Institut Mines-Télécom – IMT

Brevet d'aptitude délivré par les grandes écoles en Régulation des Télécommunications (Badge RegTel)

Promotion 2018-2020

EXPLOITATION DES DONNÉES À CARACTÈRE PERSONNEL : QUELLE APPROCHE DE CONFORMITÉ POUR LES OPÉRATEURS DE TÉLEPHONIE MOBILE EN GUINÉE ?

CAS DE MTN GUINÉE.

MÉMOIRE DE FIN DE FORMATION DE : Amadou Tidiane BARRY

DIRECTEUR DU MÉMOIRE : Yann BALGOBIN

Remerciements

Je souhaiterais adresser mes remerciements à mon employeur Areeba Guinée S.A (MTN Guinée) de m'avoir financé cette formation et m'accordé le temps nécessaire pour participer aux différentes sessions du Badge RegTel, session 2018-2020.

Je voudrais en plus remercier mon directeur Monsieur Labila Haba qui m'a toujours conseillé le long de cette formation et mon collègue Diemory Kouyaté qui a accepté sans se lasser d'assurer mon intérim à chaque fois que je devais m'absenter pour les besoins de cette formation.

Je voudrais enfin remercier mon directeur de mémoire Monsieur Yann Balgobin qui a toujours été disponible et qui m'a aidé dans mes recherches pour la préparation de ce mémoire.

Résumé

Le 26 juillet 2017, entrait en application la loi guinéenne sur la protection des données à caractère personnel pour les traitements mis en œuvre en Guinée. Moins d'un an après, le 25 mai 2018 précisément, le RGPD entre en vigueur et est applicable à des responsables de traitement même établis en dehors de l'Union européenne. À partir de cette deuxième date, les opérateurs mobiles de Guinée aussi des responsables de traitement, se trouvent être contraints à se conformer à deux différentes règlementations. Ce scenario nous amène à nous poser la question de savoir, quelle approche de conformité les opérateurs devront-ils suivre pour être en conformité à ces deux textes.

Mots-clés

Autorité chargée de la protection des données personnelles, Opérateur, Données à caractère personnel, Personne concernée, Règlement général sur la protection des données personnelles.

SIGLES ET ABRÉVIATIONS

BCR……Binding Corporate Rules

CIL……Correspondant Informatique et Liberté

CNIL…… Commission Nationale de l'Informatique et des Libertés

CEDEAO……Communauté Économique des État de l'Afrique de l'Ouest

CPDP……Comité de Protection des Données Personnelles.

DPD……Délégué à la Protection des Données Personnelles

DPC……Data Protection Champion

GSM……Global System for Mobile Communications

IMEI……. ……International Mobile Equipment Identity

RGPD…… ……Règlement Général sur la Protection des Données Personnelles

SMS……Short Messaging Services

Sommaire

INTRODUCTION

> « Il est devenu aujourd'hui lieu commun de dire que les données seraient le 'pétrole' du XXIe siècle. S'il serait sans doute correct de les comparer aux énergies renouvelables eu égard à leur caractère non exclusif, l'image a le double mérite, d'une part, de montrer que nous sommes en présence d'une nouvelle révolution industrielle et économique et, d'autre part, de rappeler la valeur susceptible d'être tirée de l'exploitation de ces données, laquelle peut se faire au détriment du respect de la vie privée des internautes. »[1]

Les responsables de traitement établis en Guinée ont depuis toujours développé des outils de traitement leur permettant d'utiliser les données personnelles de leurs clients à des fins commerciales et ce, dans le but de maximiser leur profil. On pourrait citer par exemple le scoring dans les banques et la segmentation de la base des abonnés chez les opérateurs mobiles. Cette approche n'est pas sans conséquence pour les personnes concernées. Dans ce schéma, le responsable du traitement se préoccupe peu des risques sécuritaires auxquels sont exposées les personnes concernées en cas de violation ou de fuite de données en raison de la précarité, voire l'inexistence de mesures de sécurité pour une meilleure protection des traitements et des données personnelles collectées. Ceci est aussi évident chez les opérateurs mobiles établis en Guinée qui traitent les données personnelles de plus de dix millions (10 000 000) de guinéens pour une population estimée à quatorze-millions trois-cent-neuf-milles et quatre-vingt-quinze personnes (14 309 095)[2].

La négligence des mesures de sécurité permettant de protéger les données personnelles collectées, peut ainsi exposer une grande majorité de guinéens à des risques financiers, réputationnels et sécuritaires.

Au cours du deuxième trimestre de l'année 2019, un opérateur guinéen a été victime d'hameçonnage. En effet, les employés de cette entreprise ont reçu un mail de la direction générale qui leur demandait de fournir leurs données bancaires pour des besoins de vérification à la suite de la mise à jour de la base de paie. Rassurés, beaucoup d'employés ont transmis les données demandées avant d'être informés que cette demande ne venait pas de la direction de l'entreprise. Cet évènement nous rappel la violation de données dont l'opérateur T-Mobile avait été victime en novembre 2019 à cause d'une faille de sécurité. Cette violation avait touché les données (noms, numéros de téléphone, adresses de facturation, numéros de

[1] Francis DONNAT, Droit européen de l'internet, Réseaux, données, services, avril 2018.

[2] https://countrymeters.info/fr/Guinea

compte T-Mobile de clients et des détails concernant des tarifs et des forfaits) de plus d'un million des clients de cette entreprise[3].

Ces fuites de données ne sont pas anodines, elles sont souvent le fruit du travail de hackeurs qui utilisent les données volées pour procéder à des attaques informatiques comme l'hameçonnage.

Pour éradiquer les risques auxquels les personnes concernées sont exposées, les opérateurs doivent impérativement mettre en place des mesures techniques et organisationnelles permettant de sécuriser les traitements qu'ils mettent en œuvre ainsi que les données qu'ils collectent. Ceci ne peut se faire sans l'implication des autorités étatiques.

C'est pourquoi, pour protéger les guinéens contre les risques redoutés dans le cadre du traitement de leurs données personnelles, l'État guinéen a adopté le 26 juillet 2016 la loi L2016/037/AN relative à la cybersécurité et la protection des données à caractère personnel pour le traitement de données personnelles en Guinée. Ce texte qui est encore à la traine pour des raisons économiques et potentiellement politiques, n'a jusque-là porter ses fruits. Le texte qui déclenchera plus tard la prise d'actions sérieuses pour la protection des personnes physiques à l'égard des traitements de leurs données personnelles en Guinée est le Règlement Général sur la protection des Données (RGPD) applicable à des responsables de traitement établis en Guinée depuis le 25 mai 2018. À partir cette dernière date, les responsables de traitement établis en Guinée à savoir les banques (utilisation de carte visa par un client en territoire européen) et les opérateurs mobiles (itinérance internationale d'un abonné en territoire européen) pour ne citer que ceux-ci, se sont vus obligés à se conformer à deux différentes règlementations.

Cette étude étant essentiellement axée sur le traitement des données personnelles par les opérateurs mobiles, il est important de se demander, quelle approche de conformité lesdits opérateurs devront suivre pour se conformer à la fois au RGPD et à la loi guinéenne sur la protection des données personnelles.

Pour y répondre, Il sera présenté le contexte guinéen de la protection des données à caractère personnel (I) avant de proposer un plan de mise en conformité prenant en compte les exigences de la loi nationale sur la protection des données personnelles et le RGPD (II).

[3] https://www.fredzone.org/t-mobile-des-pirates-ont-vole-des-donnees-de-plus-dun-million-de-clients-531

PRMIÈRE PARTIE I.

LE CONTEXTE GUINÉEN DE LA PROTECTION DES DONNÉES A CARACTÈRE PERSONNEL

Chapitre 1 :

LE CADRE RÈGLEMENTAIRE DE LA PROTECTION DES DONNÉES PERSONNELLES EN GUINÉE

L'adoption en Guinée d'une loi sur la protection des données à caractère personnel peut s'expliquer par deux raisons principales. Il s'agit du besoin d'avoir un cadre légal de protection des personnes physiques à l'égard des traitements effectués sur les données personnelles les concernant et la mise en application par l'État de ses engagements internationaux issus de conventions internationales et d'actes sous-régionaux comme l'Acte Additionnel de la CEDAO relatif à la protection des données personnelles.

Il est tout de même curieux de constater que les facteurs ayant conduit à l'adoption d'une règlementation sur les données personnelles en Guinée ne viennent pas d'une pression populaire comme ce fut le cas en France dans les années 1970[4]. Ce constat s'explique surtout par le manque de sensibilisation des populations sur les risques auxquels elles sont exposées à cause de leurs traces sur internet et l'étendu des informations que disposent d'elles, les opérateurs mobiles.

Ce premier chapitre sera consacré à la loi guinéenne sur la protection des données à caractère personnel (Section I) et d'autres cadres règlementaires qui, dans une certaine mesure, s'appliquent aux traitements de données personnelles effectués en Guinée (Section II).

[4] L'article de Philipe Boucher paru dans le Monde en 1974, SAFARI ou la chasse aux français a alerté l'opinion publique française et a donné naissance à la loi informatique et libertés en France.

SECTION I.

LA LOI L2016/037/AN RELATIVE A LA CYBERSÉCURITÉ ET LA PROTECTION DES DONNÉES A CARACTÈRE PERSONNEL EN GUINÉE

La loi L2016/037/AN dans sa deuxième partie, fixe les fondements légaux de la protection des données personnelles en Guinée.

En effet, cette loi institue une autorité chargée de la protection des données à caractère personnel. En son article 48, elle précise que cette autorité veille à ce que le traitement soit mis en œuvre conformément à ses dispositions ou toutes autres règlementations en vigueur en Guinée. En plus de l'exigence de formalités préalables avant la mise en œuvre d'un traitement, la loi met à la charge du responsable du traitement un certain nombre d'obligations et reconnait des droits pour les personnes concernées.

