fins de recherche scientifique ou historique ;
- Les traitements à des fins statistiques ;
- Les traitements archivistiques répondant à un intérêt public.

NB : Toute la réutilisation doit se faire dans les conditions prévues par la loi à savoir : Même si la compatibilité des finalités de recherche scientifique avec celles pour lesquelles les données ont été initialement collectées facilitent la réutilisation secondaire des données, elle ne dispense pas les chercheurs de respecter les conditions de licéité, d'informer les personnes concernées et d'obtenir une autorisation s'il y a lieu pour le nouveau traitement mis en œuvre.

2.2.2. Licéité du traitement

Les données à caractère personnel doivent être traitées de manière licite, c'est-à-dire autorisée par la loi

Pour être licite, un traitement de données doit reposer sur un des fondements juridiques énumérées par l'article 383.7 du CDN :

- **La personne concernée a consenti au traitement de ses données pour une ou plusieurs finalités spécifiques ;**
- **Le traitement est nécessaire à l'exécution de mesures contractuelles ou précontractuelles prises à sa demande ;**

Le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

- **Le traitement est nécessaire à la sauvegarde de la vie de la personne concernée ou d'une autre personne ;**

- **Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'autorité publique dont est investi le responsable du traitement ;**
- Le traitement est **nécessaire aux fins des intérêts légitimes** poursuivies par le responsable du traitement ou par des tiers, à moins que ne prévalent les intérêts et les libertés et droits fondamentaux de la personne concernée.

2.2.3. **Loyauté et transparence du traitement**

L'exigence de loyauté et de transparence renvoie à l'information des personnes concernées [**Art 437 à 451 CDN** relatif au Respect des droits des personnes concernées] et vise à éviter les traitements occultes ou cachés. Un traitement déloyal exposera son auteur à un risque de sanction.

2.2.4. **Confidentialité et de sécurité**

Les données à caractère personnel doivent être traitées de manière confidentielle et être protégées, notamment lorsque le traitement comporte des transmissions de données dans un réseau. [**Art. 385 du CDN]**

La sécurité des données a été érigée par le Code en principe de base de la protection des données. Cette exigence est donc renforcée. Les données doivent être « traitées de façon à garantir une sécurité appropriée des données à caractère personnel [...] à l'aide de mesures techniques ou organisationnelles appropriées ». [Art. 426 du CDN].

Cette obligation incombe aux responsables de traitement et aux sous-traitants qui doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté aux risques. Le caractère approprié des mesures de sécurité à mettre en place s'apprécie au regard :

- **De la nature, de la portée, du contexte et des finalités du traitement ;**
- **De l'état des connaissances, des coûts de mise en œuvre ;**

II. PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES PERSONNELLES

Des risques (probabilité et gravité) pour les droits et libertés des personnes.

La sécurité vise à garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement. Au nombre des mesures à mettre en œuvre, on peu citer :

- **La pseudonymisation et le chiffrement des données à caractère personnel (qui doivent être mis en place par défaut pour la recherche sauf justification) ;**
- **Le Plan de reprise et de continuité d'activité ;**
- **Les procédures d'audit**

Cette liste n'est pas exhaustive. Les mesures de sécurité doivent être revues régulièrement pour être ajustées en fonction de l'évolution des risques.

De cette obligation de sécurité découle l'obligation nouvelle de notifier à l'APDP certaines brèches de sécurité. Cette brèche devra également dans certains cas être communiquée à la personne concernée.[Art. 427 du CDN]

II. PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES PERSONNELLES

2.2.5. Principe du consentement et de légitimité [Art. 389 du CDN]

Le traitement des données personnelle est légitime si la personne concernée donne son consentement libre, spécifique, éclairé et univoque sauf dans les cas suivants :

- **l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique;**
- **l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande;**
- **la sauvegarde de l'intérêt ou des droits fondamentaux ou à l'intimité de la vie privée physique de la personne concernée.**

- **l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique;**
- **l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande;**

II. PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES PERSONNELLES

- **la sauvegarde de l'intérêt ou des droits fondamentaux ou à l'intimité de la vie privée physique de la personne concernée.**

Etc,

La personne concernée par le traitement peut retirer à tout moment son consentement sans compromettre la licéité du traitement fondé sur le consentement effectué avant ce retrait.[Art. 390 du CDN]

La durée de conservation est fixée par le responsable du traitement, toutefois certaines durées de conservation sont fixées par les textes législatifs et réglementaires.

Certains textes de lois imposent également aux organismes de conserver des informations (contenant des données à caractère personnel), pendant une durée précise [cas des institutions financières] , à des fins de preuve ou en prévision d'un éventuel contentieux jusqu'à la prescription de l'action en question. Les organismes sont donc dans l'obligation de les conserver bien qu'elles n'en aient plus aucun usage.

II. PRINCIPES FONDAMENTAUX DE PROTECTION DES DONNÉES PERSONNELLES

Le Code prévoit que les données soient “conservées sous une forme permettant l’identification des personnes concernées pendant une durée n’excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées” [Art. 383.6 du CDN]. Une dérogation est toutefois admise par le texte applicable à la recherche scientifique

JE VOUS REMERCIE