# République du Bénin

**Fraternité - Justice - Travail**

# RAPPORT ANNUEL D'ACTIVITÉS

# 2018

APDP

AUTORITE DE PROTECTION DES DONNEES PERSONNELLES

# AUTORITE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

# RAPPORT ANNUEL D'ACTIVITÉS

# 2018

**Prévu par l'article 481 de la loi n°2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.**

# SOMMAIRE

# PARTIE - III

**Question d'actualité :**

**Le téléphone et la vie privée**

# PARTIE - IV

## Annexe

# MOT DU PRESIDENT

La fin de chaque exercice offre l'occasion de jeter un regard rétrospectif sur les actions engagées au cours de l'année achevée et de s'inscrire dans une vision prospective relativement aux tâches qu'il reste à accomplir.

C'est à travers la publication de son rapport annuel d'activités que l'Autorité de Protection des Données à caractère Personnel (APDP) s'attèle avec minutie, à élaborer son bilan au titre de l'année écoulée.

En effet, l'année 2018 n'a pas échappé à la tradition. Elle aura permis de voir les actions majeures initiées en 2017, se poursuivre et se parachever avec efficacité et efficience, dans un cadre législatif nouveau porté par la promulgation de la loi n°2017-20 du 20 avril 2018 portant code du numérique qui consacre en son livre 5 la protection des données personnelles et de la vie privée.

Ainsi, aux termes des nouvelles dispositions légales, la Commission Nationale de l'Informatique et des Libertés (CNIL) devient Autorité de Protection des Données à caractère Personnel (APDP). Elle se trouve renforcée dans son autonomie de gestion, confortée dans ses missions républicaines de veille, de régulation et de contrôle de toutes les opérations de collecte et de traitement des données à caractère personnel.

Les différentes statistiques relatives au nombre de sessions organisées et de décisions rendues sont une source de légitime fierté et d'encouragement à poursuivre la mission républicaine assignée à l'APDP car, elles témoignent de l'assiduité de l'ensemble des animateurs de l'Institution.

Au titre des actions phares de l'année 2018, il convient de mettre en exergue la sensibilisation des citoyens et la formation des responsables de traitements sur les questions relatives à la protection des données personnelles ; toutes choses qui ont véritablement renforcé la visibilité de l'APDP.

Aussi, l'institution a-t-elle joué un rôle éminent dans le contrôle des opérations de Recensement Administratif à Vocation d'Identification de la Population (RAVIP).

Le gouvernement de la République a, par ailleurs, bénéficié de l'appui-conseil de l'APDP relativement à ses initiatives touchant aux données à caractère personnel.

L'année 2018 aura également permis l'élaboration et l'adoption du manuel des procédures administratives, financières et comptables ainsi que du règlement financier de l'Autorité. La gestion du fonctionnement des services techniques et administratifs de l'Autorité s'est aussi améliorée.
Au plan de la coopération nationale, régionale et

internationale, l'APDP a pris toute sa part dans les diverses rencontres, manifestations, colloques et autres ayant réuni ses paires et partenaires œuvrant dans le domaine de la protection des données personnelles.

Au titre des perspectives, l'Autorité place un grand espoir dans les effets bénéfiques de ses actions d'Information, d'Éducation et de Communication (IEC) en direction des citoyens et plus spécifiquement de la jeunesse, dans l'optique de prévenir les dérives liées à la diffusion des données personnelles notamment sur les réseaux sociaux.

L'accompagnement pédagogique des entreprises qui collectent et traitent des données personnelles, reste une des priorités de l'APDP.

Les contrôles seront effectués et les sanctions résolument appliquées conformément aux textes en vigueur.

Avant de finir, je voudrais féliciter et remercier les principaux animateurs de l'Institution que je préside, pour leur abnégation au travail. Je les exhorte surtout à poursuivre avec détermination la noble et exaltante mission assignée à l'APDP par les lois et règlements de la République. La performance à laquelle nous aspirons tous, est à ce prix.

Ma sincère gratitude va au Commissaire du Gouvernement pour sa contribution de qualité au rayonnement de notre Institution commune.

À l'ensemble du personnel technique et administratif, j'adresse ma réelle satisfaction pour son appui et son implication de tous les instants à l'atteinte des objectifs que nous nous sommes fixés dans la protection des données personnelles et de la vie privée dans notre pays.

Ensemble, relevons les défis qui sont les nôtres !

Le Président de l'APDP

**Etienne Marie FIFATIN**

# Les principaux acteurs de l'APDP

L'Autorité de Protection des Données à caractère Personnel (APDP) est composée de onze (11) membres issus de différents secteurs socioprofessionnels ainsi que le prévoit l'article 464 de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin

## Le bureau

**Etienne Marie FIFATIN**

Président

**K. Jocelyn DEGBEY**

Vice-président

**Imourane LEKOYO**

Secrétaire du Bureau

# Les Conseillers

**Nicolas BENON**

**Soumanou OKE**

**Amouda ABOU SEYDOU**

**Onésime MADODE**

**Wally M. ZOUMAROU**

**Ismath BIO-TCHANE**

**Guy-Lambert YEKPE**

**Valère TCHOBO**

## Commissaire du Gouvernement près l'APDP

**Félicité AHOUANDOGBO TALON**

## Secrétaire Général

**Ambroise Djima ZINSOU**

# PARTIE - I

## LE NOUVEL ENVIRONNEMENT JURIDIQUE DE LA PROTECTION DES DONNEES PERSONNELLES

# I- Le Code du numérique et le renforcement de la protection des données personnelles

L'explosion prodigieuse des nouvelles technologies de l'information et de la communication, la mise en place de nouveaux modèles économiques dans le monde et les divers usages du numérique ici et ailleurs avec leur impact sur les données personnelles, ont conduit le Gouvernement béninois et le législateur à engager des réformes profondes dans la sphère du numérique. En effet, la loi n° 2009-09 du 22 mai 2009 portant protection des données à caractère personnel autrefois en vigueur, ne permettait plus de répondre aux nouvelles exigences de la protection des données personnelles face aux défis actuels. Le code du numérique adopté par la Représentation nationale est venu renforcer le cadre juridique de la protection des données personnelles au Bénin notamment en son livre cinquième porteur d'importantes innovations.

## A. De l'Autorité de Protection des Données à caractère Personnel (APDP)

La loi n° 2009-09 du 22 mai 2009 abrogée par le code du numérique a connu des changements notables en ce qui concerne la dénomination de l'Institution en charge de la protection des données à caractère personnel.

En effet, avec la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, la Commission Nationale de l'Informatique et des libertés (CNIL) en charge de la protection des données à caractère personnel a été érigée en une autorité dénommée "**Autorité de Protection des Données à caractère Personnel** (**APDP**)."

S'agissant de la composition de l'autorité, bien qu'elle n'ait pas connu de modification, les modalités de désignation de certains membres ont été revues : Les deux (02) personnes qualifiées pour leur connaissance en informatique sont désignées par l'Assemblée Nationale mais désormais sur une liste de cinq (05) personnes retenues par le Bureau de l'Assemblée après appel à candidature.

De même, avant leur entrée en fonction, selon les dispositions de l'article 468 du code du numérique, les membres de l'Autorité prêtent désormais serment devant la Cour suprême siégeant en audience solennelle, alors que dans la précédente loi, la prestation de serment a lieu devant la Cour d'Appel de Cotonou.

Aux termes des dispositions de l'article 463 de ladite loi, l'APDP est une structure administrative indépendante dotée de la personnalité juridique, de l'autonomie administrative, financière et de gestion.

Aussi, les prérogatives, les attributions et missions de la structure ont-elles été étendues par le législateur à travers les dispositions de l'article 483 du code du numérique.

# B. Du traitement des Données à caractère Personnel

Le code du numérique a également apporté des innovations en ce qui concerne le rôle et les obligations incombant aux responsables de traitement et a renforcé le droit des personnes concernées par le traitement.

- Le renforcement des obligations existantes des responsables de traitement (art. 387, 388, 415-436)

  Avec le code du numérique, les obligations mises à la charge des responsables de traitement se sont accrues.
  Outre l'obligation de déclarer auprès de l'Autorité les opérations impliquant la collecte et le traitement des données à caractère personnel (art.405), le législateur contraint le responsable à observer les règles essentielles en matière de protection des données personnelles. Il s'agit entre autres du :

  - principe du consentement et de légitimité ;
  - principe de transparence ;
  - principe de confidentialité et de sécurité ;
  - principe de responsabilité du responsable de traitement.

- Obligations nouvelles à la charge du responsable de traitement

  - Obligations en cas de responsabilité conjointe du traitement (art. 388) ;
  - Obligation du responsable du traitement dans la collecte indirecte des données (art. 416) ;
  - Réalisation de l'analyse d'impact par le responsable de traitement avant la mise en œuvre de certains traitements (art.428-429) ;
  - Respect des différents droits des personnes concernées par le traitement ;
  - Tenue d'un registre des activités liées au traitement (art. 435) ;
  - Rapport annuel à établir et à transmettre à l'APDP (art. 387) ;
  - Désignation d'un délégué à la protection des données à caractère personnel (art. 430-431-432).

La loi a aussi prévu d'autres dispositions faisant intervenir le Conseil des Ministres dans certains cas de transfert des données personnelles vers des Etats ou Organisations Internationales ne présentant pas les garanties requises en matière de protection des données personnelles. Ainsi, « Sans préjudice des dispositions de l' article 391, le Conseil des ministres peut, par décret et après avis conforme de l'Autorité, autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un État tiers ou une organisation internationale n'assurant pas un niveau de protection adéquat et suffisant, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants. »

## C. De l'exercice des droits des personnes concernées

- Droit au consentement (art. 389, 390) qui donne une légitimité au traitement si la personne concernée donne son consentement ;
- Droit d'interrogation (art. 439) ;
- Droit à l'oubli (art. 443) ;
- Droit à la portabilité des données (art. 438).

De même, en ce qui concerne l'exercice des droits d'accès, d'opposition, de rectification et de suppression, des délais sont désormais impartis aux responsables de traitement pour leur mise en œuvre.

Ainsi, en cas d'exercice d'un de ces droits, le responsable du traitement, après avoir reçu une demande datée, signée et transmise par voie postale ou électronique de la personne concernée par le traitement, doit :

- Communiquer sans délai et au plus tard dans les soixante (60) jours de la réception de la requête, une copie des renseignements demandés dans le cas du droit d'accès (art. 437) ;
- Indiquer dans les trente (30) jours qui suivent la réception de la requête, la suite réservée à la demande de la personne concernée en cas d'exercice du droit d'opposition (art. 440) ;
- Communiquer les rectifications ou effacements des données effectués à la personne concernée dans les quarante-cinq (45) jours qui suivent la réception de la requête dans le cas d'exercice des droits de rectification et de suppression (art. 441).

Relativement aux mesures de sécurité physique et logique, le code du numérique a mis un accent particulier sur les normes de sécurité et de confidentialité auxquelles doivent se conformer les responsables de traitement.
Le nouvel environnement du numérique reste influencé par des réformes extérieures comme c'est le cas du Règlement Général sur la Protection des Données Personnelles (RGPD).

# II- Le Règlement Général sur la Protection des Données Personnelles (RGPD) dans le cadre européen et ses implications hors Union Européenne

Le Règlement général sur la protection des données personnelles, connu sous le sigle RGPD constitue une réforme d'harmonisation du cadre juridique européen en matière de protection des données personnelles.

Le Règlement Général sur la Protection des Données (RGPD) relatif à la protection des données des personnes physiques à l'égard du traitement des données et à la circulation de ces données, est entré en vigueur le 25 mai 2018. Ses dispositions ayant vocation à moderniser le cadre européen afin de prendre en compte les avancées technologiques, sont applicables dans l'ensemble des Etats membres afin de réduire les écarts juridiques entre les différentes législations.

Bien qu'applicable à l'ensemble des Etats membres de l'Union Européenne (UE), le RGPD a un impact sur l'environnement juridique des pays hors UE, y compris le Bénin.

## A. Le RGPD : Un changement de paradigme dans la mise en conformité

Dans son ensemble, le Règlement conserve les grands principes de protection des données personnelles. Toutefois il réduit de façon significative les formalités préalables auprès des autorités de contrôle, en les remplaçant par des obligations de conformité plus accrues. Ainsi, il est mis à la charge du responsable de traitement ou du sous-traitant l'obligation de prendre en compte les préoccupations liées à la protection des données, dès la conception du traitement ou du produit, de documenter ces derniers et de tenir un registre récapitulant toutes les données traitées.

L'application du Règlement au-delà de l'Europe apparaît principalement comme un moyen de pression pour mieux cerner l'action des Fab Five (Google, Apple, Facebook, Amazon et Microsoft), des sites d'e-commerce et des prestataires de publicités ciblées jusque-là à l'abri de la régulation mais également d'encadrer la délocalisation des entreprises européennes traitant de données personnelles hors UE, notamment en Afrique.

## B. Le renforcement des droits des citoyens

Un des objectifs du législateur européen est d'obliger les entreprises à mieux communiquer sur la collecte et l'usage des données. Dès lors, certains droits existants ont été consolidés et renforcés par de nouveaux mécanismes. De manière non exhaustive, on peut citer au bénéfice de ses droits :

- Le droit à l'autodétermination informationnelle, c'est-à-dire le droit pour toute personne de décider et de contrôler l'utilisation de ses données à caractère personnel et les modalités de l'exercice des droits de la personne concernée ;
- La transparence des informations et communications et un consentement éclairé requis à chaque étape;
- L'exercice d'un droit à l'effacement « droit à l'oubli ». La clause du RGPD relative au « droit à l'oubli » oblige les établissements à supprimer de leurs systèmes toutes les données d'un client si celui-ci le demande ;
- Le droit à la limitation (voire minimisation) du traitement en termes de données collectées et d'utilisation ultérieure ;
- Le nouveau droit à la portabilité des données qui permet aux personnes concernées de transférer les données personnelles d'un prestataire de services, par exemple un réseau social, à un autre ;
- La réparation des dommages matériels et moraux par un recours collectif des victimes dans le périmètre spécifique de la protection des données.

## C. L'impact géopolitique : Le transfert des données hors UE

Afin de faciliter la prise en compte des nouvelles règles concernant le transfert de données hors UE (Article 44), le Règlement prévoit la possibilité de se fonder sur un code de conduite (Binding Corporate Rules) par secteur d'activité, contribuant à l'application du Règlement ou sur un label/certificat. Le Règlement affirme par ailleurs expressément, qu'un transfert hors UE ne peut être imposé par les lois et règlements d'un pays tiers à l'UE.

Aujourd'hui utilisés que par les Autorités de protection européennes pour des transferts de données vers des pays situés en dehors de l'UE, ces outils demeurent incontournables pour réguler la gestion des données, même au-delà de l'Europe.

Il existe des Règles d'Entreprise Contraignantes applicables aux responsables de traitement pour les transferts vers des entreprises qui agissent en qualité de responsables de traitement et des Règles d'Entreprise Contraignantes à la charge des sous-traitants pour les transferts vers des sous-traitants hors UE.

## D. L'encadrement des flux de données

En quoi les Règles d'Entreprise Contraignantes permettent t'elles aux autorités de protection comme l'APDP de tester le niveau de conformité à sa réglementation des données à caractère personnel ?

Si des Règles d'Entreprise Contraignantes sont acceptées par les Autorités européennes par le biais de la reconnaissance mutuelle, l'entreprise (responsable de traitement ou sous-traitant) établie au Bénin par exemple qui applique lesdites règles peut saisir l'APDP pour l'homologation de ces règles au regard de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin. Toutefois l'homologation des Règles d'Entreprise Contraignantes n'exonère pas l'entreprise de ses obligations déclaratives, notamment si elle souhaite transférer des données vers un pays tiers.

Concrètement, les entreprises béninoises gérant la clientèle européenne en matière de gestion de la relation client (Télécommunications, E-commerce, Banques, Assurances et autres) doivent appliquer le RGPD. Par ailleurs, ils ne sont pas exonérés de leurs obligations déclaratives au niveau de l'Autorité de Protection des Données à caractère Personnel.

Ces mesures vont permettre de prendre convenablement en compte les obligations de sécurité et de confidentialité qui seront mis en exergue dans le contrat de sous-traitance. Mais, pour une meilleure prise en compte il faut que les employés de ces sous-traitants saisissent l'enjeu de cette protection ; dans ce cas de figure, une responsabilisation des agents au front office est vivement recommandée. Mieux, il faut répercuter l'obligation de sécurité et de confidentialité dans les contrats des agents.

Les Autorités africaines peuvent, à l'instar de ce qui se fait dans l'UE, avoir des accords de reconnaissance mutuelle avec les autorités chef de file européennes. De ce fait, les entreprises peuvent appliquer des Règles d'Entreprise Contraignantes (article 40 RGPD) reconnues par les Autorités européennes et celles africaines.

En définitive, l'Europe, au travers du RGPD envoie au monde ses valeurs en matière de protection de la vie privée afin de mieux protéger ses nationaux contre l'usage abusif du traitement des données. L'évolution de ce cadre européen de référence en la matière doit amener les acteurs du digital à faire preuve de responsabilité à l'égard des citoyens mais aussi

doit amener les entreprises à mettre en avant leur conformité en tant qu'avantage concurrentiel et d'inventer de nouveaux modèles économiques dans leurs stratégies de gestion des données personnelles.