Après avoir défini une donnée à caractère personnel, il sera nécessaire d'aborder les formalités préalables à la mise en œuvre d'un traitement de données personnelles en droit guinéen.

Définition :

L'article 1er de la loi guinéenne relative à la protection des données à caractère personnel défini les données à caractère personnel 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, psychique, culturelle, sociale ou économique ».

§ 1. EXIGENCE DE FORMALITÉS PRÉALABLES

Alors que le RGPD abolit la quasi-intégralité des formalités préalables à observer avant la mise en œuvre d'un traitement pour un responsable de traitement établi au sein de l'Union européenne, la loi guinéenne maintient quant à elle l'observation desdites formalités avant la mise en œuvre d'un traitement de données personnelles sur le territoire guinéen.

I. Déclaration préalable

Par principe, le traitement de données à caractère personnel sur le territoire guinéen n'est possible qu'après une déclaration faite auprès de l'autorité en charge de la protection des données personnelles. Toutefois, cette déclaration ne dispense pas le responsable du traitement de ses obligations découlant de la loi sur la protection des données personnelles pour les traitements qu'il met en œuvre.

Dans sa déclaration, le responsable du traitement doit s'engager à mettre en œuvre son traitement conformément aux dispositions de la loi guinéenne sur la protection des données à caractère personnel et tous autres textes règlementaires en matière de données personnelles.

À la date de la rédaction de ce mémoire, les modalités de dépôt des déclarations auprès de l'autorité de protection n'étaient pas encore fixées par un texte règlementaire comme le prévoit l'article 13 de la loi guinéenne sur la protection des données à caractère personnel.

L'autorité de contrôle dispose d'un délai de deux (2) mois pour examiner et se prononcer (accord ou refus) sur une déclaration. Ce délai peut être prorogé de deux (2) mois supplémentaires sous réserve de motivation ou de justification de la prorogation par l'autorité de contrôle.

L'accord de l'autorité est matérialisé au travers d'un récépissé délivré au responsable du traitement.

Par ailleurs, la loi accorde une dérogation au principe de déclaration préalable avant la mise en œuvre d'un certain nombre de traitement. Il s'agit notamment, des traitements mis en œuvre dans un cadre exclusivement privé et des traitements dont leurs publications sont prescrites par une disposition règlementaire. S'ajoute à cette liste, les traitements pour lesquels le responsable du traitement a désigné un correspondant à la protection des données personnelles, qui de manière indépendante, veille au respect des dispositions de la loi sur la protection des données personnelles et tous autres textes règlementaires sur la protection des données personnelles en Guinée.

II. Autorisation préalable

Pour mettre en œuvre un traitement portant sur des données sensibles et des données d'infraction, le responsable du traitement doit obtenir l'autorisation de l'autorité en charge de la protection des données à caractère personnel.

En droit guinéen, la notion de données sensibles inclut les données d'infraction et est définie par l'article 1er de la loi sur la protection des données personnelles comme étant : « Toutes données à caractère personnel, relatives aux opinions ou activités religieuses, philosophiques, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ».

L'article 7 de la loi guinéenne sur la protection des données à caractère personnel établi une liste de catégories de traitement pour lesquelles une autorisation est requises.

§ 2. GRILLE DES DROITS ET OBLIGATIONS

Pour mieux protéger les personnes concernées contre tout abus dans le cadre du traitement des données personnelles les concernant, le droit guinéen leur accorde plusieurs droits et met à la charge du responsable du traitement un certain nombre d'obligations.

I. Droits des personnes concernées.

Le droit guinéen voudrait que les personnes concernées soient maîtres de leurs données personnelles et pour cela, elle met à leur disposition un certain nombre de droits qu'il y a lieu d'énumérer.

- Droit à l'information :

Le responsable du traitement doit informer la personne concernée de l'existence d'un traitement sur les données personnelles la concernant ainsi que les catégories de données sur lesquelles porte le traitement, de l'existence de traitements automatisés sur ses données personnelles ou non, de transfert de ses données vers un pays tiers et de la survenance d'une violation sur ses données personnelles dans un délai raisonnable.

- Droit d'accès :

La personne concernée doit pouvoir accéder à l'ensemble des traitements effectués sur les données personnelles la concernant sans que le responsable du traitement n'y fasse obstacle.

- Droit d'opposition :

La personne concernée ne doit pas se voir obliger de faire l'objet d'un traitement. Elle doit pouvoir s'opposer à ce qu'un traitement soit effectué sur les données personnelles la concernant. Le fait pour la personne concernée de s'opposer à un traitement ne donne pas par principe le droit au responsable du traitement de la priver d'un service.

- Droit de rectification :

Lorsque la personne concernée constate que les données personnelles la concernant sont incomplètes, non à jour ou ne sont pas correctes après avoir exercé son droit d'accès, elle peut exiger du responsable du traitement la rectification desdites données personnelles afin qu'elles reflètent sa situation réelle et actuelle.

- Droit au verrouillage des données :

Le verrouillage des données personnelles dans le droit guinéen correspond en pratique au droit à la limitation des données personnelles (RGPD : Art-18) et permet à la personne concernée de demander au responsable du traitement de rendre inaccessible (pour le public) et de surseoir (pour le responsable du traitement et éventuellement son sous-traitant) la totalité ou non d'un traitement.

Ce droit peut être exercé par la personne concernée lorsqu'elle conteste l'exactitude de ses données personnelles (i) le temps pour les parties de vérifier les données personnelles contestées, lorsque le traitement est illicite (ii) et que la personne concernée s'oppose à leur effacement mais à la place demande que les données soient verrouillées, lorsque le responsable du traitement n'a plus besoin des données (iii) aux fins d'un traitement mais les données sont nécessaires pour la personne concernée pour constater, exercer ou de défendre un droit en justice, et enfin lorsque la personne concernée exerce son droit d'opposition (iv), les données doivent être limitées en attendant de vérifier si les motifs légitimes poursuivis par le responsable du traitement n'affecte pas la vie privée et les libertés de la personne concernée.

- Droit à l'oubli numérique :

La loi guinéenne sur la protection des données personnelles permet à la personne concernée d'exiger du responsable du traitement que soient supprimées de bout en bout les données personnelles la concernant. Une fois lesdites données supprimées, le responsable du traitement ne doit plus procéder à un traitement ultérieur desdites données.

- Droit à la portabilité :

Dorénavant, la personne concernée peut, pour les traitements automatisés et basés sur son consentement, demander que lui soient communiquées dans un fichier structuré, les données personnelles la concernant (les données personnelles fournies par elle-même ou générées du fait de ses activités) pour transmission à un autre responsable de traitement. Cette demande doit être facilitée par le responsable du traitement recevant la demande qui ne peut en aucun moment opposer un refus à la personne concernée.

- Droit au déréférencement :

Le droit au déréférencement permet à la personne concernée de demander au responsable du traitement (moteurs de recherche), de supprimer des liens menant sur des informations la concernant sous certaines conditions.

II. Obligations du responsable de traitement

Le responsable de traitement est tenu à deux obligations principales[5]. Il doit mettre en œuvre des mesures techniques et organisationnelles appropriées (obligation de moyens) et être en mesure de démontrer que les traitements mis en œuvre sont conformes à la loi informatique et libertés (obligation de preuve). En droit guinéen, c'est le chapitre X de la loi sur la protection des données à caractère personnel qui traite des obligations auxquelles sont soumis les responsables de traitement.

1. Obligations portant sur le traitement

C'est l'obligation de mettre en œuvre un traitement licite (i), loyal et transparent (ii), sécurisé (iii) et enfin l'interdiction par principe du traitement des données sensibles (iv).

i. Licéité du traitement :

Pour qu'un traitement soit licite, le responsable du traitement doit obtenir le consentement de la personne concernée. A défaut, le traitement doit être nécessaire.

[5] Francis DONNAT, Droit européen de l'internet, Réseaux, données, services, avril 2018.

- Le consentement de la personne concernée

Le consentement doit être claire, libre et univoque à travers un acte positif avant qu'il ne soit entrepris un traitement sur les données personnelles.

- La nécessité du traitement

Dans certaines circonstances, le responsable du traitement peut passer outre le consentement de la personne concernée et procéder au traitement à condition qu'il soit nécessaire.

Pour que le traitement soit nécessaire, il doit être :

- mis en œuvre pour l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles à l'initiative de la personne concernée,
- mis en œuvre pour le respect d'une disposition légale à laquelle le responsable du traitement est soumis,
- mis en œuvre aux fins des intérêts légitimes poursuivis par le responsable du traitement sans qu'ils ne prévalent sur la vie privée et la liberté de la personne concernée,
- mis en œuvre pour la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique,
- mis en œuvre pour l'exécution d'une mission d'intérêt public ou qui relève d'une telle mission dont le responsable du traitement est investi.

ii. Loyauté et transparence du traitement :

La personne concernée doit être informée de l'existence d'un traitement sur les données personnelles la concernant et des droits dont elle bénéficie conformément à la loi.

iii. Sécurité du traitement :

Le traitement doit être sécurisé. Le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté aux risques qui peuvent survenir sur le traitement.

L'approche de sécurité doit être basée sur le risque. Cette approche voudrait que les mesures de sécurité soient renforcées en fonction du danger potentiellement redouté sur la vie privée et la liberté des personnes concernées.

iv. Interdiction par principe de traiter des données sensibles.

Le traitement des données sensibles est par principe interdit en droit guinéen.

