Leçon 3 : La protection des données à caractère personnel (PDCP)

Les progrès importants réalisés dans le domaine des technologies de l'informations et de la communication et de l'internet font que leurs utilisations inappropriées dans la vie quotidienne est susceptible de poser des problèmes dans la vie privée et professionnelle de ses utilisateurs. Aussi, une technologie comme l'internet et ses facilités de profilage et de traçage des individus constitue un vecteur favorable de collecte, de conservation, de traitement et de diffusion d'informations aussi sensibles que relatives à la vie privée en un temps record à travers le globe juste en un clic de clavier. Il s'avère alors évident que l'utilisation croissante des technologies de l'information et de la communication peut être préjudiciable à la vie privée et professionnelle des utilisateurs et/ou de nature à porter un coup sérieux à leurs image de marque et à leur réputation.

D'où la nécessité, face à de potentiels risques hautement préjudiciable aux utilisateurs des technologies de l'informations et de la communication, de soumettre la collecte, la conservation, le traitement et la diffusion des différentes informations personnelles à des règles de droit en vue de garantir une protection des données personnelles.

Ainsi, le droit des données à caractère personnel régit les problèmes créés par l'émergence de la société de l'information et vise principalement la protection de la vie privée rendue particulièrement vulnérable par la collecte informatique des données. Cette vulnérabilité est encore plus élevée en Afrique en raison de la fracture numérique.

I - La détermination des données à caractère personnel à protéger

En Côte d'Ivoire, la protection des données à caractère personnel fait l'objet d'une protection juridique sur divers fondements. Cette protection des données à caractère personnel puise ses sources, d'une part, dans le droit communautaire CEDEAO à travers l'Acte Additionnel A/SA.1/01/10 du **16 février 2010** relatif à la Protection des Données à Caractère Personnel dans l'espace CEDEAO adopté à Abuja au Nigéria à la 37ème session des Chefs d'État et de Gouvernement (CCEG). D'autre part, et sur le plan national, le régime juridique de la protection des données à caractère personnel est déterminé par la loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel.

Il faut bien se le dire, il semble en l'état actuel de l'évolution technologique impossible d'utiliser les TIC sans laisser aucune trace ou données personnelles en ligne. C'est dire que l'utilisation

des TIC est intimément liée à la collecte, au stockage et au traitement des données à caractère personnel. La protection des données à caractère personnel implique tout d'abord de définir les données à caractère personnel à protéger. Cela suggère ensuite de comprendre la mise en œuvre de cette protection.

1 - ***Définition légale des Données à Caractère Personnel (Côte d'Ivoire, CEDEAO)***

Conformément à l'article 1er tiret 17 de la loi 2013-450 relative à la protection des données à caractère personnel, une donnée à caractère personnel est définie comme « ***toute information de quelque nature qu'elle soit*** *et* ***indépendamment de son support****, y compris le son et l'image* ***relative à une personne physique*** *identifiée ou identifiable directement ou indirectement,* ***par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques****, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique* ». En réalité, cette définition législative ivoirienne a été reprise de l'Acte additionnel A/SA.1/01/10 du **16 février 2010** relatif à la Protection des Données à Caractère Personnel dans l'espace CEDEAO en son article 1er point 5.

Remarque : Une donnée à caractère personnel, c'est :

- *toute information de quelque nature que ce soit* (son et images, y compris) ;
- *peu importe le support* (physique ou virtuelle, papier, clef USB, Disque dur, cassette, téléphone, ordinateur, tablette, etc) *sur lequel repose l'information ;*
- *relative à une personne* ***physique (ce qui exclut les personnes morales)*** *;*
- *la personne concernée doit être identifiée ou identifiable, directement ou indirectement*
- *par référence* ***à un numéro d'identification ou à un ou plusieurs éléments spécifiques****, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique* ;

2 – ***Distinction avec des notion voisines ou proches***

Il convient de distinguer les données à caractère personnel d'autres notions proches ou voisines.

En premier lieu*, il faut distinguer* ***les données à caractère personnel*** *(DCP) des* ***données informatiques****.* En effet, les *données informatiques* sont constituées de « toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire exécuter une fonction par un système d'information »,

(Art.1er, tiret 18). Ainsi, si une DCP peut bien être une donnée informatique, toute donnée informatique n'est pas nécessairement une DCP. A preuve, une donnée informatique peut concerner des faits ou informations relatifs à une personnes morales ou même à une espèce animale ou végétale. De même, alors que les DCP peuvent reposer sur divers supports, les données informatiques sont caractérisées par le fait qu'elles se prêtent à un traitement informatique.