En ce qui concerne les pays africains, le RGPD provoquera indubitablement pour eux une incitation à leur mise en conformité plus accrue. Aussi, doivent-ils s'engager de façon proactive à diffuser, voire apprivoiser la culture informatique et libertés. Ceci doit passer prioritairement par une simplification des formalités déclaratives pour mieux protéger les droits et libertés fondamentaux afin de ne plus être à la traîne lors de prochains bouleversements de la gouvernance des données.

Dans ce domaine du numérique, comme dans tant d'autres, il vaut mieux prévenir que guérir.

## E. Le RGPD au-delà de l'UE

Le RGPD a un champ d'application qui va au-delà du cadre de l'Union Européenne : un champ d'application extraterritorial et un champ d'application extranational.

- **Champ d'application extranational**

  Le RGPD s'applique aux traitements de données personnelles de citoyens européens mais également des citoyens non européens, dès lors qu'il s'agit de traitements effectués sur le territoire européen.

- **Champ d'application extraterritorial**

  Le RGPD s'applique aux traitements effectués par des acteurs non établis sur le territoire de l'UE, dès lors qu'il vise des personnes se trouvant sur le territoire de l'Union Européenne. Ces traitements peuvent concerner, soit des offres de biens et services, soit le suivi de comportements au sein de l'UE.

A titre d'illustration, une entreprise béninoise qui commercialise des produits ou des services à destination de citoyens européens sans pour autant être présente sur le territoire de l'Union européenne sera assujettie au règlement et devra s'y conformer.


RÉPUBLIQUE DU BÉNIN
AUTORITÉ DE PROTECTION DES DONNÉES
À CARACTÈRE PERSONNEL (A. P. D. P.)
E-mail: contact@apdp.bj 01BP: 04837 Cotonou Tél:(+229) 21 32 57 88 / 69 55 00 00 Site Web: www.apdp.bj
179

# PARTIE - II

## LES ACTIVITES DE L'APDP AU COURS DE L'ANNEE 2018

# I. Les activités de régulation

L'année 2018 a été marquée par la promulgation de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.

L'avènement de cette loi a eu un impact sur l'organisation et les modalités de fonctionnement des directions et services de l'APDP.

Pour se conformer aux prescriptions de la loi n° 2017-20 du 20 avril 2018 certaines structures aussi bien publiques que privées ont saisi l'APDP aux fins de déclarations et de demandes d'autorisations relativement à la mise en œuvre de collecte et de traitement des données à caractère personnel. Aussi l'APDP a-t-elle été saisie de demandes d'avis.

Pour faire suite à ces demandes, l'APDP a adopté du 1er Janvier au 31 Décembre 2018, quarante-huit (48) délibérations portant sur des demandes d'autorisations, d'avis et sur des déclarations.

## A. Les autorisations

### 1- Délibération n°2018-001/AT/CNIL du 28 février 2018 portant autorisation de traitement des données à caractère personnel alphanumériques du personnel de Canal+Bénin.

Le Directeur Général de la société Canal+ Bénin, a saisi la CNIL d'une demande d'autorisation en vue de la collecte et du traitement manuel et électronique des données à caractère personnel alphanumériques des employés de ladite société.

Le traitement a été autorisé par la Commission.

## 2- Délibération n°2018-002/AT/CNIL du 28 février 2018 portant autorisation de traitement des données à caractère personnel alphanumériques du personnel de CanalBox Bénin.

L'Administrateur Général Adjoint de CanalBox Bénin a saisi la Commission d'une demande d'autorisation aux fins de collecte et du traitement manuel et électronique des données à caractère personnel alphanumériques de ses employés.

Sous réserve des injonctions prononcées et de la prise en compte de recommandations faites, la CNIL a autorisé l'Administrateur Général de CanalBox Bénin à procéder au traitement objet de la requête.

## 3- Délibération n° 2018-003/AT/CNIL du 14 mars 2018 portant autorisation de collecte et de traitement par le Cabinet Militaire du Président de la République, des données alphanumériques et biométriques du personnel et partenaires/prestataires de services de Présidence de la République.

Le Directeur du Cabinet Militaire du Président de la République a sollicité une autorisation de la Commission Nationale de l'Informatique et des Libertés, en vue du traitement automatisé des données alphanumériques et biométriques du personnel et partenaires/prestataires de services de la Présidence de la République.

La finalité poursuivie par le traitement envisagé est d'assurer la sécurité du site de la Présidence de la République en procédant à l'identification du personnel et des partenaires/prestataires de services autorisés à y accéder.

Le requérant a été autorisé par la CNIL a effectué le traitement objet de la requête.

## 4- Délibération n° 2018-004/AT/CNIL du 11 avril 2018 portant autorisation de traitement des données alphanumériques et biométriques des clients et des usagers de SAM AY S.a.r.l

Le Directeur Général de SAM AY S.a.r.l a sollicité une autorisation en vue du traitement automatisé des données alphanumériques et biométriques de ses clients et usagers.

Les finalités poursuivies par le traitement des données à caractère personnel des clients de la société sont entre autres l'assistance technique des clients, la gestion rationnelle et efficace de la base de données clients, etc.

Sous réserve des injonctions prononcées et de la prise en compte de recommandations faites, le Directeur Général de SAM AY S.a.r.l a été autorisé par la Commission à procéder au traitement objet de la requête.

## 5- Délibération n°2018-005/AT/APDP du 27 décembre 2018 portant autorisation de collecte, de traitement et de transfert de la base de données clients des abonnés de MTN Mobile Money vers le Ghana

L'APDP a été saisie par le Directeur Général de MTN Mobile Money, d'une demande d'autorisation aux fins de collecte, de traitement et de transfert des données alphanumériques de ses abonnés du Bénin vers le Ghana.

MTN Mobile Money indique que la finalité poursuivie par le traitement envisagé est d'assurer la synchronisation et la réplication des données à caractère personnel en vue de la restauration de la base de données en cas de sinistre ou d'incident.

Le requérant a été autorisé par l'APDP à procéder au transfert de données à caractère personnel objet de la demande d'autorisation.

## 6- Délibération n° 2018-006/AT/APDP du 27 décembre 2018 portant autorisation de collecte et de traitement des données alphanumériques et biométriques des propriétaires et présumés propriétaires de parcelles dans la Commune d'Abomey-Calavi.

Le Maire de la Commune d'Abomey-Calavi, dans le cadre de la constitution d'une base de données des propriétaires et présumés propriétaires de parcelles de la Commune qu'il administre, a saisi l'APDP d'une requête aux fins de l'autoriser à procéder à la création de ladite base.

A l'issue de l'examen en plénière de la requête, le Maire de la Commune d'Abomey-Calavi a été autorisé à procéder à la constitution de la base de données sous réserve d'injonctions et recommandations.

# B. Les déclarations

## Déclarations simples

### 1- Déclaration de la base de données du Compendium des compétences féminines du Bénin (RD n° 034-2018/APDP/Pt/SG/DAJC/SA du 10 décembre 2018)

Le Ministère des Affaires Sociales et de la Microfinance (MASM) à travers son Directeur de l'Informatique et du Pré-archivage a saisi l'Autorité d'une déclaration relative à la création de la base de données à caractère personnel du compendium des compétences féminines du Bénin.

L'APDP a pris acte de la déclaration du requérant et, à travers le Récépissé de Déclaration délivré a fait des recommandations relatives à la durée de conservation et à la sécurisation des données personnelles traitées.

### 2- Déclaration de la base de données des étudiants, des enseignants-chercheurs et des Agents administratifs, Techniques et de Service (ATS) de l'Université de Parakou

Le Recteur de l'Université de Parakou a déclaré auprès de l'APDP, les bases de données des étudiants, Enseignants-Chercheurs et des Agents administratifs, Techniques et de Services (ATS) de l'Institution dont il est responsable.

Sous réserve de recommandations, l'Autorité a donné son accord relativement aux traitements déclarés.

# Déclarations de système de vidéosurveillance

## 1- Société Générale Bénin (SGB) : requête aux fins de prorogation du délai de conservation des données personnelles issues des caméras de vidéosurveillance (RD n° 021-2018/APDP/Pt/SG/DAJC/SA du 05 septembre 2018)

Le Directeur Général de la Société Générale Bénin, suite aux difficultés rencontrées dans la mise en application de l'injonction prononcée par l'APDP relativement à la durée de conservation des données à caractère personnel provenant des images et sons enregistrés par les caméras de vidéosurveillance installés au siège et dans les agences de la banque, a sollicité une autorisation aux fins de prorogation dudit délai de conservation.

De l'analyse du dossier et conformément aux dispositions de l'article 383.6 du code du numérique, la requête de la SGB a été jugée pertinente et justifiée. L'APDP a donc fait droit à la banque en l'autorisant à conserver les données objet de la requête, pour une durée bien définie.

Un récépissé de déclaration a été délivré au requérant.

## 2- Déclaration du système de vidéosurveillance au siège et dans les agences de SPACETEL Bénin S.A (RD n° 026/APDP/Pt/SG/DAJC/SA du 05 décembre 2018)

La société SPACETEL Bénin S.A a déclaré à l'Autorité de Protection des Données à caractère Personnel (APDP), un traitement de données à caractère personnel portant sur les images et sons enregistrés par le système de vidéosurveillance installé à son siège et dans ses agences (115 caméras).

Un récépissé de déclaration a été délivré sous réserve de ce que le requérant saisisse l'APDP dans un délai deux (02) mois, une déclaration de conformité portant sur l'engagement à respecter les injonctions et recommandations faites.

## Déclarations de site web

### 1- Déclaration du site web du Ministère des Affaires Sociales et de la Microfinance (MASM) (RD n° 029/APDP/Pt/SG/DAJC/SA du 14 décembre 2018)

Le Directeur de l'Informatique et du Pré-archivage du MASM a également déclaré à l'Autorité qu'il procède au traitement de données à caractère personnel sur le site web « www.social.gouv.bj » aux fins informer le public sur les actions et les services offerts par ledit Ministère.

Un récépissé de déclaration a été délivré sous réserve de ce que le requérant saisisse l'APDP, dans un délai deux (2) mois, une déclaration de conformité portant sur l'engagement à respecter les recommandations faites.

### 2- Déclaration du site web de la Bank of Africa Bénin (BOA-Bénin) (RD n° 012/APDP/Pt/SG/DAJC/SA du 12 juillet 2018)

Le Directeur Général de la BOA-Bénin a saisi l'Autorité d'une déclaration de traitement de données à caractère personnel sur son site web dénommé « https://www.boabenin.com».

Un récépissé de déclaration contenant des recommandations a été délivré au requérant.

# C. Les plaintes

### 1- Plainte relative au chantage à la webcam

L'APDP a reçu une plainte provenant d'un individu de nationalité algérienne contre un ressortissant béninois supposé demeuré à Parakou. Le plaignant a sollicité l'intervention de l'APDP afin que les menaces dont il était l'objet de la part du béninois cessent.

A l'issue de l'instruction de la requête par les services techniques de l'Autorité, il a été révélé qu'il s'agissait d'un acte cybercriminel. Le dossier a été transmis à l'Office Central de Répression de la Cybercriminalité (OCRC) du Bénin pour la suite.

### 2- Plainte relative à la diffusion sans consentement de données personnelles sur internet

L'APDP a enregistré le 14 février 2018, une plainte provenant d'une personne physique contre une société de gardiennage et de sécurité de la place.

En effet, Monsieur X affirmait que ses données personnelles notamment des numéros de téléphone, figureraient sur le lien internet de son ancien employeur, bien que la relation de travail entre les deux parties ait été rompue depuis fort longtemps. Les numéros de téléphone affichés avaient pour conséquence de troubler la quiétude du plaignant étant donné qu'il recevait une multitude d'appels de façon régulière. Bien qu'il se soit adressé à la société de gardiennage aux fins de retrait de ces données, ses réclamations sont restées vaines.

La société de gardiennage mise en cause ayant finalement retiré les données à caractère personnel du plaignant de son site web, le dossier a été classé.

## D. Les avis

L'Autorité a été appelée à émettre son avis sur une requête à elle adressée par un opérateur de téléphonie mobile établi au Bénin.

Compte tenu du caractère sensible des informations communiquées et du traitement envisagé, l'avis requis par le responsable du traitement a été donné par l'APDP dans la stricte confidentialité.

## E. Le contrôle des traitements

L'activité de contrôle la plus importante au cours de l'année 2018 a été celle du Recensement Administratif à Vocation d'Identification de la Population (RAVIP). En effet, l'APDP a effectué sur toute l'étendue du territoire national une mission de contrôle dans le cadre des opérations du RAVIP, mission consistant à vérifier la régularité des traitements des données des populations.

***Mission de contrôle dans le cadre du déroulement du Recensement Administratif à Vocation d'Identification de la Population ( RAVIP) dans les départements du Bénin***

Les vérifications ont porté sur l'environnement des opérations du RAVIP, la méthodologie de l'enregistrement des données et leur sécurisation.

### Contrôle de l'environnement des opérations

Ce contrôle a consisté à :

- Récupérer une copie de la fiche de collecte des informations ;
- vérifier le contenu des fiches d'enregistrement des données à caractère personnel collectées ;
- relever sur chaque fiche les informations pertinentes (Ethnie, origine raciale, religion, appartenance politique et syndicale) ;
- collecter les références des équipements d'enregistrement (Référence, fonction, fournisseur, logiciel de collecte de cryptage, logiciel de protection contre les intrusions, etc…).

### Méthodologie d'enregistrement

Il s'est agi de vérifier :

- Le type de données collectées (Alphanumérique, numérique, etc…) ;
- la forme d'enregistrement des adultes (questionnaire, renseignement directe, témoignage, etc…) ;
- la forme d'enregistrement des mineurs (par personne interposée, parents et autres, etc…) ;
- la vérification per les membres des formes d'enregistrement biométriques sur le terrain (empreinte digitale, nombre de doigts, photo, etc…);
- le niveau d'implication des agents du fournisseur des équipements au processus de collecte.

### Sécurisation des données collectées

Le contrôle à ce niveau a permis à l'APDP de :

- S'assurer de la présence effective et du profil de chaque responsable de traitement sur le site ;

- S'assurer de la présence effective et du profil de chaque responsable de traitement sur le site ;
- s'informer sur le niveau intellectuel des agents collecteurs et de la formation reçue dans le cadre du RAVIP ;
- vérifier les mesures de sauvegarde des données collectées (dispositif de sauvegarde avant transfert) ;
- vérifier la méthode de transfert des données (au fil de l'eau ou différer, logiciel ou protocole de cryptage et de transfert) ;
- s'informer sur le traitement des données (lieu et matériels) ;
- apprécier le niveau d'implication des agents du fournisseur des équipements et des agents de collecte ;
- apprécier les mesures de sécurité des locaux d'entreposage des formulaires déjà renseignés.

A l'issue du contrôle, certains constats ont été faits et des recommandations ont été formulées à l'endroit des acteurs.

# II- Les activités d'information et de sensibilisation

## A. Les actions tendant à la visibilité de l'Institution

Pour le compte de l'année 2018, l'APDP a :

- réalisé deux (02) enseignes lumineuses pour faciliter la reconnaissance du bâtiment abritant son siège ;
- réalisé et diffusé sur les chaines de télévision et de radiodiffusion d'un spot (téléfilm de 65 secondes) intitulé « **Partager Partager** » pour sensibiliser les populations sur la diffusion des données personnelles sur les réseaux sociaux ;
- organisé une campagne d'information, d'éducation et de communication sur les chaines de radio et de télévision dénommée « **Mes Données Personnelles, C'est Moi Qui Décide** ».

## B. Les missions de sensibilisation

Au plan national, l'Autorité de Protection des Données à caractère Personnel a participé à plusieurs ateliers et forums de discussions relatifs au numérique et à la protection des données personnelles et de la vie privée.

Aussi, a-t-elle été bien présente dans nombre de débats télévisés et interviews sur les chaines de télévision et de radiodiffusions nationales.

L'APDP a organisé des séances de sensibilisation dans les universités, collèges d'enseignement secondaire du Bénin et dans d'autres structures sur le plan national. Au nombre de ces missions nous pouvons citer :

- La mission de sensibilisation tenue à l'IUT Lokossa avec les étudiants et enseignants dans le cadre de la célébration de la journée internationale de la protection des données personnelles ;

## *Sensibilisation des élèves et étudiants sur la protection des données à caractère personnel*

- la mission de sensibilisation tenue à Cotonou (Etablissement scolaire dénommé «Cours de Soutien de Cotonou») avec les élèves et les enseignants ;

- la mission de sensibilisation tenue à Abomey aux Collèges Sainte Thérèse et Pythagore d'Abomey ;

- la mission de sensibilisation tenue à l'École Nationale d'Administration et de Magistrature (ENAM) sur le thème : les données personnelles, usages, risques et protection ;

- la mission de sensibilisation tenue à Cotonou sur le thème la protection du consommateur et la protection des données à caractère personnel dans le cadre de la 17ème session de formation initiale du CIFAF (Centre International de Formation en Afrique des avocats Francophones) ;

- l'organisation de séances d'information et communication sur la protection des données personnelles dans le cadre de la sécurité publique au profit de la Police Républicaine ;

- la participation de l'APDP à un atelier sur le thème : numérique et relations professionnelles en République du Bénin au profit de l'Association pour la Promotion des Droits Fondamentaux au Travail (APDFT) ;

- la sensibilisation du conseil communal sur la collecte et le traitement des données Alphanumériques et biométriques à la mairie de Abomey-Calavi;

- le message de sensibilisation sous forme de sketch sur les chaines de télévision, des radios et sur les réseaux sociaux ;

- la mission de sensibilisation et de contrôle à la Préfecture d'Abomey.