Toutefois, cette interdiction peut être levée sous certaines conditions. Ainsi, le traitement des données sensibles et des données d'infraction peuvent être mis en œuvre lorsque la personne

concernée a expressément donné son consentement, en matière de droit du travail, pour la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne, si le traitement est mis en œuvre par une organisation à but non lucratif poursuivant une finalité philosophique ou religieuse… , le traitement est nécessaire pour l'exercice ou la défense d'un droit en justice, le traitement est nécessaire pour des motifs d'intérêt public…

2. Obligations portant sur les données personnelles.

Il s'agit notamment des obligations portant sur la finalité de la collecte (i), la nécessité de la collecte (ii), l'exactitude des données (iii), le caractère périssable des données (iv) et enfin la sécurité des données (v).

i. La finalité de la collecte :

La collecte d'une donnée personnelle doit se faire pour une ou plusieurs finalités bien déterminées. Le défaut de finalité ou son ambigüité rend illicite la collecte de la donnée donc interdit son traitement.

ii. La nécessité de la collecte :

Cette obligation renvoie au principe de la ‘’minimisation des données’’. Seules les données personnelles nécessaires à un traitement doivent être collectées par le responsable du traitement.

iii. L'exactitude des données :

Les données collectées doivent être exactes au regard des finalités pour lesquelles elles sont collectées. Cela dit, les données devenues inexactes ou dépassées doivent être mises à jour ou effacées.

iv. Périssabilité des données :

Les données collectées doivent être gardées pour une durée précise. Sauf pour certaines exceptions (exigence légale, pour des besoins de recherche ou archivistique).

v. Sécurité des données.

Les données collectées doivent être sécurisées contre tout traitement et accès non autorisé, leur intégrité doit être protégée. Le responsable du traitement doit mettre en œuvre des mesures techniques et organisationnelles permettant d'éviter toute perte, violation et détérioration accidentelle ou non des données personnelles à sa disposition.

SECTION II.

INTERVENTION DE NORMES INTERNATIONALES

Si les traitements (suivi du comportement d'un abonné en itinérance par exemple) d'un opérateur mobile établi en Guinée vont au-delà du territoire sur lequel il est physiquement établi, il n'est pas surprenant qu'en retour des dispositifs adoptés sous d'autres cieux s'appliquent à ce dernier pour les traitements qu'il met en œuvre sur les données personnelles des personnes se trouvant dans l'Union européenne.

Il existe plusieurs recommandations, bonnes pratiques, et conventions internationales ayant pour objet la protection des personnes physiques à l'égard des traitements sur les données personnelles les concernant.

Dans cette section, il ne sera pas question de passer en revue l'ensemble des textes règlementaires ou conventions internationales qui, d'une manière ou d'une autre pourrait s'appliquer à un responsable de traitement établi en Guinée. Aussi, l'objectif visé ici n'est pas d'étudier en profondeur les textes règlementaires ou conventions internationales qui seront passés en revue. Il sera plutôt question de montrer comment ces textes ou conventions internationales peuvent s'appliquer à des responsables de traitement établis en Guinée.

Après avoir passé en revue les grandes lignes de l'acte additionnel de la CEDEAO relatif à la protection des données personnelles, il serait important d'aborder le texte considéré comme étant de nos jours le plus protecteur des personnes physiques à l'égard des traitements effectués sur les données personnelles les concernant, en l'occurrence le RGPD.

§ 1. L'ACTE ADDITIONNEL DE LA CEDEAO SUR LES DONNÉES À CARACTÈRE PERSONNEL

Adopté à Abuja (Nigéria) le 16 février 2010, l'Acte Additionnel A/SA.1/01/10 relatif à la protection des données personnelles dans l'espace CEDEAO qui pourrait être qualifié de l'effet SAFARI dans la sous-région ouest africaine, s'applique à l'ensemble des responsables de traitement de la CEDEAO. Cet acte a été l'élément déclencheur de la règlementation relative à la protection des données personnelles dans l'espace.

Il a pour objectif (Article 2) d'inciter chaque État membre de l'organisation à mettre en place un cadre légal de protection des données personnelles.

Comme toutes les lois sur la protection des données personnelles, cet acte définit les obligations (Chapitre VII) auxquelles sont soumis les responsables de traitement et les droits dont bénéficient les personnes concernées (Chapitre VI). D'une manière générale, ce sont ces mêmes droits et obligations qui sont reconduits par les États membres de la CEDEAO ayant adoptés une règlementation sur la protection des données personnelles.

Pour s'assurer de la bonne mise en œuvre des futures lois nationales sur la protection des données personnelles au sein des États membres, l'acte additionnel encourage la création

d'autorités de régulation indépendantes chargées de veiller au respect (par les responsables de traitement) et à la sensibilisation (pour les responsables de traitement et les personnes concernées) sur les différentes règlementations relatives à la protection des données personnelles.

Il est important de souligner que l'acte additionnel maintient l'observation de formalités préalables pour la mise en œuvre d'un traitement de données personnelles.

Enfin, Le texte fait des renvois sur certaines dispositions qui devront être complétées ou modifiées par les États membres.

§ 2. LE RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES PERSONNELLES (RGPD)

Le 14 avril 2016, le Parlement européen adoptait le règlement n°2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données. Ce règlement, adopté par le Parlement de l'Union européenne, est entré en application le 25 mai 2018 pour le monde entier.

Il existe plusieurs critères qui déclenchent la mise en application du RGPD (i), certains rendent obligatoire le respect de ses dispositions pour un responsable de traitement établi hors de l'Union, notamment les opérateurs mobiles guinéens (ii).

i. Critères d'applicabilité du RGPD :

Les critères déclenchant la mise en application du RGPD peuvent être subdivisés en trois (3), il s'agit notamment du critère d'établissement (a), du critère lié à la fourniture des produits et services (b) et enfin le critère du suivi de la personne concernée (c).

a. Le critère d'établissement

D'office le RGPD s'applique à un responsable de traitement établi sur le territoire de l'Union européenne.

Toutefois, l'interprétation de ce critère ne doit pas être faite au sens strict du terme. En fait, ce critère est pris en compte même lorsque le responsable du traitement n'a pas un établissement physique sur le territoire européen. Ainsi, le fait d'avoir un représentant (personne physique) sur le territoire européen qui a pour mission d'effectuer des tâches administratives pour le compte du responsable du traitement suffit pour mettre en application le RGPD.

b. Le critère lié à la fourniture des produits et services

Lorsque le responsable du traitement se trouve en dehors de l'Union et que l'essentiel de ses activités de traitement se fait depuis un autre territoire, mais propose des produits et services (mêmes gratuits) à des personnes se trouvant dans l'Union, le RGPD lui est applicable.

Seulement, pourque le RGPD s'applique dans ces conditions, il doit être démontré que les produits et services sont effectivement à destination des personnes se trouvant dans l'Union.

Pour le faire, les critères pris en compte de manière générale sont la monnaie du pays de l'Union et la langue parlée.

L'accès à un site commercial à partir de l'Union ne déclenche pas nécessairement la mise en application du RGPD.

c. Le suivi du comportement de la personne concernée

Lorsque le traitement est mené hors l'Union mais consiste en une activité de suivi de comportement (le profilage d'un abonné en itinérance) d'une personne physique se trouvant dans l'Union, le RGPD s'applique.

ii. Situations dans lesquelles le RGPD s'applique à un opérateur mobile établi en Guinée.

Si l'opérateur peut trainer le pas à se conformer au RGPD pour les critères relatifs aux produits et services à destination de clients entreprise établis dans l'Union (a), tel ne sera pas le cas pour le service d'itinérance internationale (b).

a. Produits et services à destination de clients entreprise établis dans l'Union

L'opérateur à travers son unité Affaires d'Entreprise peut proposer des services d'internet dédiés, de flotte mobile et d'autres services de messagerie (A2P ou application à personne) à des entreprises établies dans l'Union depuis la Guinée.

A travers les offres entreprises, l'opérateur établi en Guinée peut être amené à collecter des données personnelles de personnes physiques se trouvant dans l'Union dans le but de les traiter pour des motifs légitimes (facturation de produits et services), dans le cadre d'une relation contractuelle…

Il appartient donc à l'opérateur, de s'assurer du respect des dispositions du RGPD à chaque fois qu'il propose directement des offres de services à des entreprises voire à des individus se trouvant dans un des pays de l'Union.

b. Le service d'itinérance internationale

L'opérateur peut décider de ne pas proposer des offres de services à des personnes physiques ou morales se trouvant dans l'Union. Toutefois, il ne peut se passer du service d'itinérance internationale.

Le service d'itinérance internationale rend quasi-obligatoire la mise en application des dispositions du RGPD pour un opérateur mobile établi en Guinée.

Les abonnés de la téléphonie mobile sont fréquemment en itinérance internationale entre la Guinée et l'Union européenne pour des raisons personnelles ou professionnelles.

Lorsqu'un abonné est en itinérance au sein de l'Union, son opérateur d'origine suit ses mouvements et sa consommation. Dans le cadre de cette étude, pour un abonné au départ de la Guinée et à destination de l'Union, son opérateur d'origine sait dans quel pays il se trouve

au sein de l'Union et sur quel opérateur il est raccordé et connait aussi sa consommation. Le suivi de ces éléments liés aux mouvements et à la consommation de l'abonné déclenche le critère d'applicabilité du RGPD pour suivi du comportement.

Dans une certaine mesure, l'opérateur du pays d'origine (guinéen) de l'abonné en situation d'itinérance au sein de l'Union peut obtenir de l'opérateur du pays visité (un des pays de l'Union) les données de géolocalisation de l'abonné en itinérance. Aussi, l'opérateur du pays d'origine a accès aux historiques des communications (appels émis et reçus, SMS…) de son abonné en itinérance dans l'Union.

Les scénarios ci-dessus contraignent l'opérateur établi en Guinée à mettre en application les dispositions du RGPD.

CHAPITRE 2 :

TRAITEMENTS DES DONNÉES PERSONNELLES PAR LES OPÉRATEURS MOBILES ÉTABLIS EN GUINNÉE

Les opérateurs mobiles sont des responsables de traitement pour les traitements effectués sur les données personnelles de leur personnel d'une part, et pour les traitements qu'ils effectuent sur les données personnelles de leurs abonnés et utilisateurs d'autre part.

