L'URGENCE D'UN CADRE JURIDIQUE SPECIFIQUE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL AU CAMEROUN

Le 21ème Siècle est marqué par une démocratisation du e-commerce (vente en ligne). Celle-ci a connu une croissance exponentielle en 2020 en raison de la crise sanitaire mondiale Covid-19. L'ensemble des transactions (commerciales, administratives etc.) nécessitent désormais des plateformes dématérialisées et obligent les consommateurs à mettre à la disposition des marchands des données dites à caractère personnel.

Les « données à caractère personnel » sont entendues comme étant "toute information se rapportant à une personne physique identifiée ou identifiable (dénommée « personne concernée »)

Est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'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, économique, culturelle ou sociale."

Les exigences de transformation digitale et le développement des produits et services électroniques (plus innovants et plus personnalisés) accroissent le volume des données échangées au niveau mondial. Aussi, se pose la problématique de la collecte, du traitement, et de la sécurité des données à caractère personnel. Dans de nombreux Etats, les gouvernements au niveau régional ou national ont pris des mesures pour protéger les données à caractère personnel et palier aux risques d':

- ➔ e-réputation (ce qui se trouve sur Internet ne disparait pas, cybercriminalité, etc.)
- ➔ e-consentement (consentement pour la collecte et l'utilisation des données à caractère personnel)
- ➔ Atteinte aux droits de la personne humaine (atteinte au droit à la vie privée, au droit à l'image etc.).

1. ETAT DES LIEUX DU CADRE JURIDIQUE DE LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

I. AU NIVEAU MONDIAL

Les données à caractère personnel jouissent d'un cadre règlementaire au sein de l'Union européenne. Le Règlement Général de Protection des Données (RGPD) est un texte réglementaire adopté par le parlement européen (loi n° 2016/679 adoptée le 27 Avril 2016 par l'Union Européenne et entrée en vigueur le 25 mai 2018) qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne. Il s'applique également aux entreprises établies hors du territoire européen *« mais dans un lieu où le droit d'un État membre s'applique en vertu du droit international public »* - article 3 du RGPD (cas

du traitement des données à caractère personnel des ressortissants européens hors de l'Union européenne).

Il a été conçu autour de trois (3) objectifs :

- ➔ Renforcer les droits des personnes
- ➔ Responsabiliser les acteurs traitant des données
- ➔ Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.

Le RGPD encadre les droits de la personne concernée par le traitement des données ainsi que les obligations qui incombent aux responsables de traitement des données à caractère personnel. Quelques principes fondamentaux découlent du RGPD :

- ➔ **Le principe de finalité :** le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but bien précis, légal et légitime
- ➔ **Le principe de proportionnalité et de pertinence :** les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de la finalité du fichier
- ➔ **Le principe d'une durée de conservation limitée :** il n'est pas possible de conserver des informations sur des personnes physiques dans un fichier pour une durée indéfinie. Une durée de conservation précise doit être fixée, en fonction du type d'information enregistrée et de la finalité du fichier
- ➔ **Le principe de sécurité et de confidentialité :** le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient. Il doit en particulier veiller à ce que seules les personnes autorisées aient accès à ces informations (articles 32 à 34)
- ➔ **Les droits des personnes** (articles 13 à 21)

II. AU NIVEAU RÉGIONAL ET SOUS-RÉGIONAL

L'absence de cadre juridique spécifique à la protection des données personnelles dans certaines régions constitue un important défi pour sa régulation. Sur 54 pays en Afrique, 28 possèdent une législation sur la protection des données à caractère personnel (soit 52%), 9 pays disposent de projet de lois (soit 17%) et 13 pays n'ont pas de législation sur la protection des données à caractère personnel (soit 24%)[1].