***Animation d'un atelier sur la protection des données personnelles dans le cadre de la sécurité publique***

# III- Autres activités de fonctionnement de l'APDP

## A. La tenue régulière des sessions plénières

Au titre de l'année 2018, l'APDP a pu organiser une vingtaine de sessions plénières qui ont permis à l'Autorité d'accroître considérablement le nombre de dossiers traités. Ces dossiers dont le point est fait précédemment portent sur des déclarations, des demandes d'autorisation et d'avis, des plaintes et autres.

## B. La participation de l'APDP aux séminaires et ateliers

L'APDP a répondu présente à de nombreux ateliers et séminaires organisés en 2018. Au nombre de ces activités, on peut citer :

- La semaine du Numérique au Bénin édition 2018 organisé par le MENC;
- le projet d'installation d'une plateforme block Chain au Bénin organisé par le MENC;
- le Workshop sur l'intelligence artificielle à l'Université d'Abomey-Calavi;
- la journée Technologique du Bénin organisée par Oracle et CFAO Bénin;
- le projet e-Gouvernance au Bénin organisé par l'Agence des Services et Systèmes d'Information (ASSI);
- le forum des DSI organisé par le club DSI-Bénin;
- la séance d'échange et de travail avec l'ARCEP Bénin sur « Etude portant sur les perspectives des Internet of Things (IoT) en République du Bénin ».

Ces rencontres ont permis à l'APDP de souligner l'importance de la protection des données à caractère personnel, de rappeler ses missions et d'insister sur les droits des citoyens ainsi que les devoirs des responsables de traitement.

## C. Le renforcement du cadre organisationnel

Le cadre institutionnel et organisationnel de l'APDP a été renforcé au cours de l'année 2018 par la mise en place de plusieurs outils et documents de gestion. Il s'agit :

- De la finalisation et de l'adoption du manuel de procédures administrative, financière et comptable dont les travaux d'élaboration ont commencé en 2017 ;
- de l'élaboration et de l'adoption du règlement financier ;
- de l'élaboration et de la transmission à la Chambre des comptes de la Cour Suprême de divers documents de réédition des comptes ;
- des travaux de révision et de mise en conformité du règlement intérieur à la loi ; 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin ;
- du démarrage en collaboration avec les services techniques du Ministère du Travail et de la Fonction Publique, des travaux d'élaboration du document portant accord d'établissement de l'APDP ;
- de la mise en place des organes de passation et de contrôle des marchés publics.

## D. Le renforcement de l'effectif du personnel

Pour remédier au déficit de l'effectif du personnel, des agents ont été recrutés et mis à la disposition du secrétariat général, du service juridique et de la direction financière. Trois (03) stagiaires ont également été admis à l'APDP pour combler le déficit en personnel.

## E. L'édition de différents documents

La promulgation de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin a induit la mise à jour des documents de l'Autorité.

L'APDP s'est chargée de l'édition de plusieurs documents. Au nombre de ces documents on peut citer :

- La conception du logo de l'APDP;
- la loi n° 2017-20 portant code du numérique en République du Bénin;
- les flyers pour les sensibilisations de la population;

## F. La mise à jour des formulaires de l'APDP

Au cours de l'année 2018, l'APDP a procédé à une mise à jour de tous ses formulaires suite à la promulgation de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin. Cette opération consiste à renforcer les mesures de sécurité et les droits des béninois comme l'exige le code du numérique.

L'APDP a également élaboré de nouveaux formulaires pour les contrôles sur le terrain, en ligne des sites web à distance et des grilles d'évaluation de site web.

## G. L'amélioration du cadre informatique

### Acquisition de matériels informatiques

Au titre de l'année 2018, l'APDP a procédé à l'acquisition de divers matériels informatiques (Imprimantes réseau, supports de sauvegarde, ordinateurs de bureau de hautes performances, onduleurs de 1.5 kva et ordinateurs portables) dans le but de renforcer les ressources informatiques et de sécuriser les équipements du réseau.

L'Autorité s'est équipée d'un appareil photo numérique pour la couverture de ses missions et pour l'animation de son site web.

### Evolution du réseau informatique

L'année 2018 a été également marquée par des acquisitions majeures et la volonté de diversifier les missions du service informatique.

Les services techniques de l'APDP assurent au quotidien la bonne marche et la continuité du réseau de desserte de hauts débits de 5 Mbps. La maintenance des équipements de réseau et de la liaison internet a été effectuée deux (02) fois en 2018 conformément aux termes du contrat signé avec le prestataire.

### Déploiement et mise à jour du nouveau site web de l'APDP

La promulgation de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin a induit un changement du nom CNIL en APDP. Cette situation a conduit l'APDP à migrer le site internet initial www.cnilbenin.bj vers le nouveau site www.apdp.bj.

### Numérisation des documents de l'APDP

Dans la perspective de déployer une plateforme collaborative à l'APDP, les travaux de numérisation de tous les rapports annuels d'activités et de toutes les délibérations depuis 2010 ainsi que leurs dossiers d'analyse ont été réalisés. Ce travail apporte une plus-value car il permet de disposer de la version numérisée des documents, pour toute autre exploitation.

# IV- Les activités de l'APDP au plan régional et international

Au cours de l'année 2018 l'APDP a été très active aux plans africain et mondial.
Elle a pris part à diverses rencontres tant au plan régional qu'international. On peut citer :

- La conférence internationale sur la protection de la vie privée et des données personnelles en Afrique, tenue à Casablanca (Maroc) en février 2018 ;
- le séminaire international de formation sur « le Règlement Général sur la Protection des Données Personnelles (RGPD) et son impact dans l'environnement africain » tenu au Burkina Faso en juillet 2018 ;
- la 12ème Assemblée Générale de l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP) et la réunion annuelle des autorités francophones de protection des données personnelles tenues à Paris en octobre 2018;
- l'atelier de validation du rapport sur la mise à jour des études sur le visa unique de l'UEMOA, tenu au Burkina Faso en octobre 2018 ;

*12ème Assemblée Générale de l'AFAPDP (Paris, octobre 2018)*


# Internet n'est pas un confident !

**Préservez autant que posssible vos informations personnelles et votre vie privée.**

# V- La contribution du Commissaire du Gouvernement aux activités de l'APDP

La loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin en son article 465, dispose qu'« un Commissaire du Gouvernement, désigné par le Président de la République en conseil des ministres, siège auprès de l'Autorité…».

Dès sa nomination, le Commissaire du Gouvernement, prenant la mesure de son rôle, a servi d'interface entre l'Autorité et les administrations, notamment le pouvoir exécutif.

Par ailleurs, le Commissaire du Gouvernement a donné son avis sur tous les projets de délibération relativement aux demandes (autorisations, et avis) dont l'APDP a été saisie.

En outre, le Commissaire du Gouvernement s'est investi dans plusieurs activités relevant de ses attributions à savoir :

- Présenter les observations du Gouvernement lors des séances de l'APDP ;
- assister les personnes morales de droit public et celles de droit privé gérant un service public à l'accomplissement des formalités préalables liées aux déclarations, aux demandes d'avis ou d'autorisations dans le cadre de la mise en œuvre d'un traitement de données personnelles ;
- informer et conseiller les ministères sur l'ensemble des questions touchant à la protection des libertés dans les traitements informatiques des administrations ;
- coordonner le rôle des ministères dans la protection des données personnelles ;
- apporter son concours aux services du Président de la République sur tout sujet intéressant les traitements automatisés et la protection des données à caractère personnel.

# VI- Le point d'exécution du budget de l'APDP au 31 Décembre 2018

Au titre de la gestion 2018, l'Autorité de Protection des Données à caractère Personnel a bénéficié de l'Etat, une subvention d'un montant de trois cent cinquante-trois millions trois cent cinquante-deux mille (354 352 000) FCFA.

Au 31 décembre 2018, le budget a été exécuté à hauteur de trois cent quarante-sept millions six cent quarante-sept mille six cent soixante-dix-sept (347 647 677) FCFA, soit un taux d'exécution de 98,11% comme indiqué dans le tableau ci-dessous.

| RUBRIQUE | PREVISIONS | REALISATION | "TAUX D'EXECUTION (%)" | OBSERVATIONS |
|---|---|---|---|---|
| DEPENSES DU PERSONNEL | 233 382 000 | 228 275 000 | 97,81 | |
| ACHATS DE BIENS ET SERVICES | 102 312 200 | 101 775 677 | 99,48 | |
| ACQUISITIONS DES EQUIPEMENTS | 18 657 800 | 17 597 000 | 94,31 | |
| TOTAL | 354 352 000 | 347 647 677 | 98,11 | |

# VII. Les difficultés et les perspectives

Les résultats obtenus au titre des activités de l'année 2018 ont été possibles grâce à la participation active de tous les acteurs de l'APDP et au soutien appréciable du Gouvernement qui a mis à disposition la totalité des prévisions budgétaires de l'exercice.

Malgré ces efforts, certaines faiblesses ont caractérisé le fonctionnement de l'Autorité et méritent d'être mises en relief.

En effet, au regard des missions assignées et des actions qui en découlent, on note une insuffisance prononcée des ressources humaines, matérielles et financières ; ce qui a handicapé de façon considérable les activités de l'Autorité.

S'agissant du niveau de protection des données personnelles des populations, il y a lieu d'indiquer qu'en dépit des nombreuses séances de sensibilisation et d'information, des organismes tant publics que privés continuent de traiter les données au mépris des prescriptions de la loi et en violation des droits des personnes concernées. En cela, les fruits n'ont pas pleinement porté la promesse des fleurs.

Par ailleurs, l'absence d'une plateforme collaborative est source de lenteur dans le traitement diligent des dossiers.

Au plan financier, la difficulté majeure rencontrée au cours de l'année 2018 est l'insuffisance de ressources financières. Faute de ressources, des activités qui pourtant avaient été jugées importantes et prioritaires, ont dû être reportées en 2019, avec l'espoir d'une amélioration sensible des moyens financiers alloués. A ce niveau, il convient d'indiquer que les crédits réservés à l'acquisition des biens et services ne représentent que 34,13% de la subvention d'exploitation, cela n'a pas permis à l'Autorité de faire face aux besoins d'acquisition de biens de première nécessité.

Par ailleurs, il y a lieu de souligner la prise en charge en plein exercice, sur le budget de l'APDP, de certaines dépenses, notamment le paiement des primes spécifiques et de rendement aux agents de l'État en service à l'APDP. Ces dépenses supplémentaires sont consécutives à l'autonomie financière conférée à l'Autorité.

Pour pallier les difficultés sus évoquées, certaines pistes de solution sont envisageables. Il s'agit de :

- Renforcer les séances de sensibilisation tant à l'endroit des responsables de traitement intervenant dans divers secteurs d'activités que des populations elles-mêmes sur la nécessité et les exigences de protection de la vie privée ;

- procéder au recrutement du personnel qualifié pour mettre l'APDP au diapason des nouvelles technologies et des enjeux actuels de la protection des données personnelles ;

- organiser des séances de formation et outiller le personnel aux techniques d'instruction des différentes requêtes;

- effectuer des contrôles réguliers afin de s'assurer du respect, par les responsables de traitement, des prescriptions de la loi ainsi que des recommandations et injonctions contenues dans les délibérations de l'Autorité;

- poursuivre le plaidoyer afin de mettre à la disposition de l'Autorité, un budget plus conséquent, à même de lui permettre d'accomplir au mieux sa mission de protection des données personnelles dans le contexte actuel de développement exponentiel des technologies de l'information et de la communication avec les risques induits auxquels sont exposés les utilisateurs.

# *Présentation du budget APDP 2018 à l'Assemblée Nationale du Bénin*

# PARTIE - III

## QUESTION D'ACTUALITE

## *LE TELEPHONE ET LA VIE PRIVÉE*

**PAR Me YVON DETCHENOU**

**A L'OCCASION DES 2EMES JOURNEES NATIONALES DE L'INFORMATIQUE ET DES LIBERTES**

# INTRODUCTION

Un téléphone mobile est un appareil électronique permettant d'échanger des communications sans fil ou par onde radioélectrique (fréquences). Ainsi définie, l'expression « téléphone mobile » pourrait limiter les perspectives de la réflexion à la seule fonction vocale d'usage de ces terminaux mobiles alors qu'ils sont devenus de vrais condensés de technologie, des outils informatiques dotés ou capables de fonctions ou services intelligents (smartphones). Cette intelligence est la capacité des équipements embarqués associés ou non à des services à distance, à gérer des paramètres de notre vie quotidienne et pour cela à mémoriser nos activités, nos conversations, nos goûts, nos centres d'intérêts ou nos habitudes, à transmettre nos écrits et nos émotions, nos déplacements, à s'immiscer dans l'intimité de nos vies pour mieux nous servir. Ainsi, les évolutions techniques ont à ce point changé l'outil téléphone que son mode d'utilisation est en mesure de dévoiler des éléments d'informations sensibles, personnelles, intimes relevant en principe de la vie privée des personnes ou protégées comme telles. La vie privée désigne précisément par opposition à la vie publique, la sphère des activités de la personne qui relève de l'intimité et de la dignité humaine et qu'il conserve ou doit conserver à l'abri du regard d'autrui. Ceci évoque à la fois une présence intrusive du téléphone mobile dans la vie privée et une problématique évidente de cette présence au cœur de la vie privée des personnes.

# I. UNE PRÉSENCE INTRUSIVE

Selon que le téléphone mobile est de première, deuxième ou troisième génération, il embarque des composantes et des fonctions plus intrusives à partir desquelles il est possible de reconstituer tout ou partie d'un individu ou d'avoir accès à des données qui lui sont personnelles et sont protégées par la loi comme telles. Tantôt ces données émanent des utilisateurs eux-mêmes en contrepartie de services ou de transactions offertes par ou à travers le terminal, tantôt elles sont dévoilées ou collectées à leur insu par l'opérateur, le fabricant ou toute personne intéressée.

## A. LES DONNÉES VOLONTAIREMENT TRANSMISES

Dire que certaines données sont volontairement transmises ne préjuge pas de la conscience que l'utilisateur du terminal mobile a des implications de cette transmission. Cela exprime juste que l'information est donnée par l'utilisateur. Il n'est même pas acquis que l'information personnelle soit donnée librement ou en toute connaissance des implications ou des utilisations qui peuvent en être faites.

Les données volontairement transmises sont les informations qui permettent de nous identifier soit directement, soit indirectement, telles que :

a. **Les noms, prénoms, photos, date de naissance, adresse postale ou la situation géographique**. L'activation d'un iPhone d'Apple demande l'ensemble de ces éléments et plus encore une connexion internet active. Or, les noms et prénoms en tant que moyen d'identification personnelle et de rattachement à une famille, concernent la vie privée et familiale de cette personne.

b. L'accès à certains terminaux se fait au moyen **d'empreintes digitales ou d'autres éléments d'identification biométrique**, l'Iphone 5s et le Samsung Galaxy S5 sont équipés de capteurs d'empreintes.

c. Certaines fonctions du système d'exploitation du terminal mobile synthétisent **une empreinte vocale** de l'utilisateur : il en est ainsi de Siri sur l'iPhone.

d. **La reconnaissance faciale** permet d'identifier le propriétaire et de déverrouiller l'écran d'accueil de certains terminaux sous Android (Huawei P7, Samsung S6, etc.). Or, l'image du visage est considérée comme un attribut de la personnalité protégé par le droit au respect de la vie privée.

e. L'enregistrement des contacts favorise **le réseautage social** c'est-à-dire la mise en évidence des liens entre les personnes.

On peut ajouter à cette liste l'adresse e-mail, le statut matrimonial, les identifiants sociaux (numéro de sécurité sociale, de carte de fidélité), le numéro de carte bancaire, etc.

Ce qu'il faut retenir est que toutes ces informations données au système informatique du terminal mobile sont enregistrées dans des petits fichiers systèmes et stockées dans la mémoire du téléphone et sur des bases registres sauvegardées parfois dans le nuage ou sur les serveurs du fabricant du téléphone ou de son système d'exploitation ou des applications qui y sont installées. L'utilisateur n'a pas la totale maîtrise de l'usage de ces fichiers au contraire du fabricant ou de l'éditeur du système d'exploitation qui peuvent traiter ces informations voire permettre à des tiers, développeurs d'application, d'avoir accès à ces informations.