Dans ce chapitre, l'étude sera principalement axée sur les traitements que font les opérateurs sur les données personnelles de leurs abonnés.

De manière générale, les opérateurs justifient les traitements qu'ils effectuent sur les données personnelles de leurs abonnés et utilisateurs par des deux raisons.

Premièrement, ils ont besoin de collecter et de traiter certaines données personnelles pour la facturation des produits et services, la connaissance du client et la proposition d'offres de services spécifiques et adaptées aux besoins du client. Ces traitements se justifient par un motif d'intérêt légitime poursuivi par l'opérateur.

Deuxièmement, ils sont tenus de collecter et de communiquer à des tiers autorisés les données personnelles de leurs abonnés pour des besoins d'enquêtes ou tous autres motifs liés à la sécurité publique. Cette catégorie de traitement est justifiée par un fondement légal ou règlementaire.

Enfin, l'opérateur procède à la collecte de plusieurs catégories de données personnelles (Section I) qui font l'objet de différents types de traitement en fonction de la finalité qu'il poursuit (Section II).

SECTION I.

CATÉGORIES DE DONNÉES PERSONNELLES ET PERSONNES PHYSIQUES CONCERNÉES PAR LES TRAITEMENTS D'UN OPÉRATEUR MOBILE

Pour les motifs cités plus haut, l'opérateur se voit obliger de collecter plusieurs catégories de données personnelles sur lesquelles il effectue différents types de traitement en fonction des finalités poursuivies.

§ 1. LES CATÉGORIES DE DONNÉES PERSONNELLES COLLECTÉES PAR UN OPÉRATEUR MOBILE

Pour se conformer à ses obligations légales tout en utilisant les données personnelles de ses abonnés et utilisateurs à des fins commerciales afin d'avoir une base d'abonnés stable tout en maximisant son revenu, l'opérateur collecte des données personnelles qui peuvent être classées ainsi qu'il suit : les données d'utilisateurs (i), les données relatives au trafic (ii), les données de localisation (iii) et enfin les données d'utilisation (iv)[6].

i. Les données d'utilisateurs :

Il s'agit de données personnelles permettant à l'opérateur :

- d'identifier un abonné, un client ou un utilisateur : les noms et prénoms, les documents d'identification : la carte d'identité nationale, le passeport…,
- de pouvoir contacter un abonné, un client ou un utilisateur : l'e-mail, l'numéro de téléphone…,
- de connaître les caractéristiques personnelles d'un abonné, d'un client ou d'un utilisateur : il s'agit de l'âge, le sexe, la couleur des cheveux…,
- de connaître les habitudes de consommation d'un abonné, d'un client ou d'un utilisateur : composition du ménage, forfaits achetés par un utilisateur …

ii. Les données relatives au trafic :

Les données du trafic permettent à l'opérateur d'apprécier la qualité de son service et de régler le trafic d'un utilisateur de son réseau. Il s'agit entre autres des adresses IP et les IMEI (identité internationale d'équipement mobile) des terminaux des abonnées.

iii. Les données de localisation :

Les données de localisation permettent à l'opérateur de localiser une carte SIM d'un abonné sur son réseau et de savoir sur lequel de ses sites la carte SIM est connectée.

[6] Politique de confidentialité d'Orange Finances Mobiles Sénégal.

iv. Les données d'utilisation :

Ces données permettent à l'opérateur de connaitre la préférence de ses produits et services par ses abonnés. Elles permettent en outre à l'opérateur de connaitre les communications téléphoniques de ses abonnés et les détails de leurs connexions à internet.

§ 2. LES PERSONNES PHYSIQUES CONCERNÉES PAR LE TRAITEMENT D'UN OPÉRATEUR MOBILE

Les abonnés et autres utilisateurs des produits et services d'un opérateur sont nombreux et variés.

La majorité des abonnés et les autres utilisateurs d'un réseau mobile sont des majeurs (âgés d'au moins 18 ans). Toutefois, les mineurs, qu'ils s'agissent de ceux utilisant une carte SIM pour les services de téléphonie et de donnée mobile, de ceux accédant à internet au travers d'un boitier WIFI se comptent par milliers voire par millions chez certains opérateurs.

Enfin, bien que les personnes morales ne soient pas protégées par la loi sur la protection des données à caractère personnel, il y a toutefois lieu de rappeler que l'opérateur collecte des données nominatives de personnes physiques travaillant pour le compte d'une personne morale d'une part, et collecte des données qui, combinées avec d'autres données permettent d'identifier une personne physique travaillant pour le compte d'une personne morale (adresse IP, numéro de téléphone utilisé pour la donnée mobile) d'autre part.

SECTION II.

LES TRAITEMENTS EFFECTUÉS PAR UN OPÉRATEUR MOBILE : EXEMPLE DE MTN GUINÉE

Dans le cadre de ses activités, l'opérateur effectue plusieurs types de traitement sur les données personnelles de ses abonnés et utilisateurs à des fins commerciales, pour des raisons techniques, légales ou règlementaires ou encore de lutte contre la fraude Simbox (Fraude sur les appels internationaux entrants) etc. Ces traitements sont automatisés ou non en fonction des capacités techniques de l'opérateur ou de la particularité du traitement en cause.

§ 1. LES TRAITEMENTS AUTOMATISÉS

Parmi les traitements dans lesquels MTN Guinée investit le plus dans des moyens automatisés et sophistiqués, figurent les traitements effectués par son service marketing à des fins commerciales. Il s'agit notamment :

- Des offres Kinder Garden ou Nursering, permettant de maintenir les nouveaux abonnés sur son réseau,
- Des offres appelées Day of Last Activity ou encore DOLA[7], ciblant les abonnés qui sont restés d'un (1) jour à une semaine sans faire au moins une activité génératrice de revenu pour les inciter à renouer à la consommation,
- Des offres plus agressives et quasi-gratuites à l'intention des abonnés qui sont restés plusieurs jours sans faire une activité génératrice de revenu dans le but de les rendre à nouveaux actifs et de prévenir leurs désabonnements.

La base d'abonnés d'un opérateur est composée de différents abonnés avec des profils variés. Les abonnés se distinguent par leurs consommations, leurs préférences de produits et services, leurs revenus et leurs emplacements géographiques. Au niveau de MTN Guinée, la segmentation marketing et la gestion de la valeur client sont les méthodes utilisées pour la gestion de la base d'abonnés.

- Segmentation marketing

Pour arriver à une segmentation aboutie de sa base d'abonnés, l'opérateur fait une analyse approfondie du comportement de chaque abonné pour pouvoir regrouper ceux qui ont des profils rapprochés.

Chez MTN Guinée, la base d'abonnés se subdivise en plusieurs segments dont deux (2) principaux. Un segment jeune et un segment à la facturation normale (facturation avec le plan tarifaire en vigueur). Pour arriver à cette segmentation, l'opérateur a croisé plusieurs catégories de données personnelles de ses abonnés à savoir : les historiques des recharges, les

[7] Jour de la dernière activité

types de services utilisés (SMS, données mobiles, appels téléphoniques …), les moments d'utilisation (jours, nuits), les emplacements géographiques de l'abonné etc. Ces données ainsi que d'autres, ont permis à MTN Guinée d'établir les différents segments de sa base d'abonnés.

Ainsi les abonnés qui font moins de recharges téléphoniques, utilisant beaucoup plus la messagerie et les données mobiles (forfaits internet), passant plus d'appels téléphoniques et à des heures tardives ont été considérés comme étant jeunes (Segment jeune). Dans leur segment, ils bénéficient d'offres spécifiques souvent composées de forfaits : appels, données mobiles et SMS.

Les abonnés utilisant moins de SMS, ayant une consommation constante de données mobiles ou pas et qui passent plus d'appels la journée sans se préoccuper d'achats de forfaits sont dans le segment facturation normale.

- La gestion de la valeur clients

Dans la téléphonie, chaque abonné est surveillé en permanence. Les historiques des recharges, les historiques des communications, les emplacements géographiques de l'abonné et ses habitudes de consommation sont monitorés en temps réel par l'opérateur. Ces données permettent à MTN Guinée par exemple de mieux connaitre chacun de ses abonnés et d'être au plus proche d'eux. En outre les données collectées sur la base de la gestion de la valeur client permettent à cet opérateur de connaitre le besoin réel de chaque abonné ainsi que sa capacité financière. Ainsi, MTN s'appuie sur ces données pour proposer des offres spécifiques et personnalisées à chaque catégorie d'abonné en fonction de sa capacité financière.

Avec la gestion de la valeur client, l'opérateur vise entre-autres :

- À fidéliser ses nouveaux abonnés :

Le marché des télécommunications est un marché très compétitif et concurrentiel, les nouveaux abonnés sont souvent raccordés à la concurrence.

Pour fidéliser ses nouvelles acquisitions à son réseau, l'opérateur leur propose des offres spécifiques et très avantageuses pour qu'elles restent dans sa base active. Cette offre est nommée 'Welcome Pack' chez MTN.

- À inciter les abonnés à consommer plus :

Il existe des abonnés qui sont constamment actifs mais générant un revenu faible pour l'opérateur (les abonnés de faible valeur ou les abonnés de valeur moyenne). Pour pousser de tels abonnés à fort potentiel à consommer plus pour accroitre le nombre de ses abonnés à grande valeur, l'opérateur leur propose des forfaits spécifiques à tarifs intermédiaires dans le but de changer leurs habitudes de consommation.

- À éviter le désabonnement massif de ses abonnés :

D'une manière générale, un opérateur considère comme étant abonnés actifs de sa base, les abonnés qui ont généré du revenu durant les quatre-vingt-dix (90) derniers jours encore appelés AGR90 (Aboné générant du revenu). Tout abonné qui ne génère donc pas du revenu et qui reste inactif durant cette période, entre dans le processus de désabonnement et n'est plus compté comme abonné actif au bout de trois (3) mois consécutifs.