L'Union Africaine a légiféré sur la protection des données à caractère personnel via la Convention de Malabo sur la cybersécurité et la protection des données à caractère personnel adoptée le 27 Juin 2014. Malgré des manquements observés comme l'absence d'une définition harmonisée de « donnée à caractère personnel » ou encore le régime des infractions et les sanctions appliquées. Elle définit en son article 13, les principes fondamentaux régissant le traitement des données à caractère personnel :

1. Le consentement du propriétaire des données à caractère personnel
2. La licéité des traitements

[1] - https://unctad.org/page/data-protection-and-privacy-legislation-worldwide?utm_source=newsletter&utm_medium=email&utm_campaign=Renforcement%2520de%2520la%2520protection%2520des%2520donn%25C3%25A9es%2520personnelles%2520en%2520Afrique%2520%253A%2520Une%2520urgente%2520n%25C3%25A9cessit%25C3%25A9

3. La finalité des traitements
4. L'exactitude des données à caractère personnel
5. La transparence des données à caractère personnel
6. La confidentialité des données à caractère personnel

Au niveau sous-régional, le Législateur a également adopté la 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. Elle vise « à garantir aux utilisateurs, un certain nombre de droits en termes de respect de la vie privée, de qualité et de permanence des services, d'information, de traitement des données à caractère personnel et de protection à l'égard de la cybercriminalité ».

Au Cameroun, le cadre juridique de la protection des données à caractère personnel ne s'arrime pas à l'évolution rapide de l'écosystème et la digitalisation des entreprises/administrations.

2. ÉTAT DES LIEUX DU CADRE JURIDIQUE DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL AU CAMEROUN

I. LOI N° 2010/013 DU 21 DÉCEMBRE 2010 MODIFIÉE ET COMPLÉTÉE PAR LA LOI N°2015/06 DU 20 AVRIL 2015 RÉGISSANT LES COMMUNICATIONS ÉLECTRONIQUES AU CAMEROUN

Cette loi ne traite pas des données à caractère personnel mais évoque la protection des données personnelles en son article 3. Il dispose que l'interopérabilité des réseaux et celle des équipements terminaux, ainsi que la protection des données personnelles doivent être garanties par l'établissement et l'exploitation des réseaux ainsi que la fourniture des services de communications électroniques.

II. LOI N° 2010/012 DU 21 DÉCEMBRE 2010 RELATIVE À LA CYBERSÉCURITÉ ET À LA CYBERCRIMINALITÉ AU CAMEROUN

Le législateur prévoit dans ce cadre, un ensemble de dispositions relatives à la protection des données à caractère personnel, notamment aux articles 26, 31, 35, 55, 66 ,67, 68, 69, 71 et 74 qui traitent des obligations et des sanctions relatives à la protection des données à caractère personnel. Ces obligations vont de l'accord préalable des concernés avant la conservation des données aux mécanismes à mettre en place pour leur protection, en passant par leur stockage et leur accessibilité au juge.

Cependant, l'absence de définition des données à caractère personnel dans la loi de 2010 pose des difficultés quant à sa compréhension par les responsables de traitement des données à caractère personnel. Par ailleurs, le champ d'application de cette loi se limite uniquement aux données traitées par les opérateurs de réseaux, les fournisseurs de contenus, les hébergeurs.

III. DÉCRET N° 2013/0399 /PM DU 27 FÉVRIER 2013 FIXANT LES MODALITÉS DE PROTECTION DES CONSOMMATEURS DES SERVICES DE COMMUNICATIONS ÉLECTRONIQUES

Ce décret a pour objectif de garantir les droits relatifs à la vie privée, à l'information et aux traitements des données à caractère personnel.

Le décret impose dans son Article 5 aux opérateurs de réseaux d'assurer la confidentialité des données à caractère personnel des clients. Toutefois, aucune définition n'est faite concernant les données à caractère personnel. L'Article 7 impose l'obtention du consentement du consommateur avant toute activité de prospection. Le décret s'attarde très peu sur les données à caractère personnel et met l'accent sur la qualité et la performance des services de communications électroniques, du règlement de litiges entre opérateurs et consommateurs, du droit des consommateurs relativement aux produits et services offerts.