La protection apportée par la loi à l'utilisateur en ce sens est le droit d'accéder aux informations collectées, de les modifier ou de les supprimer. L'accession et la modification permettent l'actualisation des données et génèrent un historique tout aussi utile d'un autre point de vue car cet historique retrace, dans le temps et la durée, des informations de la vie privée des utilisateurs ou de leurs contacts.

L'historique assure le suivi et une meilleure analyse ou traitement des données collectées. La suppression, quant à elle, a une réalité bien différente de ce que l'on en pense. En effet, la suppression du fichier, de la fonction ou même une réinitialisation matérielle ne signifie pas systématiquement la suppression des données fournies ou collectées.

Le système conserve la trace de l'activité et parfois les données ou les métadonnées qui y sont associées. A l'instar des ordinateurs, il faut parfois réécrire plusieurs fois sur le disque dur interne ou la mémoire interne du terminal mobile, à l'endroit particulier où une information a été supprimée pour espérer que cette information ne puisse être accessible à une investigation technique. Facebook intègre un logiciel de reconnaissance faciale qui permet l'identification des personnes sur les photos figurant dans la galerie de l'utilisateur. Après avoir supprimé une image, lorsque vous téléchargez une autre image de la même personne le nom réapparaît et il est identifié à nouveau.

Les technologies informatiques comportent ainsi des possibilités de reconstituer ou d'avoir accès à des données personnelles mémorisées localement sur le terminal mobile ou à distance sur des serveurs nationaux ou étrangers. Elles augmentent les possibilités d'identification et la traçabilité de chaque utilisateur ou d'utilisateurs qui lui sont associés. Ce qui constitue une immixtion (acceptée ou non) dans leur vie privée.

# B. LES DONNÉES ACQUISES À L'INSU DE L'UTILISATEUR

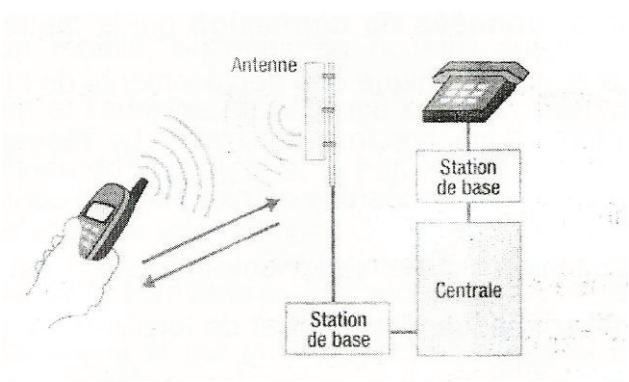
Aux données volontairement transmises, il faut opposer celles qui résultent de l'activité propre du téléphone, qu'il s'agisse des interfaces qui y sont installées ou des équipements qui la composent. Ce qui caractérise cette activité est qu'elle se déroule plutôt à l'insu de l'utilisateur, même s'il peut en avoir des notions. A cet égard, qu'il soit inactif ou actif, le téléphone mobile produit des activités dont l'incidence sur la vie privée est significative.

## 1. En mode Inactif

Inactif signifie en l'espèce que le terminal mobile n'est pas utilisé. Mais un Smartphone n'est jamais vraiment inactif.

**1.1** Il comporte, simplement alimenté par batterie ou allumé mais non utilisé, un certain nombre de composantes qui échangent avec les réseaux déployés des informations précises :

**a. L'Antenne** est intégrée au terminal mobile et permet de capter les ondes hertziennes émises par une ou plusieurs antenne(s)-relais fonctionnant sur des normes prédéfinies.
Cette antenne permet autant au téléphone de se connecter au relais le plus proche qu'audit relais de localiser les terminaux mobiles situés dans sa portée de rayonnement. Cet échange est facilité par la carte SIM.




**b. La carte SIM** est une puce utilisée en téléphonie mobile pour stocker des informations spécifiques à savoir : l'identifiant de l'abonné (numéro IMSI) et de l'opérateur mobile qui a édité la carte (MCC + MNC). La carte SIM permet l'utilisation des services du réseau de télécommunication mobile à partir du terminal mobile.

**c. La carte SIM** communique par ailleurs à l'opérateur de réseau mobile l'identifiant unique du terminal sur lequel il est installé : **l'IMEI**. C'est un numéro unique au format international identifiant chaque terminal mobile régulièrement manufacturé. Il n'y a pas, sauf manipulations spéciales, deux appareils avec le même numéro IMEI ou MEID.

Ce dispositif fournit une identité numérique spécifique à l'opérateur de réseau. Il relie en permanence un abonné identifié et un terminal spécifique à l'opérateur d'un réseau de télécommunication mobile tant que le terminal mobile est alimenté en énergie. L'opérateur dispose de ce fait, de données de connexion qui le mette en mesure de dresser une carte géographique des déplacements de l'utilisateur datée et avec des informations horaires précises. Le réseau de téléphonie mobile enregistre le cas échéant le dernier point de contact du terminal mobile.

L'opérateur de téléphonie mobile est donc en mesure d'identifier chaque utilisateur et de localiser sa position géographique à travers les échanges avec les antennes relais de son réseau. **L'historique de cette localisation permet de tracer l'utilisateur**. Ce sont d'ailleurs des données que la police affectionne en

cas d'enquête. De fait, les cahiers de charges et règlementations de sécurité publique font obligation aux opérateurs de systèmes de télécommunications mobiles d'assurer la conservation et la confidentialité des données de connexion.

Il a été jugé à cet égard que « L'obligation des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, […] de conserver les données énumérées [...] aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives à la protection tant de la vie privée que des communications [...] ainsi qu'au respect de la liberté d'expression […].

De ce point de vue, il convient de relever que les données que doivent conserver les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications,[...], sont notamment, les données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent notamment, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée.

Ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci.

Dans de telles circonstances, [...] il n'est pas exclu que la conservation des données en cause puisse avoir une incidence sur l'utilisation, par les abonnés ou les utilisateurs inscrits, des moyens de communication [...] et, en conséquence, sur l'exercice par ces derniers de leur liberté d'expression, [...].

La conservation des données aux fins de leur accès éventuel par les autorités nationales compétentes, […] concerne de manière directe et spécifique la vie privée et, ainsi, les droits garantis […]. En outre, une telle conservation des données […] constitue un traitement des données à caractère personnel au sens de cet article et doit, ainsi, nécessairement satisfaire aux exigences de protection des données découlant de la loi (arrêt Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 47). »

**Le traçage de l'utilisateur est amélioré avec la localisation géographique** pour les smartphones qui intègrent un GPS. **Les antennes équipées du système Global Positioning System (GPS) permettent en effet de recevoir, indépendamment des signaux de l'opérateur, des signaux de satellites qui fournissent la position dans l'espace du récepteur** dans un système à 3 axes pouvant être aisément converti en latitude, longitude, altitude. A noter que la plupart des portables de troisième génération est équipée d'un GPS.

**1.2** La géo localisation et l'identification du terminal mobile sont également facilitées par un certain nombre d'adresses :

a. **L'adresse IP** est un numéro attribué à chaque appareil connecté à Internet. L'adresse IP du terminal indiquée dans les paramètres du téléphone, permet l'identification de celui-ci sur le

réseau Internet. Mais outre l'identification du terminal, la connexion au réseau permet également d'obtenir des informations telles que le port utilisé, l'équipement utilisé, le nom du fournisseur d'accès à internet ou encore le pays, la localisation.

b. **Les adresses MAC** (Media Access Control) sont des identifiants physiques stockés dans une carte réseau ou une interface réseau similaire. À moins qu'elle n'ait été modifiée par l'utilisateur, l'adresse MAC de chaque terminal est unique au monde. Toutes les cartes réseau ont une adresse MAC notamment lorsqu'elles sont utilisées pour les technologies réseau, parmi lesquelles le Wi-Fi et le Bluetooth.

- **L'adresse Wi-Fi** identifie le composant Wi-Fi. C'est sous ce numéro que votre iPhone est identifié parmi tous les ordinateurs, téléphones et tablettes figurant dans la liste des équipements reconnus.
- **Le Bluetooth** permet à deux ou plusieurs appareils électroniques de communiquer par ondes radio, d'échanger des informations par ondes radio à basse fréquence. Le type d'informations échangées dépend de l'application.

A la différence des identifiants du réseau de télécommunication mobile, ces interfaces réseaux fonctionnent comme des balises radio. Les terminaux wi-fi actifs déclarent en permanence leur présence à la recherche des interfaces de connexion. Cette activité des interfaces wi-fi et Bluetooth offre matériellement la possibilité d'avoir accès à des informations telles que :

- La liste des réseaux auxquels le terminal mobile peut se connecter ou s'est connecté ;
- le nom du terminal mobile ;
- le type de terminal mobile (ordinateur, téléphone, fabricant, marque, modèle, type, etc.) ;
- le nom de la bibliothèque de média partagée.Elles peuvent ainsi être utilisées pour capturer et analyser les mouvements de leurs utilisateurs ou des porteurs des équipements. Ces informations mettent par ailleurs en cause la sécurité matérielle du terminal et la confidentialité des données qui sont échangées. Il faut observer en effet qu'à la différence des identifiants du réseau de télécommunication mobile, le trafic avec ces interfaces wi-fi et Bluetooth n'est ni chiffré ni protégé de sorte que toutes activités en ligne des utilisateurs, historique de navigation, recherches, informations de connexion, vidéos, e-mails et commentaires sur les réseaux sociaux, même en privé, sont facilement accessibles.

- Un document ultrasecret obtenu par CBC révèle que l'agence de surveillance électronique canadienne s'est servie du système wi-fi d'un aéroport pendant deux semaines pour obtenir des informations à partir des appareils mobiles des voyageurs. Les voyageurs ont traversé le terminal sans se rendre compte que les signaux de leur téléphone intelligent et de leur portable étaient interceptés. Le Centre de la Sécurité des Télécommunications du Canada (CST) a pu suivre les voyageurs à la trace pendant plusieurs jours dès qu'ils entraient dans les nombreux endroits du pays pourvus d'un réseau wi-fi et même dans des aéroports américains.
- Le smartphone offre un backdoor à la suite Google lorsqu'elle y est installée. Les vidéos consultées, les recherches effectuées, les sites consultés, l'historique de l'activité vocale et audio sur le terminal, les informations provenant de l'appareil et de tout appareil connecté (contacts, agenda, applications et autres données) sont collectées et stockées. Vos positions et points de connexion alimentent l'historique des positions qui permet de créer une carte privée des lieux où l'utilisateur s'est rendu avec les appareils sur lesquels il est connecté et le calcul des itinéraires et trajets, ceci impliquant la

détermination de la vitesse de déplacement.

- L'application mobile RATP en France accède à l'adresse MAC et au nom du terminal.

Les informations collectées par les systèmes de traçage Wi-Fi, les informations spécifiques de connexion émises par le téléphone mobile peuvent être utiles pour quiconque souhaite analyser les déplacements d'individus dans une zone d'intérêt, leurs comportements et les liens sociaux qui les unissent.

De fait, les centrales de marketing et analystes de marché, révèlent que ces systèmes sont déjà utilisés pour analyser les mouvements des clients dans les magasins et les centres commerciaux. Ils fournissent des informations telles que l'affluence en temps réel, la fréquence des visites, les rayons visités, le temps passé dans le magasin ou devant tels ou tels produits.

Ces données permettent d'améliorer l'offre commerciale, le profilage et le ciblage des individus et du chaland en vue de leur adresser des publicités ciblées :

- Sur des panneaux d'affichage dit «intelligents». Le principe est de reconnaître les passants grâce aux adresses MAC et d'afficher des publicités spécialement sélectionnées pour correspondre à leurs profils à une deuxième visite sur le site internet d'Air France pour consulter le prix du billet et si le tarif augmente ;
- lorsqu'ils effectuent une recherche sur Google, le site leur propose pendant plusieurs jours plusieurs liens qui sont relatifs à cette recherche. Cherchez des chaussures et il vous proposera plusieurs jours durant des modèles ou prestataires qui y sont relatifs.

En fait, le terminal est tout simplement fiché.

Ainsi les adresses MAC et IP et données de connexion internet favorisent la constitution et la diffusion d'historiques de connexion d'un terminal et la diffusion d'identifiants uniques permettant le traçage et le profilage comportemental ou commercial de l'utilisateur.

**1.3** Le mobile tend enfin à devenir un hub pour un ensemble d'objets connectés implants et puces électroniques grâce à des puces RFID ou NEC.

**a.** Les puces RFID sont incorporées par les multinationales dans certains de leurs produits pour en assurer la traçabilité. La puce permet ensuite de localiser le produit pendant sa distribution, mais aussi après son achat. Elle signalera au fabricant l'état, la durabilité, la résistance, les utilisations et conditions d'utilisation, les pannes et vices. Il suffira d'un simple passage ou friction avec un terminal mobile équipé. Le produit acheté devient ainsi « un mouchard électronique » et le terminal mobile sert de port ou de courroie de transmission.La puce aurait déjà été utilisée notamment par Gilette, pour «tracer» ses rasoirs jetables.

- La puce «Digital Angel» permet l'identification et la localisation par satellite des individus. Il s'agit d'une puce électronique de la taille d'un grain de riz et qui est implantée sous la peau. Elle est aussi capable de renvoyer des informations biologiques sur son porteur (température du corps, rythme cardiaque, cycle menstruel, fréquences sexuelles, etc.).
- Des hôpitaux américains ont encouragé des patients à se faire greffer une puce contenant leurs données médicales personnelles (groupe sanguin, traitements déjà en cours, etc.), dans le but d'éviter les risques d'erreur dans l'identification et le traitement des malades. Les implants devraient être aussi proposés pour une surveillance médicale à distance avec envoi automatique d'une alerte

au médecin en cas de problème.

L'application Santé de l'IPhone permet de créer à partir des données et renseignements collectés une fiche médicale qui peut être envoyée électroniquement.

- L'AppleWatch comme d'autres capteurs ou objets connectés communique au terminal mobile des informations sur le rythme cardiaque, l'activité physique, la fréquence respiratoire, la pression artérielle, la température corporelle, le poids, la capacité vitale, l'activité électrodermale, bref un ensemble de renseignements médicaux intimes et personnels pour lesquels le médecin est soumis au secret médical.

**b.** Dérivé de la technologie RFID, la NFC définit le procédé par lequel deux produits communiquent entre eux à très courte distance d'action (10 cm en théorie, ~4 cm en réalité) qui utilise des vitesses faibles (106-414 kbps) et une installation à faible friction (pas de découverte ou autre appariement) ce qui permet alors à deux appareils de communiquer automatiquement quand ils sont proches l'un de l'autre.

**1.4** Cet ensemble de matériels et d'équipements est coordonné et mis en œuvre par un système d'exploitation qui gère et contrôle l'ensemble des paramètres, fonctions et données du terminal mobile. Ce système est en principe incontournable par l'utilisateur qui en accepte l'utilisation et les contraintes.

Qu'il s'agisse d'iOS (Apple), d'Android (Google), de Windows mobile (Microsoft), de Rim (BlackBerry), l'utilisateur mesure difficilement les accès et transmissions de ses données par l'éditeur du programme d'exploitation ou les développeurs d'application qu'il autorise. Il en est ainsi des données de diagnostic et d'utilisation et des services installés par défaut qui traitent et collectent des données de configuration permettant l'évaluation des habitudes de l'utilisateur (période d'inactivités et de sommeil, mode de vie, dictionnaire personnel, vocabulaire, niveau d'instruction, handicaps particuliers (manuels, visuels, auditifs, etc.), habiletés spécifiques, tâches ordinaires), un ensemble d'informations personnelles et intimes dont même l'utilisateur n'a pas totalement conscience. Aucun accès ne peut lui être dénié, aucun code ne peut lui être opposé et aucune surveillance ne permet d'assurer la confidentialité des données notamment en cas de connexion à internet.

- II est démontré que **Windows** et son navigateur **Internet Explorer**, renferment un numéro d'identification de l'utilisateur, le GUID (Globally Unique Identifier). Ce numéro d'identification est ensuite inscrit dans tous les documents créés avec les applications de Microsoft Office. Il peut être consulté à distance par Internet grâce à des commandes spéciales prévues par Microsoft.

De la même façon, Windows Media Player génère un **identifiant unique** propre à votre ordinateur et susceptible d'être récupéré par Internet.

La fonctionnalité «Rapport d'erreur» d'Internet Explorer et d'Office **envoie à Microsoft des informations lors de vos plantages**, votre configuration, mais également sur les autres applications de Windows. De son coté, **Intel** a également placé un numéro d'identification consultable à distance dans les puces Pentium III et Xeon.

- Android permet de sauvegarder automatiquement certains paramètres et données associées à un compte Google comme les **mots de passe Wi-Fi**, les **favoris** de navigation, les **applications** installées depuis Google Play, les termes ajoutés au **dictionnaire** personnel ainsi que la plupart des **paramètres** du terminal et des applications utilisant le service de sauvegarde.

- Les données sur notre identité sont «interrogeables à distance», ainsi que le contenu du fameux

fichier «magic cookie». Ce fichier garde la trace de certains sites visités qui y inscrivent des informations afin d'identifier les utilisateurs et mémoriser leur profil.

Il est admis désormais qu'avec les logiciels adéquats, parfois en accès libre sur internet, n'importe qui peut pister les informations personnelles d'un internaute ou connaître ses identifiants numériques.