En second lieu, la loi 2013-450 relative à la protection des DCP mentionne les ***Données relatives aux abonnés***. Cette espèce spéciale de données est définie comme « *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 sur la base d'un contrat ou d'un arrangement de services* », (Art.1er, tiret 18). Notons que les *Données relatives aux abonnés* peuvent bien être des DCP si elles concernent des personnes physiques. Mais dès lors que des personnes morales peuvent être abonnées chez des fournisseurs de services, il n'est pas évident que toutes les données relatives aux abonnés soient des DCP.

En troisième lieu, la loi 2013-450 relative à la protection des DCP mentionne également les **Données relatives au trafic** qui sont définies comme « *toutes données ayant trait à une communication passant par un système d'information, 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* » (Art.1er, tiret 21). Les *Données relatives au trafic* sont distinctes des DCP dans la mesure où celles-ci ne sont pas relatives à une personne mais plutôt à un ensemble de données relatives à une communication dans un système d'information donnée (Par exemple le nombre d'appel, l'heure, la durée de l'appel des Ivoiriens de la Diaspora vers la Côte d'Ivoire) ; vers les données relatives heure d'appel).

Enfin, la loi 2013-450 relative à la protection des DCP particularise les **Données sensibles** par rapport au DCP. En effet, celles-ci (les *Données sensibles*) sont identifiées comme « *toutes données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives* », (Art.1er, tiret 21). Ainsi, les *Données sensibles* sont des DCP spécifiques traitant des données ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle ou raciale, à la santé, au sanctions (pénales & adm), etc.

II – La caractérisation du traitement des données à caractère personnel

Les données à caractère personnel sont susceptibles de faire l'objet de diverses utilisations. Ces diverses utilisations des données à caractère personnel (DCP) sont strictement règlementées de telles sont que leurs utilisations ne portent pas atteintes aux droits des personnes concernées c'est-à-dire les personnes dont les données sont utilisées. Cela suggère de mieux comprendre

1 – La définition du traitement des DCP

Constitue un traitement des données à caractère personnel en vertu de la loi 2013-450 (Art.1er, tiret 46), « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés ou non, et appliquées à des données, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction de données à caractère personnel* ». Cette définition est reprise de l'article 1er de l'Acte Additionnel de la CEDEAO relatif aux DCP.

Aussi, est-il important de relever que cette définition appelle deux observations.

En premier lieu, il convient de faire remarquer que la définition du traitement des DCP doit être entendu largement et de manière non limitative car les opérations ici indiquées ne sont qu'exemplatives et non exclusives.

En second lieu, le traitement des DCP dont il question peut se faire aussi bien par des *procédés électroniques* que par des *procédés analogiques*, c'est-à- dire notamment le traitement fait sur un support papier.

2 – Les catégories de traitements de DCP visées par la loi

En vertu de l'article 3 de la loi 2013-450, quatre catégories de traitements de DCP sont visées, il s'agit :

a) - *toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé* ;

b) - *tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier* ;

c) - *tout traitement de données mis en œuvre sur le territoire national* ;

d) - *tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de loi en vigueur*.

3 – Les catégories de traitements de DCP exclues par la loi

Conformément à l'article 04 de la 2013-450, les catégories de traitement de DCP ci-après sont exclues du du champ d'application de la loi :

a) - les traitements de données mis en œuvre par une personne physique *dans le cadre exclusif de ses activités personnelles ou domestiques*, à condition toutefois que les données ne soient *pas destinées à une communication systématique à des tiers ou à la diffusion* ;

b) - les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

c) – Il existe de manière implicite, une troisième exclusion à travers notamment « *les dérogations définies par des dispositions spécifiques fixées par des textes de loi en matière DCP relatifs à la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat » (art.3, 4ème tiret, in fine*).

III – Les formalités de protection des DCP

Il existe deux (02) formalités obligatoires prévues par la loi en vue d'assurer une protection des données à caractères personnel (DCP). Une troisième formalité est mentionnée par la loi ainsi que l'Acte Additionnel de la CEDEAO sans que son régime ne soit précisé.

1 – Formalité de Déclaration préalable

Il conviendra de voir d'une part l'obligation de déclaration préalable (A) et, d'autre part, les dispenses à l'exigence de déclaration préalable (B).

A - L'exigence d'une déclaration préalable avant tout traitement de DCP

Avant tout traitement de données à caractère personnel, le responsable du traitement ou son représentant légal est tenu obligatoirement de procéder à une **déclaration préalable** auprès de l'Autorité de protection des données à caractère personnel (article 5, loi 2013-450).
La déclaration comporte l'engagement que le traitement satisfait aux exigences de la loi.

L'Autorité de protection délivre un récépissé en réponse à la déclaration, le cas échéant, par voie électronique. Le demandeur peut mettre en œuvre le traitement dès réception de son récépissé ; il n'est exonéré d'aucune de ses responsabilités.