3. INSUFFISANCES DU CADRE JURIDIQUE

I. ABSENCE D'ÉLÉMENTS SPÉCIFIQUES À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

- ➔ Le Cameroun n'a ni signé, ni ratifié la Convention de Malabo sur la cybersécurité et la protection des données à caractère personnel, ni un autre traité international traitant de la question (Convention de Budapest sur la cybercriminalité du 23 Novembre 2001).
- ➔ Le Cameroun ne dispose pas de cadre juridique spécifique à la protection des données à caractère personnel
- ➔ Le Cameroun ne dispose pas d'un organe institutionnel ou d'une autorité indépendante chargé de protéger les données et veiller au respect des principes fondateurs régissant la collecte, le traitement, le stockage des données à caractère personnel.

L'Agence Nationale des Technologies de l'Information et de la Communication (ANTIC) qui est le bras séculier de l'Etat en matière de régulation des activités liées à la sécurité des systèmes d'information, ne dispose pas de compétences effectives quant à la protection des données à caractère personnel. Le pouvoir d'investigation dont elle dispose est uniquement limité au cadre de la sécurisation des systèmes d'information des opérateurs de réseaux de communications électroniques ouverts au public.

L'ANTIC n'est pas une entité indépendante comme la Commission Nationale Informatique des Libertés (CNIL) en France (où 12 des 18 membres de la commission sont élus ou désignés par les assemblées ou les juridictions auxquelles ils appartiennent). La tutelle technique et financière de l'Agence pourrait constituer un handicap dans le déploiement de ses activités régaliennes.

II. LES INSUFFISANCES DU CADRE JURIDIQUE ACTUEL APPLIQUÉ À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

L'absence d'une définition de données à caractère personnel : le Décret n° 2013/0399 /PM du 27 février 2013 fixant les modalités de protection des consommateurs des services de communications électroniques évoque le traitement des données à caractère personnel sans

pour autant le définir. Le contenu et les éléments constitutifs des données à caractère personnel ne sont pas identifiés ni dans le Décret de 2013, ni dans la loi de 2010 sur la cybercriminalité.

En outre, le régime juridique actuel ne définit pas de cadre approprié pour la collecte, le traitement, la transmission, le stockage ou toute autre utilisation des données à caractère personnel. Les obligations des responsables de traitement des données ne sont pas élaborées, les droits des personnes dont les données sont sujettes à collecte ne sont pas définis (de quels recours disposent-elles en cas de traitement illicite ?).

4. QUELQUES OBSERVATIONS : CAS DE L'E-REGISTRATION AUX IMPÔTS, DE L'IMMATRICULATION À LA CNPS, DE L'ENREGISTREMENT SUR BLOOSAT POUR LES TESTS COVID-19 ET DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL PAR LES ASSUREURS

I. CAS DE L'IMMATRICULATION EN LIGNE (EREGISTRATION)

L'administration fiscale du Cameroun a mis à la disposition du contribuable une plateforme digitale (https://www.impots.cm) permettant d'accélérer certains actes fiscaux tels que la télé déclaration fiscale, l'obtention d'une attestation de non-redevance ou encore l'immatriculation en ligne (eRegistration). Il apparait cependant que les données d'immatriculation de tous les contribuables camerounais (y compris les données à caractère personnel) sont accessibles en libre accès depuis le site web de l'administration fiscale. Il s'agit ici de presque 2 millions de contribuables, pour lesquels les données ci-après sont accessibles (liste non exhaustive) : noms, prénoms, numéro d'identification unique (NIU). Parmi ces données, nombreuses sont celles qui seules ou combinées, permettraient à des individus malveillants de réaliser des actions illégales. En effet, les données à caractère personnel disponibles sur cette plateforme permettraient par exemple d'usurper l'identité des personnes physiques ou de réaliser des opérations de Phishing de masse. D'autant plus que cette plateforme est accessible depuis n'importe quel point du globe, donc à des hackers de tout horizon.