## 2. En mode Actif

En mode actif, le terminal mobile, les logiciels et applications installés sur le téléphone mobile ou certaines fonctions du téléphone mobile, fournissent un certain nombre d'informations et peuvent être piratés à des fins frauduleuses.

L'appareil photo intègre un GPS et inscrit les coordonnées de l'appareil parmi les données (EXIF) incrustées dans les données numériques des clichés et fichiers.

Google récupère et établit l'historique de l'activité vocale et audio du terminal en stockant les entrées vocales et audio sur le compte de l'utilisateur, ce qui permet de reconnaître la voix et d'améliorer la reconnaissance vocale (« Ok Google » pour effectuer une recherche vocale).

Echelon utilise les technologies de reconnaissance vocale pour repérer automatiquement des mots clés dans les conversations écoutées. Les mots clés à repérer sont choisis par les officiers d'Echelon en fonction de l'actualité et des objectifs du moment.

Il faut enfin savoir que le micro du portable peut être activé à distance par les services de police grâce à un simple code de 4 chiffres, même quand le portable est éteint. N'importe qui peut être ainsi espionné à tout moment à son insu.

Cet ensemble de matériels et d'équipements est coordonné et mis en œuvre par un système d'exploitation qui gère et contrôle l'ensemble des paramètres, fonctions et données du terminal mobile. Ce système est en principe incontournable par l'utilisateur qui en accepte l'utilisation et les contraintes.

Ainsi, lorsque les fonctions du terminal mobile sont mises à contribution, elles peuvent établir une identification numérique de l'utilisateur et sa géolocalisation très précise.

Par ailleurs il n'est plus contesté que l'utilisateur d'internet est identifiable grâce aux données personnelles stockées par le navigateur et le système. Les données stockées sont mêmes interrogeables à distance qu'il s'agisse de fichiers temporaires (TEMP, THUMBS, CACHE) des cookies ou d'autres fichiers mouchards. Ces fichiers gardent en effet la trace de certaines activités ou des informations inscrites par certains sites consultés afin d'identifier les utilisateurs et mémoriser leur profil ou leurs activités.

Ainsi par ses composantes matérielles, sa configuration logicielle ou les exigences d'activation qu'il pose à l'utilisateur, par la proximité avec l'individu, en devenant le mode privilégié de communication, le terminal mobile concentre certains aspects de l'intimité des personnes. Il est par suite en mesure d'exposer l'utilisateur à des atteintes à sa vie privée en permettant par des manœuvres techniques habiles ou des positions juridiques confortables de collecter, de regrouper, de décloisonner et de disposer de données personnelles plus ou moins complètes que les utilisateurs sont censés seuls conserver.

# II. UNE INTRUSION PROBLÉMATIQUE

La problématique autour du caractère intrusif du terminal mobile dans la vie privée de l'utilisateur pose à la fois la question de la protection juridique de la vie privée et celle de la propriété des données personnelles.

## A. L'ETAT DE LA PROTECTION JURIDIQUE DE LA VIE PRIVEE

La loi en la matière organise trois protections : la protection de la vie privée, la protection des données personnelles et la protection du consommateur.

### 1. La protection de la vie privée

En droit interne, ni le code civil, ni le code des personnes et de la famille en vigueur au Bénin ne s'intéressent expressément à la notion de vie privée. Il faut se référer à l'article 2 de la loi 2009 - 09 portant protection des données à caractère personnel en République du Bénin pour voir poser très spécifiquement le principe suivant lequel « L'informatique étant une science au service de l'homme, elle ne doit pas porter atteinte à l'identité humaine, à la vie privée de l'individu, aux droits de l'homme, aux libertés publiques individuelles ou collectives ».

Le code des personnes et de la famille dispose à l'alinéa 3 de l'article 13 : « **l'usage abusif d'un nom patronymique et de tous autres éléments d'identification de la personne engage s'il y a préjudice, la responsabilité de l'auteur de l'abus** ». Ces dispositions renvoient donc au principe général posé par l'article 1382 du code civil, savoir que « tout fait quelconque de l'homme qui cause un dommage à autrui oblige celui par la faute duquel il est arrivé à le réparer ». Ainsi, en droit interne l'atteinte n'ouvrira droit à la réparation que si le préjudice est certain et établi. La preuve en repose sur la victime.

Ce régime juridique est nettement moins protecteur que celui qui résulte en France de l'article 9 du code civil aux termes duquel « Chacun a droit au respect de sa vie privée ». Il est en effet jugé sur cette base que « la seule constatation de l'atteinte à la vie privée ouvre droit à réparation », celle-ci pouvant être en nature ou par équivalent. Toute utilisation illicite d'un élément de la vie privée suffit dès lors à ouvrir droit à réparation de sorte que la victime est dispensée de la preuve d'une faute et d'un préjudice particuliers dans ce régime légal de protection.

Mais à la vérité, les parties sont dans une obligation contractuelle de sorte que pour fonder son action, l'utilisateur ne peut se placer que sur le terrain de la responsabilité contractuelle conformément au principe de l'indisponibilité de l'action en responsabilité ou au non cumul de responsabilité. Cela veut dire que **la responsabilité ne peut être engagée qu'en cas d'inexécution ou de mauvaise exécution de l'engagement contractuel**. Dans ce sens, la mise en œuvre de la responsabilité parait plus difficile et la protection plus illusoire puisque l'accès aux données privées est préalablement contractuellement autorisé.

La loi n° 2007 - 21 du 16 Octobre 2007 portant protection du consommateur en République du Bénin et applicable à toutes les transactions et activités en matière de consommation relative à la fourniture, à la distribution, à la vente ou à l'échange de biens et services notamment en matière de communication et de télécommunication, prévoit à cet effet :

**Article 24 :** Pour être commercialisé sur le marché national, tout produit non agricole fabriqué localement ou importé doit faire l'objet d'un enregistrement par les services compétents des ministères sectoriels qui délivrent un certificat preuve de l'enregistrement

**Article 25 :** L'enregistrement doit être fait avant toute mise en consommation du produit et après évaluation des critères de qualité, de sécurité et d'efficacité selon les normes et règlementations nationales ou internationales.

La référence à la sécurité est ici utile pour fonder la protection des utilisateurs, la notion supportant une conception active et une conception passive. La sécurité passive ou plus justement sécurité palliative ou sécurité secondaire est l'ensemble des éléments qui par leur présence ou leur fonctionnement peuvent minimiser la gravité de l'atteinte. La **sécurité active** ou plus justement **sécurité préventive** ou **sécurité primaire** est l'ensemble des éléments qui, par leur présence ou leur fonctionnement, peuvent éviter que l'atteinte ne se produise. Elle est donc en action avant l'atteinte.

## 2. La protection des données personnelles

Constituent des données à caractère personnel, toute information relative à une personne physique identifiée ou susceptible de l'être directement ou indirectement par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. **Les données personnelles** (ou nominatives) correspondent aux noms, prénoms, adresses (physique et électronique), numéro de téléphone, lieu et date de naissance, numéro de carte de paiement, plaque d'immatriculation d'un véhicule, photo, empreinte digitale, ADN. Les données personnelles incluent les données médicales et génétiques et, en général, toute caractéristique biométrique. Mais constituent également des données à caractère personnel tous les échanges, informations de connexion, de localisation et de trafic, transmission, émission ou réception de signes, de signaux, d'images, de sons, de texte, de voix, ou d'écrits de toute nature, par fil optique ou autres systèmes électromagnétiques dont l'émetteur et le destinataire peuvent attendre, en raison de leur caractère privé, qu'aucune tierce personne ne prenne connaissance sans leur consentement préalable.

Il est jugé dans ce cadre que « la technique dite de « géolocalisation « constitue une ingérence dans la vie privée dont la gravité nécessite qu'elle soit exécutée sous le contrôle d'un juge ». Or, cette technique n'est pas directement un usage de données personnelles. Elle est juste rendue possible par des données d'usages qui sont relatives à un utilisateur déterminé par des identifiants numériques précis. **Les données d'usage** ne sont pas expressément énoncées par la loi. Elles sont la traduction de comportements en ligne ou hors ligne (habitude de navigation, comportements, aptitudes ou incapacités), un ou plusieurs éléments propres, constitutifs d'informations capturées par les systèmes informatiques et susceptibles d'identifier la personne.

La loi n° 2009-09 du 22 Mai 2009 portant protection des données à caractère personnel en République du Bénin fonde d'autant plus le droit au maintien du caractère privé de ces données ou informations que toute opération ou ensemble d'opérations portant sur ces données quel que soit le procédé utilisé et

notamment la collecte, l'enregistrement, l'organisation, la consécration, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission ou diffusion de tout autre forme de mise à disposition, le rapprochement ou l'interconnexion ainsi que le verrouillage, l'effacement ou la destruction est constitutif d'un traitement soumis à une double prévention. La prévention de l'accès non autorisé et la prévention de l'utilisation à des fins non autorisées ou illégales.

- La prévention de l'accès non autorisée

Aux termes de l'article 5 de la loi n° 2009-09 du 22 Mai 2009 portant protection des données à caractère personnel en République du Bénin, « Un traitement de données à caractère personnel ne peut porter que sur des données remplissant les conditions ci-après :

**a.** être collectées et traitées de manière loyale et licite ;

**b.** être collectées pour des finalités bien déterminées, explicites, légitimes et non frauduleuses ;

**c.** ne pas être traitées ultérieurement de manière incompatible avec les finalités ainsi déterminées ;

**d.** être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

**e.** être exactes, complètes et, si nécessaire, mises à jour. Des mesures appropriées doivent être prises pour que les données inexactes ou incomplètes au regard des finalités pour lesquelles elles sont collectées ou traitées soient effacées ou rectifiées ;

**f.** être conservées sous une forme permettant l'identification des personnes concernées pendant un délai n'excédant pas la durée nécessaire à l'atteinte des finalités pour lesquelles elles sont collectées ou traitées.

La collecte ou le traitement des données opéré(e) par tout moyen frauduleux, déloyal, illicite est interdit(e) ».

La loi exige même l'autorisation et le contrôle préalable de la Commission Nationale de l'Informatique et des Libertés (CNIL) pour le traitement de certaines données en raison des risques particuliers pour les droits et libertés ou lorsque leur contenu et leurs finalités sont susceptibles de porter atteinte à la vie privée de la personne concernée par le traitement. Il en est ainsi notamment pour : «

**a.** les traitements comportant un numéro national d'identification ainsi que tous traitements de portée nationale recensant tout ou partie de la population ;

**b.** les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes ;

**c.** les traitements comportant des données relatives à la santé des personnes ou à leur situation ;

**d.** les traitements comportant des données relatives aux infractions et condamnations ;

**e.** les traitements intéressant la sûreté de l'Etat, la défense ou la sécurité publique et ceux qui ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales; ...» (article 43 loi n° 2009-09 du 22 Mai 2009 portant protection des données à caractère personnel en République du Bénin).

Par suite, il est fait obligation à tout responsable de traitement de données personnelles d' « informer de

manière claire et complète toute personne utilisatrice du réseau de communication électronique :

- de la finalité de toute action tendant à accéder, par voie de transmission électronique, à des informations stockées dans son équipement terminal de connexion, ou à inscrire, par la même voie, des informations dans son équipement terminal de connexion ;
- des moyens dont elle dispose pour s'y opposer ». (article 48 loi n° 2009-09 du 22 Mai 2009 portant protection des données à caractère personnel en République du Bénin).

Il est « tenu de prendre toutes précautions utiles au regard de la nature des données et des risques présentés par le traitement pour préserver la sécurité des données et, notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès ». (article 50 loi n° 2009-09 du 22 Mai 2009 portant protection des données à caractère personnel en République du Bénin).

La jurisprudence constante en la matière requiert l'autorisation ou le consentement personnel. Toute personne, quel que soit son rang, sa naissance, sa fortune, ses fonctions présentes ou à venir, a droit au respect de sa vie privée. Il est ainsi jugé que « des informations couvertes par le secret médical ne peuvent être communiquées à un tiers sans que soit constaté l'accord de la victime ou son absence d'opposition à la levée du secret » ou encore que « la fixation de l'image d'une personne, vivante ou morte, sans autorisation préalable des personnes ayant pouvoir de l'accorder est prohibée ».

Plus généralement, « Est illicite toute immixtion arbitraire dans la vie privée d'autrui. Caractérise une immixtion illicite dans la vie privée d'une personne le fait de la faire épier, surveiller et suivre », ce qui est le propre des historiques et collectes de données personnelles. Il a été jugé par suite que « Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée » ou encore que « Constitue un mode de preuve illicite tout enregistrement, quels qu'en soient les motifs, d'images ou de paroles à l'insu des salariés, pendant le temps de travail ».

Il apparait que ce qui gêne fondamentalement est la non autorisation de sorte qu'on pourrait penser que l'autorisation personnelle écarterait le reproche de l'atteinte à la vie privée ou du traitement illégal des données personnelles.

L'exigence d'une autorisation est de fait levée dans des cas strictement limités où le consentement peut se présumer. L'article 48 de la loi n° 2009-09 du 22 Mai 2009 portant protection des données à caractère personnel en République du Bénin dispose que les exigences posées « ne sont pas applicables si l'accès aux informations stockées dans l'équipement terminal de l'utilisateur ou l'inscription d'informations dans l'équipement terminal de l'utilisateur :

- soit, a pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;
- soit, est strictement nécessaire à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

De même :

- lorsque les données à caractère personnel n'ont pas été recueillies auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à cette dernière les informations énumérées à l'article 14 de la présente loi dès l'enregistrement des données ou, si une communication des données à des tiers est envisagée au plus tard lors de la première communication des données.
- Lorsque des données à caractère personnel ont été initialement recueillies pour un autre objet, les dispositions de l'alinéa précédent ne s'appliquent pas aux traitements nécessaires à la conservation

de ces données à des fins historiques, statistiques ou scientifiques.

- Ces dispositions ne s'appliquent pas non plus lorsque la personne concernée est déjà informée ou quand son information se révèle impossible ou exige des efforts disproportionnés par rapport à l'intérêt de la démarche ».

Ainsi, la théorie de l'atteinte à la vie privée se trouve nuancée suivant la nature de l'information à laquelle on accède, le mode de vie ou la nature de la personne en cause, l'existence de divulgations volontaires antérieures… « Il n'y a pas atteinte à la vie privée lorsque les prétendues révélations ne sont que la relation de faits publics ou ne présentent qu'un caractère anodin ». Il a été jugé encore que « Les questions patrimoniales concernant une personne menant une vie publique, tel un dirigeant d'une grande entreprise, ne relèvent pas du domaine de la vie privée ». Mais « le salaire de celui qui n'est pas une personne publique et ne jouit d'aucune notoriété particulière relève de sa vie privée ».

Il apparait donc le principe suivant lequel, les données personnelles des utilisateurs ne peuvent être traitées que lorsqu'ils ont donné leur accord ou lorsque ce traitement est prévu par la loi. Les utilisateurs doivent être informés de quelles données seront traitées ou transmises à d'autres parties, quand, par qui, pour quelles raisons, afin de les contrôler.

Mais alors deux questions se posent :

**i.** La première question qui se pose à l'égard du terminal mobile est de savoir si l'autorisation de l'utilisateur est donnée en connaissance de cause et de plein gré. Cette question pose deux préoccupations :

➢ Celle de l'information suffisante de l'utilisateur

L'obligation d'information prend source dans l'exécution de bonne foi du contrat posée en principe à l'article 1134 alinéa 3 du code civil, cette obligation étant renforcée par ailleurs par l'article 1135 du même code qui dispose que « **les conventions obligent non seulement à ce qui y est exprimé mais encore à toutes les suites que l'équité, l'usage ou la loi donnent à l'obligation d'après sa nature** ». Plus spécifiquement l'article 1602 du Code civil prescrit que «**le vendeur est tenu d'expliquer clairement ce à quoi il s'oblige**». Ce dispositif légal général se complète par les dispositions de l'article 1162 qui prévoit l'interprétation à l'encontre de celui qui stipule.

Mais cette information de bonne foi qui s'incorpore au contrat comme une suite naturelle, ne satisfait pas la préoccupation présente. Ce qui est nécessaire en l'espèce est **l'information suffisante pour mettre l'utilisateur en mesure d'exprimer un choix éclairé, c'est-à-dire l'éclairage juridique et la connaissance technique, suffisantes pour appréhender les implications de l'utilisation du téléphone portable**. L'utilisateur, considéré comme une personne légitimement ignorante d'une information ou d'une intention commerciale ou présumée l'être et ayant de celle-ci un besoin légitime, doit pouvoir obtenir notamment du vendeur du terminal mobile ou de l'éditeur du système d'exploitation ou de l'opérateur de réseau de télécommunication, qui connaît l'information ou, dans certains cas, est censé la connaître, qu'il la lui révèle.