Pour éviter un désabonnement massif de sa base active, l'opérateur à travers la gestion de la valeur client, propose des offres spécifiques et très agressives aux abonnés inactifs. Le but étant d'inciter ces abonnés à renouer à la consommation avec des offres à « Petits prix ». Les abonnés qui auront repris leurs habitudes de consommation se verront à nouveau facturer aux tarifs normaux et ceux qui ne reviennent pas au bout des trois (3) mois qui suivent, sont considérés comme des abonnés ayant quitté le réseau.

Pour parvenir à une bonne segmentation de sa base d'abonnés et mieux gérer sa valeur clients, l'opérateur a besoin d'informations très précises sur chaque abonné pour mieux le servir.

§ 2. LES TRAITEMENTS NON-AUTOMATISÉS

L'opérateur fait plusieurs types de traitement non-automatisés sur les données personnelles de ses abonnés et utilisateurs. De tels traitements inclus entre autres la collecte des données nominatives de nouveaux abonnés au moment de l'achat d'une carte Sim, la migration d'un groupe d'abonnés vers une classe de service ou encore la fiabilisation des informations d'identification des abonnés.

Chez MTN Guinée, le processus d'identification des abonnés (i) constitue le plus important traitement non-automatisé suivi du processus de migration de groupe d'abonnés d'une classe de service à une autre (ii).

i. Le processus d'identification des abonnés

L'identification des abonnés d'un opérateur mobile est une obligation règlementaire.

Le processus d'identification est long et continu. Il commence à partir de la collecte du document d'identification du nouvel abonné (passeport, carte d'identité nationale…), en passant par l'archivage de la copie du document utilisé pour l'enregistrement de la carte SIM à la fiabilisation des informations d'identification.

Au niveau de MTN Guinée, les informations d'identification collectées par les agents de vente sont renseignées dans une plateforme dédiée et le support d'identification utilisé est joint auxdites informations. Ensuite, les informations et le support sont transmis à une deuxième équipe qui est chargée de les vérifier à nouveau avant l'activation des services de la nouvelle carte SIM.

Enfin, il existe des archivages physiques et électroniques des copies des pièces utilisées pour les besoins de l'identification et d'enregistrement des abonnés. A la demande d'un tiers

autorisé dans le cadre d'une enquête par exemple, les copies des documents d'identification sont communiquées à ce dernier.

ii. La migration d'un groupe d'abonnés d'une classe de service à une autre

Les classes de services sont utilisées pour la ségrégation de la facturation des différents produits et services de l'opérateur, aussi, la gestion des privilèges des abonnés se fait au niveau des classes de service.

Par défaut les abonnés se trouvent dans une classe de service permettant de les facturer conformément au le plan tarifaire en vigueur. Toutefois, pour diverses raisons, un abonné ou des groupes d'abonnés peuvent être migrés par l'opérateur dans d'autres classes de services pour les faire bénéficier d'une facturation spécifique (groupe d'utilisateurs proches, flottes d'entreprise ou toutes autres facturations dégressives). De même, certains abonnés sont migrés vers d'autres classes de services dans le but de les priver de certains services (restriction des émissions et des réceptions d'appels) dans le cadre de la lutte contre la fraude sur les appels internationaux entrants par exemple.

Les traitements ci-dessus sont pour la grande majorité non-automatisés. Toutefois, si d'autres opérateurs peuvent les automatiser, force est de reconnaitre qu'ils ne peuvent pas l'être de bout en bout vu leur criticité et leur caractère mesquin.

DEUXIÈME PARTIE

MISE EN CONFORMITÉS AUX CADRES RÈGLEMENTAIRES

CHAPITRE I :

AUTO-ÉVALUER SA CONFORMITÉ

Le décalage entre la mise sur le marché d'un produit ou un service de la téléphonie impliquant un traitement de données personnelles et leurs règlementations à posteriori ont sans doute mis nombre d'opérateurs mobiles dans une situation pour le moins difficile. En effet, ils se trouvent être obligés à se mettre en conformité à des lois qui entrent application après avoir mis en œuvre des traitements sans au préalable se préoccuper d'une règlementation future.

Ainsi, conscients que le défaut de conformité leur expose à des risques de sanction, les opérateurs investissent constamment dans l'apprentissage des nouvelles règles régissant leurs activités notamment, la réglementation sur les données à caractère personnel dans le but de s'y conformer.

Pour être en conformité à la loi sur la protection des données à caractère personnel, l'opérateur en tant que responsable de traitement, doit pouvoir identifier les traitements qu'il met en œuvre ainsi que les règles applicables à chaque type de traitement (Section I), c'est ainsi qu'il pourra mettre en place des mesures techniques et organisationnelles pour la sécurisation et la confidentialité des données personnelles qu'il collecte et traite (Section II).

SECTION I.

TRAITEMENTS MIS EN ŒUVRE PAR L'OPÉRATEUR ET MISE EN CONFORMITÉ DU TRAITEMENT

Plusieurs types de traitement sont effectués par un opérateur sur les données personnelles de ses abonnés et utilisateurs. Ainsi, les règles applicables aux différents traitements dépendent du type de traitement et les données personnelles sur lesquelles il porte.

S'agissant d'un opérateur mobile établi en Guinée, il devra à la fois se conformer à la loi nationale sur la protection des données à caractère personnel et la plupart du temps, aux dispositions du règlement européen sur la protection des données personnelles notamment, pour les traitements induits par les abonnés en situation d'itinérance dans un des pays de l'Union.

Il existe plusieurs méthodologies et pratiques qui permettent à un opérateur mobile d'identifier les traitements qu'il effectue sur les données personnelles de ses abonnés et utilisateurs. Aussi, nombreuses sont les approches à suivre pour mettre en conformité les traitements non-conformes.

§ 1. IDENTIFICATION DES TRAITEMENTS EFFECTUÉS PAR L'OPÉRATEUR

Lorsque l'opérateur aura compris ses obligations découlant de la règlementation sur la protection des données à caractère personnel, il devra tout de suite faire une évaluation de son niveau de conformité afin de mettre en conformité les différents traitements identifiés comme étant non-conformes à la règlementation informatique et libertés. L'opérateur doit être informé et ce, à tout moment, de l'ensemble des traitements qu'il effectue sur les données personnelles de ses abonnés et autres utilisateurs.

Avoir une cartographie exacte et à jour de l'ensemble des traitements qui sont effectués par un opérateur est un exercice complexe mais pas impossible. Pour y arriver, l'opérateur doit procéder par des approches intelligentes et prendre des actions pratiques au travers d'un plan d'actions dont l'exécution doit être rigoureusement suivie par la direction de l'opérateur. Ci-après des actions et approches permettant à un opérateur d'identifier les traitements qu'il met en œuvre :

- La désignation d'un Délégué à la protection des données (DPD) :

L'opérateur doit désigner un Champion à la protection des données personnelles (Data Protection Champion ou encore DPC). Obligé de se mettre en conformité à la loi guinéenne sur la protection des données personnelles en général et le RGPD pour certains traitements, l'opérateur doit s'efforcer raisonnablement à ce que la fonction et les missions de son DPC correspondent aux dispositions de la loi guinéenne sur la protection des données personnelles relatives au Correspondant à la Protection des Données Personnelles (Chapitre VII : art. 14 à art. 16) et celles du RGPD relatives à la fonction et aux missions du Délégué à la Protection des Données (Section 4 : art. 37 à art. 39).

La loi guinéenne ne prévoyant pas la désignation d'un Correspondant externe à la protection des données et rendant facultative la désignation interne du Correspondant, il est fortement recommandé à l'opérateur de désigner en son sein un DPC. Cette désignation permettra à l'opérateur sur le plan national de se passer de certaines formalités préalables à la mise en œuvre d'un certain nombre de traitement, et d'être en conformité aux dispositions du RGPD relatives à la désignation d'un DPD.

- La mise en place d'un Comité de protection des données personnelles :

Présidé par le DPC, il est recommandé que ce comité soit un sous-comité du Conseil d'Administration de l'opérateur auquel seront rapportés les rapports d'activités du CPDP (Comité de protection des données personnelles).

Le CPDP doit être composé du personnel cadre et opérationnel de l'opérateur qui accède aux installations utilisées pour le traitement des données personnelles et celui impliqué dans les activités de traitement. Entre autres, le comité peut être composé des membres des services ci-après :

1- Le service informatique,

2- Le service en charge des produits et services,

3- Le service en charge de la gestion clientèle,

4- Le service en charge de l'analyse des données,

5- Le service en charge de la gestion des relations clients,

6- Le service en charge des ventes en ligne.

En plus, le comité doit être complété par du personnel issu des départements des finances, juridiques et des ressources humaines de l'opérateur.

Les membres du CPDP sont les référents du DPC au sein de leurs départements et services respectifs. Par conséquent, ils doivent assister activement le DPC à la mise en conformité de l'organisation à la règlementation sur la protection des données à caractère personnel.

- Le registre des activités de traitement

La mise en œuvre des actions citées ci-dessus permet d'avoir un registre des activités de traitement exhaustif sans lequel l'opérateur ne saurait prétendre à une conformité effective.

Le contenu du registre doit être conforme à l'article 30 du RGPD. Il est vrai que l'obligation de constituer un registre de traitement est conditionné par l'atteinte d'un seuil (plus de 250 employés) ou la mise en œuvre d'un traitement portant sur des catégories particulières de données (données sensibles, données d'infraction) et que le traitement soit non-occasionnel ou susceptible de comporter un risque pour les droits et libertés des personnes concernées. Cette exception étant très limitée, et n'excluant pas les traitements mis en œuvre par un opérateur

mobile à savoir, la collecte continue de documents et d'informations d'identification de ses abonnés (traitement non occasionnel), la géolocalisation de l'ensemble des abonnés (comportant un risque pour les droits et libertés des personnes concernées). L'opérateur doit impérativement constituer un registre d'activités de traitement.