II. CAS DE LA PLATEFORME BLOOSAT E-SANTÉ POUR LES TESTS PCR COVID-19

La gestion de la crise sanitaire Covid-19 pose le problème de l'exploitation des données à caractère personnel. Concernant les tests de dépistage, plusieurs informations sensibles des personnes testées (noms, prénom, âge, numéro de téléphone, état de santé etc.) sont au préalable, collectées sur support physique (formulaire). Une plateforme (http://demo.bloosat.com/) en ligne est ouverte aux personnes testées, qui y ont accès via un code attribué lors du test Covid-19.

Cette procédure pose plusieurs problèmes :

- ➔ Le stockage des données à caractère personnel collectées sur support physique
- ➔ Le traitement de ces données : plusieurs données à caractère personnel sont disponibles et transitent par l'application WhatsApp ou sur des feuilles volantes pour des informations sensibles (avec une probabilité élevée d'erreurs humaines comme des codes mal saisis ou affectés à la mauvaise personne par exemple)

➔ La plateforme http://demo.bloosat.com/ n'est pas sécurisée et requiert des informations sensibles comme le numéro de CNI ou de passeport.

III. CAS DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL PAR LES ASSUREURS

Les assureurs traitent au quotidien des données à caractère personnel voire sensibles à l'occasion de leurs activités (nom, identifiant, dossier médical etc.). Cependant, il n'existe pas de base légale concernant leur protection. Les assurances santé, décès et épargne sont les principales qui appellent à une protection spécifique du fait d'importants flots de données qu'elles requièrent.

Le code CIMA (Conférence interafricaine des marchés d'assurance) qui régit les activités de l'assurance dans les régions Afrique centrale-Afrique de l'ouest, ne contient pas de dispositions sur la gestion des archives et le traitement spécifique des données à caractère personnel.

Malgré le vide juridique en la matière, la Direction Nationale des Assurances (DNA) exerce un contrôle sur le traitement et le stockage des données physiques d'assurance (avec l'obligation de ranger les documents dans une armoire scellée par exemple). Les assureurs s'imposent à eux-mêmes des règles en matière de traitement des données personnelles. Sur les règles et procédures écrites d'enregistrement et d'archivage, les assureurs sont tenus de *« conserver toutes les informations nécessaires pendant au moins 10 ans après la fin de la relation commerciale ou contractuelle (sous forme papier, informatique, microfiches, etc.) »* (Article 4.3 du Règlement n°0004/CIMA/PCMA/PCE/SG/08 définissant les procédures applicables par les organismes d'assurances dans les Etats membres de la CIMA dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme.

Cependant, les précautions prises par les assureurs s'avèrent limitées du fait de l'absence de cadre juridique (absence d'actions répressives à l'encontre des responsables indélicats du traitement des données à caractère personnel). D'où la nécessité de mettre en place un cadre approprié en matière de protection de ces données.

5. QUELQUES RECOMMANDATIONS

➔ Cartographier, avec le concours de tous les acteurs pertinents (y compris de la société civile) l'exhaustivité des données qui seront qualifiées de données à caractère personnel au Cameroun
➔ Mettre en place un système de données anonymisées dans la collecte de données confidentielles de manière à limiter la collecte de données propres à l'individu
➔ Accélérer l'élaboration d'une loi spécifique à la protection des données à caractère personnel. Laquelle devra se conformer aux standards internationaux en matière de protection des données à caractère personnel (RGPD)
➔ Mettre en place un organe indépendant chargé de l'application de ladite loi et de la sanction des responsables qui violent les principes de traitement des données à caractère personnel. Pour ce faire, l'on pourrait soit capitaliser sur les structures existantes en élargissant le domaine de compétences au contrôle de l'application de la loi sur la protection des données à caractère personnel, soit mettre sur pied une instance spécifique.

- ➔ Mettre en place des cadres de coopération en matière de régulation entre autorités de protection des données à caractère personnel de la sous-région
- ➔ Actualiser et harmoniser le cadre juridique de la protection des données à caractère personnel sur le plan de la sous-région Afrique centrale.

Une production de la commission économie numérique du GICAM

Avec les contributions de Inna Iberi (Evolving Consulting) et Frank Nzouetom (Mazars Cameroun).