En effet la situation est la suivante : la plupart des utilisateurs de terminaux mobiles au Bénin méconnaissent jusqu'au(x) risque(s) d'atteinte à leur vie privée par les données personnelles et/ou d'images diffusées par les smartphones. Une enquête sérieuse constatera certainement que la plus grande majorité de ces utilisateurs de téléphone mobile conserve les codes PIN standards attribués par les opérateurs de

téléphonie ou utilisent leurs adresses mails et le même mot de passe pour plusieurs appareils et comptes. A l'interrogation, on notera que l'acceptation donnée par l'utilisateur à l'activation du téléphone mobile n'est pas un blanc-seing ni un consentement éclairé ou libre à toutes les conséquences de l'utilisation. Mais il aura bien de difficulté à faire admettre en justice cette ignorance pour parvenir à la protection de ses données et de sa vie privée. La nécessité d'une politique publique d'information par la CNIL est là évidente.

Et plus encore la mise en place de concert avec l'Autorité de Régulation des Communications Electroniques et de la Poste (ARCEP) d'un contrôle de la mise en consommation des terminaux mobile et d'une politique de sécurité plus protectrice des consommateurs. Cette sécurité (dans le domaine des communications électroniques), englobe non seulement la sécurité technique (confidentialité) par les moyens de cryptologie ou autres restrictions d'accès ou interdiction logicielles mais aussi la sécurité juridique (protection).

Par ailleurs, certaines informations relatives notamment au fonctionnement du téléphone mobile ou des applications doivent être fournies aux utilisateurs, afin de rendre plus facile l'exercice du choix et le contrôle de la diffusion de leurs données personnelles. Outre l'agrément à la commercialisation constitutif d'une protection générale, les utilisateurs doivent obligatoirement être informés sur les choix de configuration étant entendu que celles-ci doivent également offrir suffisamment de flexibilité pour s'adapter à l'utilisation, il est suggéré notamment que des réglages de paramètres plus simples soit diffusées ou intégrés aux systèmes d'exploitation afin de faciliter le contrôle par les utilisateurs de leurs données partagées. **Il y a sur ces points un illettrisme technique et/ou juridique tel que le consentement non éclairé ne peut qu'en être vicié.**

**Cet illettrisme technique ou juridique évoque à lui seul un déséquilibre suffisant au détriment du consommateur pour qualifier l'avantage excessif constitutif de « l'abus sanctionnable** ». À noter qu'aux termes de la loi n° 2007 - 21 du 16 Octobre 2007 portant protection du consommateur en République du Bénin **« Les clauses abusives sont interdites dans tous les contrats relevant du domaine d'application de la présente loi** » de sorte que la disposition juridique s'il en existe, sera réputée nulle et non écrite comme contraire à l'ordre public et l'abus plus généralement ouvrira droit à des dommages-intérêts comme manquement à une obligation de ne pas faire.

Mais la violation de l'obligation d'information peut caractériser parallèlement une réticence dolosive, lorsque cette violation est intentionnelle. La jurisprudence retient que « le manquement à une obligation précontractuelle d'information, à le supposer établi, ne peut suffire à caractériser le dol par réticence, si ne s'y ajoute la constatation du caractère intentionnel de ce manquement et d'une erreur déterminante provoquée par celui-ci » .Cette intention suppose donc en réalité une tromperie sur la nature, l'espèce, l'origine, les qualités substantielles, la composition ou la teneur en principes utiles du produit telle que sans cette tromperie la victime n'aurait pas contracté, ou l'aurait fait mais à des conditions différentes. La nullité ou l'allocation de dommages-intérêts est subordonnée au caractère déterminant de la tromperie.

Or le fait de dissimuler certains risques ou contraintes ou le fait que l'une des parties ait manqué à son obligation d'information, voilé ses intentions commerciales, ou le fait même encore que le vendeur ait fourni, compte tenu des limites propres au moyen d'information utilisé et des circonstances qui l'entoure, de façon inintelligible, ambiguë ou à contretemps, une information substantielle doit être considérée formellement comme une pratique commerciale suffisamment trompeuse et sanctionnée comme telle.

Sur ce plan les dispositions de la loi n° 2007 - 21 du 16 Octobre 2007 portant protection du consommateur en République du Bénin sont une source tout à fait indiquée pour asseoir une meilleure protection juridique. Outre le contrôle de la mise en consommation par l'apposition préalable sur le

produit d'un poinçon ou d'un autre signe similaire ou la délivrance au prestataire de service par une structure de contrôle agréée d'un certificat, elle prévoit en effet très spécifiquement :

**Article 12 :** Le vendeur ou le prestataire de service avant la vente ou la prestation de service, doit informer le consommateur notamment en :

- ...
- Le mettant en garde contre tous les dangers que le produit est en mesure de provoquer même ceux liés à ses propriétés normales…

**Article 13 :** ... il est en outre tenu de remettre au consommateur un document indiquant les caractéristiques techniques du bien appuyé par un reçu comportant le prix et la durée de la garantie.

Ce dispositif permet en tous les cas la sanction des manquements à l'obligation d'information du vendeur, à l'instar de la jurisprudence qui invite à sanctionner les silences conservés sur une information importante pour l'acheteur. Il constitue un dispositif protecteur du consommateur car il n'est plus acquis qu'une meilleure sensibilisation des éditeurs puisse limiter la propension insidieuse à la collecte toujours plus intrusive de données personnelles.

- celle de son consentement libre.

Le dévoilement des caractéristiques personnelles est l'ingrédient nécessaire à la réalisation des services d'appariement fournis par les RSN (Activation de Badoo, WhatsApp, Facebook). La mise en marche d'un iPhone est subordonnée à l'acceptation sans réserve de l'utilisateur et au respect des conditions d'utilisation fixées par l'éditeur. Cette acceptation implique l'adhésion pleine et entière aux conditions générales ainsi qu'à la politique de confidentialité dont les changements par ailleurs sont laissés à la discrétion de l'éditeur. Il faut ajouter que lorsque la possibilité est offerte de s'opposer aux traitements des données, c'est au risque de ne pas bénéficier de tout ou partie des services gratuits fournis par l'application ou le terminal. « C'est à prendre ou à laisser ».

L'utilisateur accepte généralement dans ces conditions l'utilisation ou l'adhésion sans évaluer totalement les implications de son consentement mais en ne pouvant rester naïf d'un marché ou d'un contrat silencieux qui ressort du contexte : contre la gratuité de l'accès, l'éditeur de l'application ou du système d'exploitation du terminal mobile s'arroge le droit de collecter et de commercialiser les données personnelles de l'utilisateur. Il en est d'autant plus ainsi que par formules vagues et volontairement imprécises, le fabriquant ou l'éditeur n'évoque la collecte de données inhérentes à cette activation ou à l'utilisation consécutive qu'en l'entourant de garanties d'anonymat et avec la promesse ou l'engagement de créer des produits et services gratuits ou payants à destination des utilisateurs et des clients c'est-à- dire selon la formule « pour améliorer leur expérience personnelle d'utilisateur ».

Le droit de modifier les paramètres de l'application, la configuration de l'appareil et de suspendre la collecte de données appelle de même une vigilance rendue volontairement gênante pour l'utilisateur quand la chose n'est pas qu'illusion. **Deux vices dès lors dans cette relation : la sincérité incertaine des engagements et la contrainte psychologique à l'acceptation.**

Derrière ce mode à prendre ou à laisser et l'imposition à l'utilisateur de la volonté de l'éditeur ou du fabriquant il est évident que l'autorisation personnelle est souvent contrainte et que ces pratiques commerciales sont condamnables. Il convient en effet de souligner que le fait de forcer ou d'exiger

l'autorisation d'accès à des données personnelles de l'utilisateur avant de lui permettre l'utilisation ou la jouissance du logiciel acquis peut être considéré comme un abus de droit de la nature des clauses abusives interdites en droit béninois. Aux termes de l'article 10 de la loi n° 2009 - 09 du 22 mai 2009 portant protection des données à caractère personnel, « **Une clause est abusive lorsqu'elle apparaît comme imposée au consommateur par la puissance économique de l'autre partie et donne à cette dernière un avantage excessif...** »

Et ces deux conditions cumulatives sont remplies en l'espèce.

Certes la loi sur la protection des données personnelles accorde des droits d'accès, de rectification et d'opposition que chacun peut exercer en interpelant au besoin la Commission Nationale de l'informatique et des Libertés (CNIL). Mais il ne semble pas que cette possibilité de faire valoir, à posteriori, leurs droits suffise à rendre la collecte réalisée dans ces circonstances, acceptable.

**ii. L'autre question qui se pose est de savoir si l'utilisateur à une telle disponibilité de ses droits pour être capable de déroger par des conventions particulières à des lois qui intéressent l'ordre public ou les bonnes mœurs.**

On peut s'interroger quant à savoir si les droits du consommateur sont d'intérêt privé ou d'ordre public ? Si le consommateur peut renoncer à la protection édictée dans son intérêt ?

La collecte non autorisée étant seule sanctionnée et l'autorisation personnelle écartant le reproche de l'atteinte à la vie privée ou du traitement illégal des données personnelles, on peut penser que les personnes conservent la libre disposition d'eux-mêmes c'est-à-dire qu'elles restent libres de leurs choix, de leur vie privée, de l'usage qu'elles entendent faire de leur image, capacités, personne et données personnelles. Mais par cela même que les données personnelles peuvent être considérées comme un prolongement de la personne humaine, cette doctrine libérale souffre des restrictions tenant à la nécessaire protection de la dignité humaine et des bonnes mœurs, composantes de l'ordre public. Il faut nécessairement considérer en effet que la protection n'a de sens et d'efficacité que lorsque chacun est tenu envers les autres par le respect des interdictions qui assurent cette protection et les objectifs qui la rendent nécessaire ou utile.

La réponse à la question semble donc devoir être nuancée suivant les données personnelles ou à caractère personnel en cause. Mais à la vérité la disposition des droits envisagés ici ne doit pas être confondue avec la libre disposition de soi, même si les droits tendent à protéger les individus.

Le principe en matière de droit à la protection est posé par les articles 3 et 6 du code civil : « Les lois de police et de sûreté obligent tous ceux qui habitent le territoire » et « Nul ne peut déroger par des conventions particulières aux lois qui intéressent l'ordre public ou les bonnes mœurs ». En ce sens la loi n° 2007 - 21 du 16 Octobre 2007 portant protection du consommateur en République du Bénin est un dispositif de protection des droits des consommateurs. Il ne semble dès lors pas appartenir au consommateur de transiger sur les aspects réglementés par cette loi. Il est jugé ainsi qu'une disposition conventionnelle prohibée par la loi est atteinte de nullité absolue et n'est susceptible ni de confirmation ni de ratification étant entendu que la renonciation anticipée au bénéfice d'une loi impérative n'est pas valable.

La loi n° 2007 - 21 du 16 Octobre 2007 incrimine au surplus toutes infractions à ses dispositions et rend l'infraction punissable d'une amende allant de cinq cent mille (500.000) au moins à cent millions (100.000.000) de francs CFA au plus sans préjudice des peines privatives de liberté de trois (3) mois à cinq (5) ans (article 54). La peine applicable est portée au double en cas de récidive (article 55) : Cette loi ne

laisse pas la poursuite des infractions à la discrétion de la victime mais en assure l'application impérative.

Contrairement à la loi n° 2007 - 21 du 16 Octobre 2007, la loi n° 2009 - 09 du 22 mai 2009 portant protection des données à caractère personnel incrimine les accès et utilisations illégales ou illicites aux données à caractère personnel. Mais il faudra dans ce cadre réserver l'effet absolutoire notamment de l'autorisation.

Il est jugé cependant que « pour retenir la qualification de loi de police, il faudrait considérer l'application de la loi [française] comme s'imposant sans contestation possible pour la sauvegarde de l'organisation socioéconomique de notre communauté nationale ; que la seule circonstance tenant au fait que le défaut de respect de certaines de ses dispositions soit sanctionné pénalement ne permet pas d'évidence de retenir le caractère impératif de son application à la situation considérée, au regard au surplus des conditions restrictives de son champ d'application évoquées plus haut ».

Dans le même ordre d'idées, l'exception d'ordre public, au sens où l'entend le droit international privé, qui imposerait la protection n'est pas systématiquement admise dans la mesure où il n'est pas évident que les valeurs fondamentales de l'ordre juridique national se trouvent compromises par l'application du droit étranger, à le supposer même moins favorable.

- **La prévention du traitement non autorisé ou l'utilisation à des fins non autorisées ou illégales**

De plus en plus de tiers sont autorisés à collecter des données par le biais des sites ou des applications. Il est rare que ces « tiers autorisés » soient expressément nommés dans les politiques de confidentialité, ils sont donc difficilement identifiables par l'utilisateur. Ceci facilite ou entraine une circulation des données et la perte de leur maîtrise. C'est le premier risque encouru par l'utilisateur du terminal électronique mobile.

L'autre risque est celui du détournement d'usage qui consiste à modifier les finalités du traitement initialement prévu par la collecte des données. Ce détournement d'usage des données peut avoir lieu après une modification de la politique de confidentialité de l'entreprise mais également à l'insu de l'utilisateur notamment lorsqu'il n'en a pas la maîtrise ou qu'il l'a perdue.

Aux termes de l'article 5 de la loi n° 2009-09 du 22 Mai 2009 portant protection des données à caractère personnel en République du Bénin, « Un traitement de données à caractère personnel ne peut porter que sur des données remplissant les conditions ci-après :

**a.** être collectées et traitées de manière loyale et licite ;

**b.** être collectées pour des finalités bien déterminées, explicites, légitimes et non frauduleuses ;

**c.** ne pas être traitées ultérieurement de manière incompatible avec les finalités ainsi déterminées ; …

La collecte ou le traitement des données opéré(e) par tout moyen frauduleux, déloyal, illicite est interdit(e). » c'est en ce sens que « constitue une atteinte à la vie privée la publication de photographies ne respectant pas la finalité visée dans l'autorisation donnée par l'intéressé. »

A noter que la loi n° 2009 - 09 du 22 mai 2009 portant protection des données à caractère personnel incrimine comme manquement graves :

**a.** le fait de procéder à une collecte déloyale des données personnelles ;

**b.** le fait de communiquer à un tiers non autorisé des données personnelles ;

**c.** le fait de procéder à la collecte des données sensibles, des données relatives à des infractions ou à un numéro national d'identification sans respecter les conditions légales ;le fait hors les cas où le traitement des données a été réalisé dans les conditions prévues par les dispositions de la présente loi, de procéder ou de faire procéder à un traitement des données personnelles incluant parmi les données sur lesquelles il porte, des données sensibles relatives à des infractions ou des données relatives au numéro d'identification national ;

**d.** le fait de procéder ou de faire procéder à un traitement de données personnelles sans avoir mis en œuvre les mesures prescrites par les dispositions de la présente loi ;

**e.** le fait de collecter des données personnelles par un moyen frauduleux, déloyal ou illicite ;

**f.** le fait, par toute personne détentrice des données personnelles à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner et/ou de manipuler ces informations ;

**g.** le fait de procéder à un traitement des données personnelles concernant une personne physique malgré la demande de rectification ou l'opposition de cette personne, lorsque cette demande de rectification ou cette opposition est fondée sur des motifs légitimes ;

**h.** le fait de ne pas respecter les dispositions de la présente loi relatives à l'information des personnes ;

**i.** le fait de ne pas respecter les dispositions de la présente loi relatives aux droits d'accès ;

**j.** le fait de conserver des données personnelles au-delà de la durée prévue pour la déclaration préalable adressée à la Commission sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la présente loi ;

**k.** le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet, de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ;

**l.** le fait de participer à une association formée ou à une entente établie en vue de la commission d'une ou plusieurs infractions prévues par la présente loi.

Elle punit d'une peine d'emprisonnement de cinq (05) à dix (10) ans et d'une amende de dix millions (10.000.000) à cinquante millions (50.000.000) de francs ou de l'une de ces deux peines seulement.

Les droits d'accès, de rectification et d'opposition que chacun peut exercer à l'égard de la personne en charge du traitement des données à caractère personnel, n'apportent cependant dans le principe à l'utilisateur que la possibilité d'une réparation en nature et donc d'une satisfaction morale.

## B. LA QUESTION DE LA PROPRIETE DES DONNEES COLLECTEES

La protection accordée par la loi rencontre deux problèmes majeurs : le statut juridique des données personnelles et les questions liées au stockage des données notamment à l'étranger.

# 1. La question de la propriété des données personnelles

La loi n° 2009 - 09 du 22 mai 2009 portant protection des données à caractère personnel dispose :

**Article 11 :** Toute personne a le droit de s'opposer, sans frais, à l'utilisation des données la concernant à des fins de prospection, notamment commerciale, caritative ou politique, sans avoir à justifier d'un motif légitime.

**Article 13 :** Toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en œuvre les traitements automatisés dont la liste est accessible au public en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication.

**Article 15 :** Toute personne physique justifiant de son identité, peut exiger du responsable d'un traitement que soient, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées, les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation, la communication ou la conservation sont interdites.

Elle accorde ainsi aux personnes des droits opposables à tout responsable de traitement de données à caractère personnel. Ces droits et la protection ne se conçoivent que lorsque les données personnelles des individus sont considérées comme des éléments si propres et si attachés à la personne humaine ou au respect qui lui est dû; qu'elle doit être en mesure d'en contrôler le traitement c'est-à-dire la détention, l'usage et l'aliénation, par toute personne même autorisée à cette fin. On retrouve donc aisément, derrière cette conception des données personnelles, tous les attributs de la propriété fondant sa patrimonialisation. C'est qu'en effet, la question de l'exploitation voire abusive des données personnelles est aujourd'hui devenue essentielle.