Les traitements relevant d'un même organisme et ayant des finalités identiques ou liées entre elles peuvent faire l'objet d'une déclaration unique. Les informations requises au titre de la déclaration ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

B – Les Dispenses à l'exigence de Déclaration préalable

En vertu de l'article 6 de la loi 2013-450, les traitements de DCP ci-après sont dispensés de la formalité de déclaration préalable auprès de l'Autorité de protection :
a) - le traitement de données utilisées par une personne physique dans le cadre exclusif de ses activités personnelles, domestiques ou familiales ;
b) - le traitement de données concernant une personne physique dont la publication est prescrite par une disposition légale ou réglementaire ;
c) - le traitement de données ayant pour seul objet la tenue d'un registre qui est destiné à un usage exclusivement privé ;
d) - le traitement pour lequel le responsable a désigné un correspondant à la protection des données à caractère personnel chargé d'assurer, d'une manière indépendante, le respect des obligations prévues dans la présente loi, sauf lorsqu'un transfert de données à caractère personnel à destination d'un pays tiers est envisagé.

2 – Formalité d'Autorisation Préalable

La formalité d'autorisation préalable est une exigence encore plus renforcée comparativement à la formalité de déclaration préalable. En effet, alors que la déclaration préalable ne nécessite pas une acceptation de la part de l'autorité de protection des DCP, la formalité d'Autorisation préalable requiert nécessairement de l'Autorité de protection une acceptation avant tout traitement des DCP. Aussi, certains traitements de DCP sont nécessairement soumis à la

formalité d'Autorisation préalable (A) devant l'autorité de protection, d'autres traitements font l'objet d'une procédure spéciale d'autorisation (B).

A – Les traitements soumis à Autorisation Préalable

Certains traitements de données à caractère personnel sont soumis à une **autorisation préalable** de l'Autorité de protection avant toute mise en œuvre. Au titre de ces traitements soumis à une autorisation préalable de l'Autorité de protection (ARTCI), l'article 7 de la loi 2013-450 mentionne sept (07) cas.

Il s'agit notamment des hypothèses de traitements de DCP ci-après :
- le traitement des données à caractère personnel portant sur des données génétiques, médicales et sur la recherche scientifique dans ces domaines ;
- le traitement des données à caractère personnel portant sur des données relatives aux infractions, aux condamnations ou aux mesures de sûreté prononcées par les juridictions ;
- le traitement portant sur un numéro national d'identification ou tout autre identifiant de la même nature, notamment les numéros de téléphones ;
- le traitement des données à caractère personnel comportant des données biométriques ;
- le traitement des données à caractère personnel ayant un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques ;
- le transfert de données à caractère personnel envisagé à destination d'un pays tiers.

Aussi, est-il particulièrement important de faire remarquer que les traitements de DCP soumis à une autorisation préalable relèvent tous de la catégorie des **données sensibles**. Ce qui semble alors caractériser le régime juridique des données sensibles par rapport aux autres données à caractère personnel.
En outre, il n'est pas vain de faire observer qu'en vertu du même article 7 de la loi 2013-450, la demande d'autorisation est présentée par le responsable du traitement ou son représentant légal. Enfin, il est utile de souligner que l'autorisation préalable délivrée par l'Autorité de Protection des DCP n'exonère pas le responsable du traitement sa responsabilité à l'égard des tiers.

B – Les traitements soumis à une procédure spéciale d'autorisation préalable

Outre les traitements de données à caractère personnel soumis à un régime d'autorisation préalable comme précédemment évoqués, d'autres traitements de DCP font l'objet d'une

procédure spéciale d'autorisation. En effet, conformément à l'article 13 relative à protection des DCP, les traitements de DCP opérés « ***pour le compte de l'Etat, d'une personne morale de droit public ou de droit privé gérant un service public*** sont **autorisés par décret**, *après avis motivé de l'Autorité de protection* ».

Ainsi, à la différence de l'autorisation préalable délivrée par l'Autorité de protection qu'est l'ARTCI, ici le caractère spécial réside dans le fait que c'est par décret que l'autorisation est délivrée. Toutefois, l'ARTCI qui est l'Autorité de Protection des DCP *n'est pas totalement écartée* dans la mesure où *un avis motivé de l'Autorité de Protection est nécessaire* avant que n'intervienne le décret d'autorisation.

Par ailleurs, le champ matériel de cette autorisation préalable spéciale est déterminé par la loi et ne peut concerner que les traitements portant sur :

- la sûreté de l'Etat, la défense nationale ou la sécurité publique ;
- la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;
- le recensement de la population ;
- le traitement de salaires, pensions, impôts, taxes et autres liquidations.

IV - Les principes directeurs du traitement des données à caractère personnel

Plusieurs principes régissent le traitement des données à caractère personnel. C'est dire qu'en cas de traitement des données à caractère personnel, le responsable du traitement est tenu au respect scrupuleux de ces principes. Ils peuvent être résumés autour de cinq (05) principes directeurs.