Les référents à la protection des données personnelles au niveau de chaque service doivent jouer un rôle d'appuis essentiel dans le cadre de la constitution du registre des activités de traitement. Après avoir identifié les différents traitements mis en œuvre au niveau de chaque service, ils doivent les présenter au CPDP pour en discuter à l'effet d'obtenir plus de clarification sur la prochaine étape en présence du coordinateur du plan de mise en conformité (le DPC ou le DPD). Au cours de cette réunion, le DPC devra expliquer aux membres du comité la façon de renseigner une fiche de traitement, les informations à renseigner dans la fiche et la finalité recherchée par cette activité. Ainsi, les membres du comité pourront procéder aux renseignements des fiches de traitement avec les différentes personnes impliquées dans les traitements de données personnelles au niveau de chaque service de l'opérateur.

Le DPC est dépositaire des fiches de traitement qu'il pourra ensuite utiliser pour constituer son registre de traitement. Le registre doit comporter l'ensemble des traitements effectués par l'opérateur sans distinction des traitements mis en œuvre conformément à la règlementation sur les données à caractère personnel de ceux qui ne le sont pas. Cette étape constitue en réalité la porte d'entrée d'une véritable mise en conformité à la règlementation sur la protection des données personnelles. C'est seulement après cette étape que l'opérateur sera vraiment conscient des risques de sanction qu'il encoure du fait de sa non-conformité et de la dimension des traitements qu'il effectue. C'est à partir de là qu'il pourra catégoriser la criticité des traitements mis en œuvre en fonction des risques qu'ils représentent pour les personnes concernées (catégorie 1,2,3) et ainsi prioriser la mise en conformité des différents traitements conformément à la règlementation sur les données à caractère personnel (priorité 1,2,3) pour être à l'abri de tout risque de sanction pécuniaire, administratif et réputationnel.

§ 2. MISE EN CONCORMITÉ DES TRAITEMENTS

Après avoir identifié et répertorié l'ensemble des traitements mis en œuvre dans le registre de traitement, il serait important que l'opérateur se pose un certain nombre de question à savoir : le traitement en question est-il un traitement de données à caractère personnel ? La mise en conformité de ce traitement implique-t-elle le respect du RGPD ou seulement la loi nationale sur la protection des données personnelles ? Ou bien les deux règlementations lui est applicable à la fois ? les mesures techniques et organisationnelles actuellement mises en place permettent-elles d'être en conformité aux réglementations (RGPD et loi nationale) sur la protection des données à caractère personnel ?

Les réponses aux questions ci-dessus édifieront l'opérateur sur les mesures immédiates à prendre pour être en conformité aux deux textes.

Pour mettre en conformité ses traitements, l'opérateur devrait prendre en compte au moins trois facteurs :

i. Le type de traitement mis en œuvre et les catégories de données sur lesquelles porte le traitement :

La distinction des différents types de traitement mis en œuvre et les différentes catégories de données sur lesquelles porte le traitement est essentielle pour connaitre la règle applicable à chaque catégorie de traitement.

Si le RGPD a aboli la quasi-intégralité des formalités préalables à la mise en œuvre d'un traitement, les opérateurs mobiles établis en Guinée ne peuvent passer outre ces formalités pour la mise en application de la loi guinéenne.

L'observation de cette première étape permet à l'opérateur de distinguer les traitements qui nécessitent l'observation de formalités préalables auprès de l'autorité chargée de la protection des données à caractère personnel de ceux qu'il peut mettre en œuvre sans nécessairement observer de telles formalités. Aussi, cette étape permet à l'opérateur d'identifier l'existence ou non de traitement dont la mise en œuvre est interdite afin de les arrêter ou d'obtenir les autorisations requises pour ce type de traitement (traitement de données sensibles et de données d'infraction).

ii. L'existence de transfert de données à caractère personnel

L'opérateur doit avoir une définition élargie de la notion de transfert de données personnelles pour pouvoir prendre en compte la règlementation applicable (loi nationale ou RGPD). Ainsi, il doit déterminer :

a. Si le transfert à lieu entre la Guinée et un des pays membres de la CEDEAO : ce transfert est libre et l'opérateur n'a pas besoin d'autorisation préalable pour effectuer un tel transfert étant donné que le transfert de données à caractère personnel entre la Guinée et les pays membre de la CEDEAO est libre.

b. Si le transfert à lieu entre la Guinée et un pays non-membre de la CEDEAO : dans ce cas de figure, l'opérateur doit obtenir l'autorisation de l'autorité chargée de la protection des données à caractère personnel avant de procéder à un tel transfert tout en s'assurant que le pays destinataire des données personnelles assure au moins un niveau de garantie équivalant à celui de la Guinée pour les personnes concernée.

iii. Le transfert à lieu entre la Guinée et un des pays de l'Union européenne : Si l'opérateur a accès à des données personnelles se trouvant dans un des pays membre de l'Union ou collecte des données depuis un de ces pays, il doit se conformer aux dispositions du RGPD relatives aux transferts de données personnelles entre l'Union et un pays non-membre de l'Union.

A la date de la rédaction de ce mémoire, la Guinée n'était pas considérée par la commission européenne comme un pays ayant une règlementation informatique et libertés adéquate (RGPD, art. 45). Donc, l'opérateur établi en Guinée doit encadrer ses transferts de données personnelles vers l'Union ou en provenance de l'Union au travers d'un contrat (RGPD, art. 46) ou encore des règles d'entreprise contraignantes (Binding corporates rules[8] : BCR – RGPD, art. 47) pour couvrir ses transferts de données personnelles entre l'Union et la Guinée ou entre la Guinée et l'Union européenne.

La prise en compte des facteurs ci-dessus permet à l'opérateur de connaître les mesures de mise en conformité qu'il faut prendre pour chaque type de traitement à l'égard des règlementations qui lui sont applicables (RGPD et la loi guinéenne).

SECTION II.

SÉCURITÉ ET CONFIDENTIALITÉ

Aux termes de l'article 32 du RGPD, Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- la pseudonymisation et le chiffrement des données à caractère personnel;
- des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et des services de traitement;
- des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Dans la présente section, il sera question d'identifier tout d'abord des mesures ou moyens qui permettent de procéder à la sécurisation du traitement et la confidentialité des données personnelles avant de proposer une méthodologie permettant à un opérateur de mettre en place une politique de sécurité informatique.

[8] L'encadrement du transfert n'est possible que pour des opérateurs ayant une représentation effective au sein de l'UE (siège ou une représentation). Pour les opérateurs n'ayant pas de représentation au sein de l'UE, il est mieux d'opter pour un encadrement contractuel en l'absence d'une décision d'adéquation.

§ 1. SÉCURISATION DU TRAITEMENT ET CONFIDENTIALITÉ DES DONNÉES

La sécurisation du traitement et la confidentialité des données personnelles sont une exigence non-négociable pour un responsable de traitement. L'observation de cette exigence permet de garantir la protection de la vie privée et les libertés fondamentales des personnes concernées. La sécurisation du traitement et la confidentialité des données personnelles garantissent que les données collectées et traitées par l'opérateur ne soient pas endommagées, détruites, ou communiquées à des tiers non-autorisés.

Pour mettre en œuvre des mesures techniques et organisationnelles lui permettant de sécuriser ses traitements et les données personnelles collectées, l'opérateur doit procéder par une approche basée sur les risques. Cela dit, plus les données collectées sont sensibles et ont un impact crucial sur la vie privée et les libertés de la personne concernée, plus les mesures de sécurité et de confidentialité doivent être renforcées.

En pratique, l'opérateur doit mettre en œuvre des mesures de sécurité :

- physiques : verrous aux portes, des coffres-forts…
- logiques : gestion des habilitations, cryptage des données…

Aussi, l'opérateur doit pouvoir tracer et archiver les historiques d'accès et les différentes actions effectuées dans ses plateformes utilisées pour les traitements.

De plus, il est fortement recommandé à l'opérateur d'avoir une politique de mots de passe très rigoureuse. La mise en place de l'auto-verrouillage des applications ou logiciels métiers, la révision obligatoire des mots de passe après une certaine période, la confirmation via code PIN lors d'un changement de mot de passe…. sont entre autres des pratiques recommandées à tout responsable de traitement.

Enfin, l'opérateur doit avoir un système de sauvegarde des données personnelles pour éviter une perte définitive des données en cas de violation ou d'incident affectant les systèmes ou les plateformes utilisées pour le traitement.

§ 2. POLITIQUE DE SECURITÉ INFORMATIQUE

Pour bâtir un environnement sécurisé de traitement des données à caractère personnel, l'opérateur doit au préalable définir les périmètres de sécurité à respecter dans le cadre de son activité au travers d'un document qui est mis à disposition de l'ensemble de ses employés et autres contractant (stagiaires, consultants, expatriés, intérimaires…). Ce document qui est en réalité la politique de sécurité informatique encore appelé politique NTIC, doit être simple, complet, pratique et prenant en compte l'ensemble des aspects sécuritaires du système informatique et les applications utilisées pour la mise en œuvre d'un traitement.

Le RGPD et la loi guinéenne sur la protection des données personnelles exigent du responsable du traitement, la mise en œuvre de mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté aux risques. La mise en œuvre de cette

exigence de sécurité du RGPD et la loi guinéenne au travers d'une politique de sécurité informatique nécessite l'implication de professionnels et une bonne méthodologie. C'est en ce sens que la CNIL préconise la démarche méthodologique ci-après :

Recenser les traitements de données à caractère personnel automatisés ou non, les données traitées (ex : fichiers client, contrats) et les supports sur lesquels elles reposent :

- les matériels (ex : serveurs, ordinateurs portables, disques durs),
- les logiciels (ex : système d'exploitation, logiciel métier),
- les canaux de communication (ex : fibre optique, Wi-Fi, Internet),
- les supports papiers (ex : document imprimé, photocopie).