L'affirmation d'un droit de propriété sur les données personnelles aux individus est dès lors posée comme moyen de protection des personnes : « L'informatique étant une science au service de l'homme, elle ne doit pas porter atteinte à l'identité humaine, à la vie privée de l'individu, aux droits de l'homme, aux libertés publiques, individuelles ou collectives ». En posant ce principe, le législateur béninois s'est mis d'office dans une posture de défense et de défiance des systèmes informatiques dans la pure tradition juridique civiliste qui ne rend susceptible de transaction et de propriété que des choses qui sont dans le commerce.

Mais la doctrine spécialisée est très opposée à cette conception parce qu' elle : «

- renvoie à l'individu la responsabilité de gérer et protéger ses données, renforce l'individualisme et nie le rapport de force entre consommateurs et entreprises ;
- ne pourrait que générer des revenus anecdotiques pour les usagers et susciter à l'inverse un marché de la gestion protectrice des données numériques ;
- déboucherait à un renforcement des inégalités entre citoyens en capacité de gérer, protéger et monétiser leurs données et ceux qui, par manque de littérature, de temps, d'argent ou autre, abandonneraient ces fonctions au marché... »

La réalité en vérité est très complexe : une personne est en droit de s'opposer à ce que son état de santé soit commenté dans un article destiné à susciter la curiosité du public et à exploiter à des fins commerciales sa vie privée. Mais elle peut céder et vendre son image.

Les pratiques tendent en effet aujourd'hui à reconnaître à l'utilisateur la possibilité de vendre ses propres données personnelles à des fins publicitaires et plus généralement de commercialiser ses données personnelles.

Pour Google Drive (Conditions d'utilisation), vous conservez les droits de propriété intellectuelle que vous détenez sur ce contenu. Ce qui est à vous reste à vous... « Nous ne revendiquons la propriété d'aucun de vos contenus, y compris les textes, données, informations et fichiers que vous mettez en ligne, partagez ou stockez dans votre compte Drive. Nos conditions d'utilisation nous permettent de vous offrir les services que vous souhaitez. Si vous décidez de partager un document avec un autre utilisateur ou si vous souhaitez l'ouvrir à partir d'un autre appareil, nous mettons cette fonctionnalité à votre disposition.

En résumé :

- Vous contrôlez qui peut accéder à vos fichiers dans Drive. Nous ne communiquons pas vos fichiers ni vos données à d'autres personnes, sauf dans les cas décrits dans nos Règles de confidentialité. Par exemple :
    - Nous ne transformons pas un document privé en document public.
    - Nous n'utilisons pas un document privé à des fins de marketing ou dans le cadre de campagnes de promotion.
    - Nous conservons vos données aussi longtemps que vous le désirez, mais pas au-delà.
    - Vous pouvez exporter vos données si vous décidez de ne plus utiliser Google Drive. »

Mais aux termes des mêmes conditions générales d'utilisation : « En soumettant des contenus à nos Services, par importation ou par tout autre moyen, vous accordez à Google (et à toute personne travaillant avec Google) une licence, dans le monde entier, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées (des traductions, des adaptations ou d'autres modifications destinées à améliorer le fonctionnement de vos contenus par le biais de nos services), de communication, de publication, de représentation publique, d'affichage ou de distribution public desdits contenus.

Les droits que vous accordez dans le cadre de cette licence sont limités à l'exploitation, la promotion ou à l'amélioration de nos services, ou au développement de nouveaux services. Cette autorisation demeure pour toute la durée légale de protection de votre contenu, même si vous cessez d'utiliser nos services (par exemple, pour une fiche d'entreprise que vous avez ajoutée à Google Maps) ».

Cette rédaction volontairement alambiquée de la relation avec les données de l'utilisateur se retrouve chez Android :

Les informations qui concernent l'Utilisateur sont destinées à « Les Applications Android.fr », responsable du traitement, à des fins de gestion et de suivi des relations commerciales et de prospection ainsi qu'à ses partenaires commerciaux et contractuels.

Les seules informations obligatoires sont votre pseudo, votre email et votre mot de passe. L'Utilisateur peut choisir de rendre visible ou non son email sur son profil public depuis son interface membre. Son email servira à lui transmettre occasionnellement des messages relatifs à son compte membre sur Les Applications Android.fr.

Les Applications Android.fr s'engagent à ne pas transmettre ces informations à un tiers dans un but

commercial ou de prospection (partenaires commerciaux, partenaires commerciaux, etc.). »

Chez Apple comme chez d'autres éditeurs ou fabricants :

« ... Apple, ses partenaires et concédants peuvent fournir certaines fonctionnalités ou services (par exemple, Localiser mon iPhone, Localiser mes Amis) qui s'appuient sur des informations de localisation provenant des appareils qui utilisent le système GPS (lorsqu'il est disponible), ainsi que des points d'accès hot-spot Wi-Fi publics et les localisations de tours de téléphonie mobile. Pour fournir ces fonctionnalités ou services lorsqu'ils sont disponibles, Apple, ses partenaires et concédants doivent recueillir, utiliser, transmettre, traiter et conserver vos données de localisation, y compris, notamment, la localisation géographique de votre appareil et de l'information liée à votre compte iCloud (« Compte ») et tout autre appareil enregistré ci- dessous, et, notamment, votre identifiant Apple, nom et identifiant d'appareil, et type d'appareil.

Le Service sauvegarde automatiquement et périodiquement le contenu des appareils iOS lorsqu'ils sont verrouillés, connectés à une source d'alimentation et connectés à Internet via un réseau Wi-Fi. iCloud stockera vos trois dernières sauvegardes ; cependant, si un appareil n'a pas été sauvegardé sur l'iCloud pendant une période de cent quatre-vingt (180) jours, Apple se réserve le droit de supprimer les sauvegardes associées à cet appareil. La sauvegarde se limite aux paramètres de l'appareil, caractéristiques de l'appareil, photos et vidéos, documents, messages (i Message, SMS et MMS), sonneries, données d'application (dont celles de Health), paramètres de localisation (tels que les rappels de géo localisation que vous avez paramétrés), l'écran d'accueil et à l'organisation des applications. […] Le « Contenu » désigne toute information pouvant être générée ou consultée par le biais de l'utilisation du Service, telle que les fichiers de données, les caractéristiques de l'appareil, le texte écrit, les logiciels, la musique, les graphiques, les photographies, les images, les sons, les vidéos, les messages et tout matériel similaire. Vous comprenez que la personne à l'origine du Contenu est l'unique responsable de l'ensemble de ce Contenu, qu'il soit diffusé publiquement ou transmis de manière privée sur le Service. [...]

À l'exception des informations pour lesquelles nous vous concédons une licence, Apple ne revendique aucun droit sur les informations ou le Contenu que vous publiez ou mettez à disposition grâce au Service. Cependant, en publiant ce Contenu sur des parties du Service accessibles au public ou à d'autres utilisateurs avec lesquels vous acceptez de partager ce Contenu, vous concédez à Apple une licence pour le monde entier, à titre gratuit, non exclusive, d'utilisation, de distribution, de reproduction, de modification, d'adaptation, de publication, de traduction, d'exécution et de diffusion publique du Contenu sur le Service uniquement aux fins pour lesquelles un tel Contenu a été publié ou mis à disposition, sans aucune compensation ou obligation envers vous. »

Bien que l'utilité se réduise à une peau de chagrin, ce qu'il faut nécessairement distinguer des **données personnelles** et que la loi n° 2009 - 09 du 22 mai 2009 portant protection des données à caractère personnel au Bénin confond sous le vocable données à caractère personnel, ce sont les données d'usage, ces informations et fichiers découlant de l'utilisation du produit.

**La loi béninoise les soumet au même régime alors même qu'à la différence des données personnelles qui relèvent d'un droit fondamental au respect de la vie privée dont chaque individu doit pouvoir contrôler le traitement, tous les éléments de la propriété des informations et données d'usage générées à l'insu même de l'utilisateur par le fonctionnement des systèmes informatiques produits et services, échappent à sa propriété notamment intellectuelle et appartiennent ou sont détenus par l'éditeur du logiciel d'exploitation, le fabricant du terminal mobile, le propriétaire du**

**serveur, du service ou de l'application utilisée.**

Lorsque vous décidez de mettre en ligne une vidéo que vous avez prise sur Internet ou d'effectuer un enregistrement sur les serveurs du Web, le « cloud », ou un téléchargement de vos photos et documents, dès le téléchargement, cette vidéo ou la photo ou le document mis en ligne ne vous appartient plus légalement. C'est en tout cas le verdict rendu il y a quelques mois par la justice américaine envers un utilisateur de Megaupload ; ce dernier souhaitait récupérer les données qu'il avait mises sur le site de partage, avec pour seul but de les sauvegarder. La justice américaine a approuvé le fait que les données sur Internet n'appartenaient pas aux internautes qui les mettaient en ligne, mais aux propriétaires des serveurs : autrement dit, Facebook, Google et autres Apple seraient les propriétaires de « nos » données sur le réseau. Ce qui pose évidemment les questions du régime juridique des données personnelles dans le cloud ou en stockage sur des serveurs situés à l'étranger.

## 2. Les limites de la protection liées à l'extranéité des opérations visées par la loi nationale

Qu'il s'agisse de l'établissement de l'entreprise ou du fournisseur du service logiciel, du stockage et de la conservation des données, ou de l'accomplissement d'une opération de traitement rentrant dans le champ d'application de la loi nationale, l'extranéité devient un fausset à la protection.

En effet, les limites de la vie privée sont diverses selon les sociétés, les cultures et les législations. « Les lois de police et de sûreté obligent tous ceux qui habitent le territoire ». Cette territorialité de la protection en est paradoxalement la première limite.

Il se superpose à cette territorialité une réalité évidente : la plupart des serveurs et plateforme de services des grands opérateurs, des éditeurs de système d'exploitation et d'applications et des fournisseurs de stockage sont situés à l'étranger et particulièrement dans des endroits gardés confidentiels. Les métadonnées sauvegardées à partir d'un terminal mobile utilisé au Bénin sont peut-être détenus en tout ou partie dans différents pays du monde.

Le principe en la matière est que lorsqu'un service sur téléphone mobile est assuré par une entreprise située dans un pays, celle-ci doit se conformer à la loi de ce pays. A cet égard la Cour de Justice de l'Union Européenne (CJUE) a jugé conformément à l'article 4, paragraphe 1, sous a), de la directive 95/46 « qu'un traitement de données à caractère personnel est effectué dans le cadre des activités d'un établissement du responsable de ce traitement sur le territoire d'un État membre, au sens de cette disposition, lorsque l'une ou plusieurs des trois conditions suivantes sont réunies :

- l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants de cet État membre, ou
- la société mère désigne une filiale implantée dans ledit État membre comme son représentant et comme étant responsable du traitement de deux fichiers spécifiques contenant les données des clients ayant conclu des services publicitaires avec cette entreprise, ou
- la succursale ou la filiale établie dans un État membre transmet à la société mère, basée en dehors de l'Union, les réclamations et les injonctions que lui adressent aussi bien les intéressés que les

autorités compétentes en vue d'obtenir le respect du droit à la protection des données à caractère personnel, même lorsque cette collaboration a lieu de manière volontaire ».

A contrario, la loi nationale n'a pas vocation à s'appliquer au litige, lorsque l'entreprise qui propose le service n'est pas située sur le territoire, qu'aucun serveur de l'entreprise n'est situé sur le territoire national ou lorsque l'entreprise, filiale ou succursale qui s'y trouve exerce une activité distincte ou ne disposant ni n'utilisant aucun moyen de traitement de données à caractère personnel sur ce territoire. II faut à cet égard, pour que le responsable du traitement de données personnelles soit soumis à cette loi, que des moyens de traitement soient mis en œuvre sur le territoire national, à l'exclusion de ceux qui ne sont utilisés qu'à des fins de transit.

Ainsi en pratique seule a vocation à s'appliquer et s'applique la loi étrangère soit en raison de la production sur le territoire étranger du fait générateur du dommage allégué, soit en raison l'archivage des messages ou l'atteinte aux données personnelles. Ainsi il est jugé que « **les conséquences de l'atteinte à la vie privée ou de la violation du droit sur l'image relèvent de la loi du lieu où les faits ont été commis** ». Ce qui rend l'accès à la défense des droits ou l'exécution des décisions judiciaires particulièrement difficiles.

Au Bénin l'article 9 de la loi n°2009 - 09 du 22 mai 2009 portant protection des données à caractère personnel prévoit par ailleurs que « le responsable d'un traitement de données à caractère personnel ne peut transférer des données vers un Etat étranger que si ledit Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes concernées par ces données ». L'application de cette condition de réciprocité évoque deux préoccupations :

- Celle de l'autorisation recueillie de l'utilisateur du terminal ou plus généralement de certaines «exceptions» qui permettent le flux de données vers des pays tiers : C'est notamment le cas lorsque les personnes concernées donnent leur consentement indubitable au transfert de leurs données vers un tel pays, ou lorsque le transfert est nécessaire pour exécuter un contrat avec la personne concernée, ou lorsque les données proviennent d'un registre public destiné à l'information du public (annuaire téléphonique, registre du commerce, par exemple). Il est jugé dans ce cas que « force est de constater qu'une fois le choix fait par la demanderesse de s'inscrire à un ou plusieurs groupes de discussion, celle-ci ne pouvait ignorer que l'adresse électronique qu'elle faisait choix d'utiliser était portée à la connaissance de toute personne intéressée ; qu'elle a entendu faire choix de ses prénom et nom pour deux de celles qu'elle a utilisées, la troisième étant composée de la première lettre de son prénom suivie de son nom ; qu'elle demande pourtant, outre la suppression des bases de données du service Google Groupes, les messages qu'elle a envoyés, la suppression de toute information relative à ses nom et prénom des index ou de la mémoire cache du moteur de recherche de ce service.

Qu'il ne s'impose pas avec évidence à cette juridiction que le traitement mis en cause puisse consister en des opérations de collecte sans autorisation de données personnelles ».

- La seconde préoccupation est celle de la protection offerte par les lois étrangères aux étrangers dans ces pays. A ce sujet il faut observer que les lois des pays étrangers ne protègent que les personnes établies sur leurs territoires, la surveillance des communications électroniques ou le Patriot Act aux Etats Unis n'étant particulièrement applicable dans leurs aspects les plus critiquables, qu'aux étrangers. C'est dans ce contexte que la définition de **la notion de niveau de protection adéquat ou suffisant** est devenue essentielle. En effet elle n'a fait l'objet d'aucune définition dans la loi. Le

législateur béninois n'y échappe pas. Une décision de la Commission européenne, datant de 2000, dite « Safe Harbor » ou « sphère de sécurité », permettait le transfert de données personnelles d'Europe vers les Etats-Unis en ce que ce pays présente des garanties suffisantes pour la protection de la vie privée. La CJUE a apporté une réponse magistrale à cette lacune dans l'Union Européenne : « pour être adéquate, la protection doit être substantiellement équivalente. Cela suppose d'examiner l'ensemble du système de protection mis en place dans l'ordre juridique de l'État concerné, c'est-à-dire sa législation interne mais également ses engagements internationaux ». Dans son arrêt Schrems rendu le mardi 6 octobre 2015, la CJUE estime que le Safe Harbor n'est pas conforme au droit européen. La décision Safe Harbor consacre « la primauté des exigences relatives à la sécurité nationale, [à] l'intérêt public et [au] respect des lois des États-Unis ». Elle n'apporte aucune garantie contre les ingérences dans les droits fondamentaux des personnes dont les données sont transférées aux États-Unis ni contre les risques d'abus. La généralité des dérogations ainsi que leurs utilisations ne permet pas d'assurer que les ingérences dans la protection des données personnelles soient limitées au strict nécessaire ». La CJUE relève donc comme un désavantage, le champ d'application restreint de la décision Safe Harbor qui finalement laisse les autorités publiques américaines en dehors des principes qu'elle pose.

La doctrine note que « la notion de niveau adéquat de protection ne signifie pas que la protection assurée dans l'État tiers doit être identique à celle garantie dans l'UE, mais elle doit offrir une protection adéquate des droits des citoyens européens ».

# CONCLUSION

Le décloisonnement entre la vie privée et les échanges par communication électronique impacte immédiatement la vie privée des personnes et la confidentialité de leurs données personnelles.

Ces problèmes n'ont pas été causés seulement par les changements technologiques mais aussi par un changement dans leur mode d'utilisation qui a rendu le téléphone mobile plus intrusif. La préoccupation qui va accaparer désormais les esprits est la suivante. Est-ce l'atteinte qui doit être limitée ou est-ce la vie privée qui doit céder du terrain ?