1 – Le principe de légitimité ou du consentement préalable

Tout traitement de données à caractère personnel **doit avoir reçu le consentement** de la ou des personnes concernée(s), sauf dérogations prévues par la loi (art.14, loi 2013-450). Un tel consentement doit être libre, éclairé et informé. L'article 23 de l'Acte additionnel CEDEAO pose également une telle exigence. **Toutefois,** il peut être dérogé à cette exigence du consentement préalable lorsque le responsable du traitement *est dûment autorisé* **et que** *le traitement est nécessaire* : **i**) - soit au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; **ii**) - soit à 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 ; **iii**) - soit à l'exécution d'un contrat auquel la personne

concernée est partie ou à l'exécution de mesures précontractuelles prises à sa demande ; **iv**) - soit à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

2 - Le principe de licéité et de loyauté du traitement des DCP

Ce principe posé par l'article 15 de la loi 2013-450 et 24 de l'article 24 Acte CEDEAO implique que *les données doivent être collectées et traitées de manière loyale, licite et non frauduleuse*. La licéité de traitement signifie que ce dernier doit respecter toutes les règles légales de protection des données. La loyauté de traitement suppose que la collecte et le traitement doivent se faire dans la transparence, c'est-à-dire que la personne concernée doit être informée de la finalité du traitement, de l'identité du responsable de traitement et des destinataires éventuels des données collectées. L'absence de fraude est une conséquence du principe de loyauté et exige du responsable de traitement de décliner le but réel et les moyens de traitement.

3 - Le principe de finalité

Le principe de finalité posé par l'article 16 de loi Ivoirienne sur les DCP et l'article 25 de l'Acte CEDEAO est un principe directeur essentiel dans la protection des données.

En effet, il faut noter qu'à travers la protection des traitements de DCP, plus que la nature des données, c'est qui importe davantage c'est le but dans lequel les données doivent être collectées et traitées. Tant il est vrai que c'est le but ou la finalité du traitement des DCP qui peut mettre à mal la vie privée. D'où la nécessité de veiller à ce que la finalité du traitement ne nuise pas aux personnes concernées. C'est pourquoi, la loi et l'Acte additionnel CEDEAO disposent que :

- *La finalité doit être déterminée, explicite et légitime* : le but du traitement des données doit être indiqué, clair et précis. Il doit être utile et nécessaire. Ainsi, il ne saurait y avoir un traitement de données sans finalité. De même, le but du traitement ne peut être implicite ou floue.
- *La finalité doit être proportionnée :* c'est-à-dire que le traitement doit être *adéquat, pertinent et non excessif* au regard des finalités pour lesquelles les données sont collectées et traitées ultérieurement. *La proportionnalité du traitement s'analyse aussi par rapport à la durée de conservation des DCP*. En effet, *les DCP ne peuvent être conservées que pour la durée nécessaire aux finalités de leurs traitements*. Au-delà de la période requise, les DCP ne peuvent être conservées que pour répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales.

4 – Le principe d'exactitude et d'actualisation (mise à jour)

Le principe d'exactitude et d'actualisation des données à caractère personnel prescrit par l'article 17 de la loi 2013-450 implique que « *les données collectées doivent être exactes et, si nécessaire, mises à jour* ». Par conséquent, il convient de noter que l'article 17 alinéa 2 dispose que « *toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement, soient effacées ou rectifiées* ». Il en résulte que le principe d'exactitude et d'actualisation des données renferme d'autres principes applicables à tout traitement de DCP. Il s'agit notamment du principe sinon de *l'obligation de l'effacement des données inexactes ou illégitimes* et de *l'obligation de rectification* des données incomplètes ou qui ne sont plus à jour.

5 – Le Principe de transparence

Le principe de transparence est prévu par l'article 18 de la loi 2013-450. Il implique une information obligatoire et claire de la part du responsable du traitement portant sur les données à caractère personnel.

6 – Le Principe de confidentialité et de sécurité

Le principe de confidentialité résulte de l'article 19 de la loi 2013-450. Il signifie que « les données à caractère personnel doivent être traitées de manière *confidentielle et être protégées*, notamment lorsque le traitement de ces données comporte des transmissions de données dans un réseau ». Aussi, il est important de noter qu'en vertu de l'article 20 de la loi 2013-450, lorsque le traitement des données à caractère personnel est mis en œuvre pour le compte du responsable du traitement, celui-ci doit choisir un sous-traitant qui apporte des garanties suffisantes pour la protection et la confidentialité de ces données. De même, il incombe au responsable du traitement ainsi qu'au sous- traitant de veiller au respect des dispositions de la loi.