Apprécier les risques engendrés par chaque traitement :

1. **Identifier les impacts potentiels** sur les droits et libertés des personnes concernées, pour les trois évènements redoutés suivants :

- accès illégitime à des données (ex : usurpations d'identités consécutives à la divulgation des fiches de paie de l'ensemble des salariés d'une entreprise) ;
- modification non désirée de données (ex : accusation à tort d'une personne d'une faute ou d'un délit suite à la modification de journaux d'accès) ;
- disparition de données (ex : non détection d'une interaction médicamenteuse du fait de l'impossibilité d'accéder au dossier électronique du patient).

2. **Identifier les sources de risques** : (qui ou quoi pourrait être à l'origine de chaque évènement redouté ?), en prenant en compte des sources humaines internes et externes (ex : administrateur informatique, utilisateur, attaquant externe, concurrent), et des sources non humaines internes ou externes (ex : eau, matériaux dangereux, virus informatique non ciblé).

3. **Identifier les menaces réalisables :** (Qu'est-ce qui pourrait permettre que chaque évènement redouté survienne ?). Ces menaces se réalisent via les supports des données (matériels, logiciels, canaux de communication, supports papiers, etc.), qui peuvent être :

- utilisés de manière inadaptée (ex : abus de droits, erreur de manipulation) ;
- modifiés (ex : piégeage logiciel ou matériel – keylogger, installation d'un logiciel malveillant)
- perdus (ex : vol d'un ordinateur portable, perte d'une clé USB) ;
- observés (ex : observation d'un écran dans un train, géolocalisation d'un matériel) ;

- détériorés (ex : vandalisme, dégradation du fait de l'usure naturelle) ;
- surchargés (ex : unité de stockage pleine, attaque par dénis de service).

4. **Déterminer les mesures existantes ou prévues** qui permettent de traiter chaque risque (ex : contrôle d'accès, sauvegardes, traçabilité, sécurité des locaux, chiffrement, anonymisation).
5. **Estimer la gravité et la vraisemblance** des risques, au regard des éléments précédents (exemple d'échelle utilisable pour l'estimation : négligeable, modérée, importante, maximale).

Le suivi de cette méthodologie de la CNIL permet sans doute à un opérateur de rédiger et de mettre sur pied une politique de sécurité adéquate. En plus, cette méthodologie peut être complétée par l'expérience pratique que possède l'opérateur dans le cadre de ses activités de traitement et des spécificités de son environnement.

CHAPITRE 2 :

PÉRENISER SA CONFORMITÉ ET PRÉVENIR LES RISQUES DE SANCTION

La problématique liée à la conformité est devenue une préoccupation de taille pour les opérateurs mobiles compte tenu des risques de sanction auxquels ils sont exposés au quotidien. De nos jours, les opérateurs investissent assez de moyens (humains, matériels et financiers) dans le domaine de la conformité et ont même revu leurs organigrammes en créant de nouveaux services chargés de veiller au respect des exigences légales et règlementaires applicables à leurs activités (Direction Risque et Conformité pour citer MTN Guinée).

Un opérateur établi en Guinée peut être exposé à une double sanction pour défaut de conformité à la règlementation sur les données à caractère personnel. Premièrement, il est exposé à un risque de sanction à la loi guinéenne sur la protection des données à caractère personnel dont la sanction est fonction de la gravité du manquement et des avantages tirés. Deuxièmement, il est exposé aux sanctions découlant du RGPD dont la sanction pécuniaire peut s'élever à 10 000 000 EURO ou 2% du chiffre d'affaire mondial total de l'année précédente pour défaut de coopération avec les autorités de contrôle par exemple, et de 20 000 000 EURO ou 4% du chiffre d'affaire mondial total de l'année précédente pour manquement lié aux principes fondamentaux du traitement (le consentement par exemple). En plus des sanctions pécuniaires sus citées, les dirigeants de l'opérateur sont en outre exposés à des sanctions pénales.

Vu l'impact des sanctions du RGPD et de la loi guinéenne sur la protection des données personnelles, l'opérateur a grand intérêt à ménager sa conformité par la mise en place d'un service de conformité chargé d'identifier les zones de non-conformité à la réglementation sur les données à caractère personnel afin de lui faire des préconisations pour une régularisation rapide avant d'être alerté par l'autorité chargée de la protection des données personnelles.

Dans ce chapitre, l'accent sera mis sur les mesures et approches garantissant une conformité continue à la règlementation sur la protection des données à caractère personnel dont la gestion proactive des risques de non-conformité (Section I) et la gestion des parties prenantes (Section II).

SECTION I.

LA GESTION PROACTIVE DES RISQUES DE NON-CONFORMITÉ

Il y va de l'intérêt de l'opérateur de se mettre en conformité à la règlementation sur la protection des données à caractère personnel en prenant toute la diligence nécessaire pour y parvenir. L'opérateur doit prendre des mesures de mise en conformité en amont avant toute interpellation ou demande d'explication par l'autorité de contrôle. Les mesures prises par l'opérateur doivent permettre d'une part, d'identifier les zones de non-conformité afin de les régulariser (audit interne, revue de conformité, contrôle spontané…), et d'autre part, d'assurer le maintien de sa conformité à la règlementation sur les données à caractère personnel. Au cours de la présente section, il sera abordé l'importance de désigner un Délégué à la protection des données personnelles avant de parler des activités d'audit interne et les bonnes pratiques permettant à l'opérateur d'être en conformité à la règlementation informatique et libertés.

§ 1. DESIGNATION DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES.

Pour un opérateur établi en Guinée, la désignation d'un DPD doit être un préalable non négociable. Bien que cette fonction soit plus allégée par la loi guinéenne (désignation facultative de l'équivalent d'un CIL dans l'ancienne loi informatique et libertés française) et rendue obligatoire dans certaines conditions par le RGPD, l'opérateur établi en Guinée doit faire de la désignation du DPD une priorité pour une bonne mise en œuvre des exigences de la règlementation sur la protection des données personnelles.

Désignation du DPD comme preuve de volonté de mise en conformité à la loi sur la protection des données à caractère personnel : la désignation du DPD, figure parmi les diligences attestant de la volonté de l'opérateur à se conformer aux règlementations sur la protection des données personnelles et une preuve suffisante de la documentation de sa conformité.

Le DPD comme coordonnateur du programme de mise en conformité : un plan d'actions de mise en conformité à la règlementation sur les données à caractère personnel est vaste, complexe et varié. Sa bonne mise en exécution nécessite qu'il soit piloté par un spécialiste de la règlementation des données personnelles. Le DPD est en quelque sorte le chef de projet de la mise en conformité. La loi lui accorde toute l'indépendance et le temps nécessaire pour la mise en œuvre et le suivi du plan de mise en conformité afin d'assurer sa bonne exécution.

Le DPD comme interlocuteur de l'autorité chargée de la protection des données personnelles et conseiller de l'opérateur : un interlocuteur qui maitrise la loi sur la protection des données à caractère personnel et conscient des risques qui en découlent pour défaut de conformité est mieux placé pour interagir avec l'autorité de contrôle et mieux conseiller l'opérateur en la matière.

Enfin, une des conditions qui rend obligatoire la désignation d'un DPD, est l'activité de base du responsable du traitement ou d'un sous-traitant qui consiste en des opérations de traitement

qui, du fait de leur nature, de leur portée et ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées. Cette condition rend obligatoire pour l'opérateur la désignation d'un DPD pour les traitements ci-après : la géolocalisation des abonnés, la collecte de milliers de données nominatives des nouveaux abonnés, le suivi systématique du profil de l'ensemble des abonnés…

§ 2. LES OPÉRATIONS D'AUDITS ET LES BONNES PRATIQUES

Opérations d'audit :

L'opérateur doit encourager les opérations d'audit pour s'assurer de la mise en œuvre et du respect des procédures, clausiers, préconisations et les exigences de la règlementation sur la protection des données personnelles par son personnel opérationnel et cadre impliqué dans les activités de traitement et de collecte des données personnelles.

L'audit permet d'évaluer l'efficacité et la pertinence des contrôles (procédures, politiques, gestion d'habilitations…) mis en place pour sécuriser les traitements effectués par l'opérateur et la confidentialité des données collectées.

L'audit peut être mené par le DPD ou les membres du département chargé de l'audit de l'opérateur. Dans l'un ou l'autre des cas, l'approche à suivre devra rassurer les collaborateurs en les faisant comprendre que le but de l'audit est de les protéger et de protéger l'entreprise contre tout risque de sanction ou de réparation de dommage à la suite de plaintes éventuelles des personnes concernées à l'encontre de l'opérateur. Cela dit, l'audit doit être une opération à blanc avec pour objectif d'obtenir la collaboration des collaborateurs dans le but d'identifier les zones de risque et de non-conformité afin d'y remédier avant toute interpellation de l'autorité de contrôle.

L'opérateur doit avoir un plan annuel d'audit, il est fortement recommandé à l'opérateur d'engager des cabinets spécialisés dans le domaine de la protection des données personnelles pour mener des opérations d'audit plus approfondies en plus de celles menées par les services compétents de l'opérateur.

Les bonnes pratiques :

Pour assurer la stabilité et de la pérennité de sa conformité à la règlementation sur la protection des données personnelles et l'ensemble des contrôles cités plus haut, l'opérateur doit encourager les pratiques ci-après :

- Les opérations de sensibilisation et de formation : la majorité des employés ignore l'existence de règles contraignantes (procédures, politiques internes et réglementations) relatives à la protection des données personnelles voire même la notion de données personnelles. Pour obtenir l'adhésion du personnel au projet de conformité défini par l'opérateur, des programmes de formation et de sensibilisation doivent être définis et exécutés. Les formations peuvent se dérouler en présentielle, à travers des outils e-learning ou encore des ateliers…. Le contenu de la formation

diffère en fonction du personnel cible avec des sessions allégées pour les employés qui ne sont pas directement impliqués dans le traitement des données à caractère personnel et des sessions approfondies pour les employés impliqués dans les processus de traitement.

- L'opérateur doit sensibiliser son personnel à travers son canal de communication interne : des mails à tout le personnel, l'intranet, des SMS… sur des thèmes spécifiques et de manière approfondie. Il pourrait s'agir par exemple d'une communication interne relative à la sensibilisation sur la question du transfert de données à caractère personnel. En plus, l'outil intranet peut servir de plateforme d'accès rapide et simple aux clausiers et procédures relatives à la protection des données à caractère personnel pour l'ensemble du personnel.

- L'opérateur établi en Guinée n'est pas par principe assujetti aux dispositions du RGPD relatives au privacy impact assessment (PIA) et aux principes du privacy by design ou du privacy by default. Toutefois, l'opérateur devra prendre en compte ces principes pour certains types de traitement impliquants un niveau de risque élevé pour la vie privée et les libertés des personnes concernées. Par exemple, les services marketing pourront inviter le DPD à participer à tout projet impliquant un traitement sophistiqué de données personnelles afin qu'il évalue l'impact potentiel sur la vie privée et les libertés des personnes concernées.

SECTION II.

LA GESTION DES PARTIES PRENANTES

Il est important que l'opérateur ait une bonne relation et une très bonne collaboration avec les parties prenantes internes et externes impliquées dans son processus de traitement pour le bon maintien de sa conformité et la prévention de certains risques pour défaut de conformité à la règlementation sur les données à caractère personnel. Qu'ils s'agissent des parties prenantes internes (personnel cadre ou collaborateur) et des parties prenantes externes (autorité de protection, tiers autorisés, associations des consommateurs, législateurs…), toutes peuvent apporter un soutien non négligeable à l'opérateur dans le cadre de la mise en œuvre de son plan de conformité. A titre illustratif, une bonne relation avec les législateurs permet à l'opérateur de savoir s'il existe des projets de lois relatives à la protection des données personnelles en cours d'adoption, cette information permet à l'opérateur de faire un lobbying pour que certaines dispositions de la loi future soient revues ou retirées, ou encore, de prendre des mesures proactives de conformité. Aussi, les collaborateurs peuvent être des lanceurs d'alertes lorsqu'ils constatent l'existence d'un risque potentiel causé par un manquement à la règlementation.

Dans la présente section, il sera abordé la gestion de la relation avec l'autorité chargée de la protection des données personnelles et d'autres entités importantes avant de dire un mot sur la gestion de la relation avec les personnes concernées.

§1 : RELATION AVEC L'AUTORITÉ CHARGÉE DE LA PROTECTION DES DONNÉES PERSONNELLES ET D'AUTRES ENTITÉS IMPORTANTES

L'opérateur doit avoir une politique claire de gestion de ses parties prenantes à la tête desquelles doit figurer l'autorité de protection des données à caractère personnel.

L'opérateur, par la nature de ses activités, reste un responsable de traitement. De ce fait, il doit s'assurer du maintien d'une relation stable avec l'autorité de protection et s'assurer du maintien d'une relation amicale et collaborative avec ladite autorité.

Le maintien d'une relation étroite avec les agents de contrôle de l'autorité de protection permet à l'opérateur d'être au courant de certaines initiatives prévues ou à prévoir par l'autorité. La connaissance de ses informations permet à l'opérateur de revoir en amont sa conformité et son dispositif de sécurisation des données personnelles et des traitements qu'il effectue avant un contrôle inopiné des agents de l'autorité.

Un des critères d'atténuation des sanctions prises à l'encontre d'un responsable de traitement, est sa volonté de coopérer avec les agents de l'autorité de contrôle lors des missions de contrôle et d'audit. Ainsi, si l'opérateur est réputé être coopératif et ouvert aux agents de l'autorité de contrôle, cela pourrait contribuer à l'allègement des sanctions qui pourraient être prononcées à son encontre en cas de manquement.

En outre, la règlementation sur les données à caractère personnel est complexe et parfois difficile à déchiffrer, Le DPD aura toujours besoin de l'appui des agents des services techniques et juridiques de l'autorité de protection pour des clarifications et d'interprétations de certaines dispositions de la règlementation informatique et libertés. Pour obtenir la disponibilité et l'ouverture des agents de l'autorité de contrôle, le DPD doit en amont s'assurer de l'existence d'une bonne collaboration entre lui et lesdits agents.

Au-delà de l'autorité chargée de la protection des données à caractère personnel, l'opérateur doit aussi s'assurer du maintien d'une bonne relation avec d'autres parties prenantes telles que les associations des consommateurs, les tiers autorisés à recevoir communication des données à caractère personnel et certaines associations de professionnels (association des responsables de conformité par exemple) à travers son DPD et son service en charge des relations publiques et institutionnelles.

§2 : RELATION AVEC LES PERSONNES CONCERNÉES.

Certes, le fait d'être en bon terme avec l'autorité chargée de la protection des données personnelles est fondamental pour tout responsable de traitement. Toutefois, si dans la pratique les responsables de traitement sont beaucoup plus préoccupés de leurs relations avec l'autorité de protection, la pratique devrait être l'inverse. Cette perception inverse permet à l'opérateur de penser comme l'autorité de contrôle lorsqu'il met en œuvre son programme de conformité qui sera une approche plus rigoureuse et orientée sur la protection des personnes concernées. En outre, cette approche établie un climat de confiance entre l'opérateur et ses abonnés et lui permet de solidifier sa conformité et sa réputation.

L'autorité de protection a pour mission d'assurer que les données personnelles sont traitées dans le strict respect de la règlementation informatique et libertés. Cela dit, la priorisation du respect de la vie privée et des libertés fondamentales des personnes concernées doivent passer au-delà de tout intérêt commercial de l'opérateur. L'opérateur peut mettre en œuvre cette démarche à travers les principes du privacy by design et du privacy impact assessment pour ses traitements existants et futurs.

Surtout, l'opérateur doit maintenir une relation de confiance avec les personnes concernées qui de bonne foi et par confiance mettent à sa disposition leurs données personnelles sans contrepartie aucune. Pour cela, l'opérateur doit impérativement respecter ses obligations découlant de la règlementation sur la protection des données personnelles et informer les personnes concernées de leurs droits et leur faciliter l'exercice desdits droits. De plus, l'opérateur à travers son DPD, doit établir un canal de communication avec les personnes concernées.

Enfin pour compléter les mesures juridiques et organisationnelles mises en place par l'opérateur pour être à l'écoute et proche des personnes concernées, il doit aussi avoir des rencontres périodiques avec les associations des consommateurs et mener des enquêtes terraines auprès de ses abonnés et utilisateurs pour connaître leur opinion et recueillir leurs avis sur la façon dont ils perçoivent le traitement de leurs données personnelles.

CONCLUSION

Comme nous l'avons vu plus haut, le risque auquel un opérateur peut être exposé pour défaut de conformité à la règlementation informatique et libertés à l'heure du RGPD est lourd de conséquence. Récemment, L'opérateur allemand 1&1 a été condamné à une amende de 9,55 millions d'euros pour ne pas avoir protégé, au mépris du RGPD, les informations personnelles de ses clients au sein de ses centres d'appels[9].

Pour être à l'abris de toutes sanctions et protéger leurs Groupes, les opérateurs mobiles établis en Guinée doivent mettre en œuvre des mesures techniques et organisationnelles permettant de protéger les données personnelles qu'ils collectent ainsi que les traitements qu'ils mettent en œuvre et ce, en s'inspirant du RGPD en attendant la mise en place par les autorités guinéennes d'un organe de contrôle et les textes d'application de la loi L2016/037/AN relative à la cybersécurité et la protection des données à caractère personnel pour le traitement de données personnelles en Guinée.

Au regard de l'état actuel des choses, allant des efforts entrepris par les responsables de traitement pour le respect de la vie privée des citoyens sans la présence d'une autorité de contrôle et une loi nationale sur la protection des données personnelles remplie de faiblesses, il ne serait pas étonnant que la future autorité guinéenne de protection des données personnelles remette en cause certaines mesures de conformité prises par les responsables de traitement tout en faisant de la révision de la loi de juillet 2016 une de ses priorités.

[9] https://www.zdnet.fr/actualites/rgpd-l-operateur-allemand-1-1-condamne-a-une-amende-de-955-millions-d-euros-39895875.htm

BIBLIOGRAPHIE

LOIS ET ACTE ADDITIONNEL

- La loi L/2016/037/AN relative à la cybersécurité et la protection des données à caractère personnel en Guinée

Acte Additionnel A/SA.1/01/10 relatif à la protection des données personnelles dans l'espace CEDEAO

REGLEMENTS

- Règlement (UE) 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

GUIDE PRATIQUES

- Commission Nationale de L'Informatique et des Libertés, La sécurité des données personnelles, Edition 2018
- Commission Nationale de L'Informatique et des Libertés, Sensibilisation au RGPD pour les petites et moyennes entreprises

ENTRETIENS

- Des entretiens avec des employées de MTN Guinée

OUVRAGE

- Catherine VIOT, Le Marketing – La connaissance du marché et des consommateurs, De l'étude de marché aux choix stratégiques, Le marketing mix, Gualino éditeur, octobre 2005.
- Francis DONNAT, Droit européen de l'internet – Réseaux, données, services, LGDDJ, avril 2018.
- Myriam QUÉMÉNER, Le droit fac à la disruption numérique, Gualino, avril 2018
- Guillaume Desgens-Passanau, La protection des données personnelles – Le RGPD et la nouvelle loi française, LexisNexis, 3ème édition, juin 2018

AUTRES

- ALLEN & OVERY, Preparing for the General Data Protection Regulation, Janvier 2018.
- Politique de confidentialité d'Orange Finances Mobiles Sénégal.