# PARTIE - IV

## ANNEXE

## QUELQUES DELIBERATIONS

**Délibération n° 2018-004/AT/CNIL du 11 Avril 2018**

**Portant autorisation de traitement des données alpha-numériques et biométriques des Clients et Usagers de SAM AY SARL**

La Commission Nationale de l'Informatique et des Libertés (CNIL), réunie en séance plénière, sous la présidence de M. Etienne Marie FIFATIN ;

Étant également présents, les Commissaires :

- DEGBEY Jocelyn ;
- BIO TCHANE MAMADOU Ismath ;
- ABOU SEYDOU Amouda ;
- TCHOBO Valère ;
- LEKOYO Imourane ;
- BENON Nicolas ;
- ZOUMAROU Wally Mamoudou ;
- YEKPE Guy-Lambert ;

**Vu** la loi n° 2009-09 du 22 mai 2009 portant protection des données à caractère personnel en République du Bénin ;

**Vu** le décret n° 2015-533 du 06 novembre 2015 portant nomination des membres de la Commission Nationale de l'Informatique et des Libertés (CNIL), deuxième mandature ;

**Vu** le décret n° 2016-513 du 24 août 2016 portant nomination de Madame Félicité AHOUANDOGBO née TALON en qualité de Commissaire du Gouvernement près la Commission Nationale de l'Informatique et des Libertés (CNIL) ;

**Vu** le décret n° 2016-606 du 26 septembre 2016 modifiant le décret n° 2015-533 du 06 novembre 2015 portant nomination de Madame Ismath BIO-TCHANE et de Monsieur Onésime Gérard MADODE, en qualité de membres de la Commission Nationale de l'Informatique et des Libertés (CNIL) ;

**Vu** le règlement intérieur de la Commission Nationale de l'Informatique et des Libertés (CNIL) en date du 05 janvier 2011 ;

**Vu** la lettre n°004/DO/DG en date du 28 Février 2018 portant demande d'autorisation de traitement de données à caractère personnel transmise avec le formulaire y afférent dûment rempli, aux fins de la mise en œuvre de collecte et de traitement des données à caractère personnel des clients et Usager de SAM AY SARL ;

**Vu** le rapport du Commissaire Guy-Lambert YEKPE ;

Après en avoir délibéré en présence du Commissaire du Gouvernement, Madame Félicité AHOUANDOGBO née TALON qui a fait ses observations ;

**EMET LA DECISION SUIVANTE :**

## *I- Objet de la demande d'autorisation et responsable du traitement*

### *I-1. Objet*

Le Directeur Général de SAM AY SARL sollicite une autorisation (lettre n°004/DO/DG en date du 28 Février 2018) de la Commission Nationale de l'Informatique et des Libertés, en vue du traitement automatisé des données alpha-numériques et biométriques de ses clients et usagers.

### *I-2. Responsable du traitement*

Est considérée comme responsable de traitement, toute personne qui, « seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ».

En l'espèce, le Directeur Général de SAM AY SARL Bénin est le responsable du traitement.

## *II- Examen de la demande d'autorisation du traitement*

### *II-1. Recevabilité*

Au regard des dispositions des articles 1 et 43 de la loi n° 2009-09 du 22 mai 2009 portant protection des données à caractère personnel en République du Bénin, la demande est recevable.

### *II-2. Finalité*

Aux termes des dispositions de l'article 5-a-b-c de la loi portant protection des données à caractère personnel, « un traitement de données à caractère personnel ne peut porter que sur des données remplissant les conditions ci-après :

a) être collectées et traitées de manière loyale et licite ;
b) être collectées pour des finalités bien déterminées, explicites, légitimes et non frauduleuses ;
c) ne pas être traitées ultérieurement de manière incompatible avec les finalités ainsi déterminées…».

SAM AY SARL déclare que les finalités poursuivies par la collecte et le traitement des données à caractère personnel de ses clients sont :

- l'assistance technique ;
- la gestion rationnelle et efficace de sa base de données clients ;
- le suivi en temps réel des activités de ses clients.

La Commission estime que les finalités existent, qu'elles sont légitimes, explicites et non frauduleuses.

### *II-3. Droits des personnes concernées*

#### ***Droit à l'information préalable***

Aux termes des dispositions de l'article 12-a-b-c de la loi 2009-09 du 22 mai 2009, « la personne auprès de laquelle sont recueillies des données à caractère personnel la concernant doit être informée par le responsable du traitement ou son représentant :

a) de l'identité du responsable de traitement ou de celle de son représentant ;
b) de l'objectif poursuivi à travers le traitement ;
c) du caractère obligatoire ou facultatif des informations qui sont demandées et des réponses fournies …».

La CNIL note que les clients et usagers de SAM AY SARL exercent leur droit à l'information préalable par le biais des questionnaires et des affiches.

#### ***Droit d'accès***

Aux termes des dispositions de l'article 13 de la loi no 2009-09 du 22 mai 2009 portant protection des données à caractère personnel en République du Bénin, « Toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en œuvre les traitements automatisés dont la liste est accessible au public en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échant, d'en obtenir communication ».

La Commission constate que l'exercice du droit d'accès des personnes concernées par le traitement est garanti par le requérant. La personne concernée fait une demande verbale et jouit du droit d'accès immédiat.

La CNIL en prend acte mais suggère au requérant de prévoir également d'autres voies de réclamations notamment par courrier postal ou électronique.

- ***Droits de rectification, d'opposition et de suppression***

Conformément aux dispositions des articles 12-e et 15 de la loi informatique et libertés, des modalités d'exercice des droits de rectification, d'opposition et de suppression par les personnes concernées, doivent être assurées par le responsable du traitement.

Selon les renseignements fournis par le requérant, aucune mesure n'a été prise en ce qui concerne l'exercice des droits d'opposition, de rectification et de suppression.

### *II-4. Proportionnalité*

Conformément aux dispositions de l'article 5-d, les données collectées doivent « être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ».

Les catégories de données collectées sont : nom et prénoms, raison sociale, adresses, téléphone, personnes à contacter (nom, prénoms, numéro de téléphone des personnes), empreintes digitales.

La CNIL considère que les catégories de données visées par le traitement sont adéquates, pertinentes et non excessives au regard des finalités.

### *II-5. Durée de conservation des données collectées*

Selon le requérant, la durée de conservation des données est illimitée pour des besoins de gestion et d'exploitation des activités de l'entreprise.

La CNIL rappelle qu'aux termes des dispositions de l'article 5-f de la loi no 2009-9 du 22 mai 2009, les données à caractère personnel collectées doivent « être conservées sous une forme permettant l'identification des personnes concernées pendant un délai n'excédant pas la durée nécessaire à l'atteinte des finalités pour lesquelles elles sont collectées ou traitées ... ».

Par conséquent, SAM AY SARL devra procéder à la suppression des données collectées dès cessation des relations d'affaires avec les clients et usagers.

### *II-6. Traitement des données biométriques*

Le recours à la collecte des données biométriques par le demandeur se justifie par l'existence d'un contrat d'assistance technique.

Il précise par ailleurs que ces données sont conservées et stockées sur les équipements de traitement de données.

La CNIL estime que le traitement des données biométriques est justifié au regard de la loi.

### *II-7. Sécurité*

Aux termes des dispositions de l'article 50 de la loi portant protection des données à caractère personnel, « Le responsable du traitement est tenu de prendre toutes précautions utiles au regard de la nature des données et des risques présentés par le traitement pour préserver la sécurité des données et, notamment empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès ».

#### ***Sécurité physique des équipements et locaux***

La sécurité physique des locaux abritant les équipements de traitement des données est assurée par des verrous de sécurité.

La CNIL en prend acte mais juge que les dispositions de sécurité physique des locaux doivent être renforcées par des systèmes de gardiennage et d'accès électroniques pour une bonne gestion des accès.

#### ***Sécurité pour assurer la sauvegarde et la confidentialité des données***

Les mesures prises pour la sauvegarde et la confidentialité des données se fait grâce aux générations de logs système.

La CNIL en prend acte mais juge les mesures insuffisantes et recommande le recours aux mots de passe renforcés (au moins 8 caractères composés de lettres, de chiffre et des caractères spéciaux).

**Par ces motifs,**

**Enjoint à SAM AY SARL de :**

**1- Notifier à la CNIL dans un délai de deux (02) mois à compter de la réception de la présente délibération, une déclaration de conformité portant sur les dispositions adéquates à prendre afin d'assurer la sécurisation optimale des locaux et salles hébergeant les équipements informatiques de traitement et des données ;**

2- **prendre des dispositions appropriées afin que les mesures de sécurité de son système respecte les normes de sécurité informatique requises : mot de passe d'au moins 8 caractères (lettres, chiffres et caractères spéciaux) et des mesures appropriées pour la sauvegarde et la confidentialité des données.**

3- **conserver les données personnelles des clients et usagers pendant un délai n'excédant pas la durée nécessaire à l'atteinte des finalités, dès cessation des relations d' affaires, suivant les dispositions de l'article 5-f de la loi 2009-09 du 22 mai 2009 portant protection des données à caractère personnel en République du Bénin ;**

4- **prendre des mesures appropriées pour que l'exercice des droits d'opposition, de rectification et de suppression des personnes concernées par le traitement soient assurées aux personnes concernées.**

5- **prévoir d'autres formes de droit d'accès (courrier postal, électronique) en plus de la demande verbale.**

**Sous réserve de la prise en compte de ce qui précède,**

**Autorise SAM AY SARL à mettre en œuvre le traitement de données visé dans la présente délibération.**

**Conformément à l'article 19 et 21-b de la loi portant protection des données à caractère personnel en République du Bénin, la CNIL se réserve le droit de procéder à des contrôles ultérieurs aux fins de s'assurer du respect, par le requérant, des recommandations et décisions objets de la présente délibération.**

Le Président,

**Etienne Marie FIFATIN**

**Délibération n° 2018-005/AT/APDP du 27 décembre 2018**

**Portant autorisation de collecte, de traitement et de transfert de la base de données clients des abonnés de MTN Mobile Money vers le GHANA**

L'Autorité de Protection des Données Personnelles (APDP), réunie en séance plénière, sous la présidence de M. Etienne Marie FIFATIN ;

Etant également présents, les Conseillers :

- BENON Nicolas ;
- ZOUMAROU Wally Mamoudou ;
- YEKPE Guy-Lambert ;
- ABOU SEYDOU Amouda ;
- OKE Soumanou ;
- MADODE Onésime Gérard ;
- LEKOYO Imourane.

**V**u la loi no 90-32 du 11 décembre 1990 portant Constitution de la République du Bénin ;

**V**u la loi n° 2017-20 du 20 avril 2018 portant code du Numérique en République du Bénin ;

**V**u le décret n° 2015-533 du 06 novembre 2015 portant nomination des membres de l'Autorité de Protection des Données Personnelles (APDP) précédemment, Commission Nationale de l'Informatique et des Libertés (CNIL), deuxième mandature ;

**V**u le décret n° 2016-513 du 24 août 2016 portant nomination de Madame Félicité AHOUANDOGBO née TALON en qualité de Commissaire du Gouvernement près l'APDP précédemment, Commission Nationale de l'Informatique et des Libertés (CNIL) ;

**V**u le décret n° 2016-606 du 26 septembre 2016 modifiant le décret n° 2015-533 du 06 novembre 2015 portant nomination de Madame Ismath BIO TCHANE et de Monsieur

Onésime Gérard MADODE, en qualité de membres de l'APDP précédemment, Commission Nationale de l'Informatique et des Libertés (CNIL) ;

**V**u le règlement intérieur de la Commission Nationale de l'Informatique et des Libertés (CNIL) en date du 05 janvier 2011 ;

**V**u la lettre n° 148/MSF/AML//DG/2018 en date du 30 octobre 2018 par laquelle le Directeur Général de MTN Mobile Money a sollicité une autorisation de l'Autorité de Protection des Données Personnelles (APDP), relative au traitement automatisé et au transfert des données alphanumériques de ses clients vers une des filiales du groupe MTN GHANA ;

**V**u le rapport du Conseiller Amouda ABOU SEYDOU de l'Autorité de Protection des Données Personnelles ;

Après en avoir délibéré en présence du Commissaire du Gouvernement, Madame Félicité AHOUANDOGBO née TALON qui a fait ses observations ;

**EMET LA DECISION SUIVANTE :**

## *I- Objet de la demande d'autorisation et responsable du traitement*

### *I-1. Objet*

Par lettre n° 148/MFS/AML/DG du 30 Octobre 2018, le Directeur Général de MTN Mobile Money, a demandé à l'Autorité de Protection des Données Personnelles (APDP), l'autorisation de collecte, de traitement et de transfert des données alphanumériques de ses abonnés du Bénin vers le Ghana.

### *I-2. Responsable du traitement*

Est considéré comme responsable de traitement, aux termes des dispositions de l'article 1er du livre préliminaire de la loi no 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin :

« Toute personne physique ou morale, l'autorité publique, le service ou tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités et les moyens ».

En l'espèce, le responsable du traitement est le Directeur Général de MTN Mobile Money.

## *II- Examen de la demande d'autorisation du traitement*

### *II-1. Recevabilité*

Au regard des dispositions des articles 380 et 407 de la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, la demande est recevable.

### *II-2. Finalité*

Aux termes des dispositions de l'article 383 de la loi portant code du numérique, :

« Les données à caractère personnel doivent être :

 collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables ».

MTN Mobile Money indique que la finalité poursuivie par le traitement envisagé est d'assurer la synchronisation et la réplication des données à caractère personnel en vue de la restauration de la base de données en cas de sinistre ou d'incident.

L'Autorité estime que la finalité existe, qu'elle est légitime, explicite et non frauduleuse.

### *II-3. Droits des personnes concernées*

#### *II.3.1- Droit à l'information préalable et au respect du principe de consentement et de légitimité*

 ***Droit à l'information préalable***

Aux termes des dispositions de l'article 415 de la loi portant code du numérique en République du Bénin :

« Le responsable du traitement ou son représentant doit fournir à la personne dont les données font l'objet d'un traitement, ou au plus tard, lors de la collecte et quels que soient les moyens et supports employés, ou au moins les informations suivantes :

- Son identité et l'adresse de sa résidence habituelle et le cas échéant, les coordonnées de son représentant… ».

L'Autorité note, au regard du formulaire renseigné par le requérant, que les personnes concernées bénéficient du droit à l'information préalable sur la base de mentions légales et par voie de courrier électronique.

- ***Respect du Principe de consentement et de légitimité***

Conformément aux dispositions des articles 389 alinéa 1er, 390 et 415 points 8 et 10 de la loi portant code du numérique, le consentement des personnes concernées est requis.

Le réquérant précise qu'il requiert le consentement des personnes dont les données sont collectées sous forme écrite et par le biais d'un formulaire.

L'Autorité note que le requérant a prévu et garanti le respect du principe de consentement préalable et de légitimité aux personnes concernées par le traitement envisagé.

### *II.3.2- Droit d'accès*

Aux termes des dispositions de l'article 437 du code du numérique portant protection des données à caractère personnel en République du Bénin, « Toute personne physique dont les données à caractère personnel font l'objet d'un traitement peut demander au responsable de ce traitement :

1- les informations permettant de connaître et de contester le traitement de ses données à caractère personnel ;

2- la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de traitement, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées ;

3- la communication sous forme intelligible des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ; … ».

L'Autorité note que le droit d'accès des clients à leurs données personnelles est assuré par MTN Mobile Money. Ce droit s'exerce par une requête adressée au responsable du traitement par courriel ou lors d'une visite en agence.

Conformément aux dispositions de l'article 437 du code du numérique, l'APDP note que le délai de communication des informations demandées en cas d'exercice du droit d'accès fixé à quatorze (14) jours par le requérant est raisonnable.

### *II.3.3- Droit d'opposition*

Conformément aux dispositions de l'article 440 du code du numérique, « Toute personne physique a le droit de s'opposer, à tout moment, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement… ».

L'exercice de ce droit par les personnes concernées par le traitement, se fait auprès du responsable de traitement et entraine de fait la rupture du contrat les liant.

L'APDP rappelle au requérant qu'il dispose de trente (30) jours pour donner suite à la demande d'opposition de la personne dont les données sont collectées.

### *II.3.4- Droit de rectification et de suppression*

Conformément aux dispositions de l'article 441 de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin, les droits de rectification et de suppression par les personnes concernées doivent être assurés par le requérant.

Ce droit est garanti par le requérant à ses clients et se fait par une demande adressée par ceux-ci au responsable de traitement pour la mise à jour des informations les concernant.

L'Autorité en prend acte mais rappelle que le délai de réponse ne saurait excéder les quarante-cinq (45) jours qui suivent la réception de la demande du client conformément aux dispositions de l'article sus-cité.

### *II-4. Proportionnalité*

Conformément aux dispositions de l'article 383-4 :

« Les données collectées doivent être :

… ;

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

… ».

En l'espèce, les personnes concernées par le traitement sont les abonnés de MTN Mobile Money.

Les catégories de données collectées sont de deux ordres. Il s'agit principalement des données :

a. d'identification des abonnés à l'état civil ( nom et prénoms, Numéro de pièce d'identité, date de naissance, adresse);

b. financières.

Lesdites informations sont recueillies directement auprès des personnes concernées.

L'APDP considère que les catégories de données objets du traitement sont adéquates, pertinentes et non excessives au regard des finalités poursuivies.

### *II-5. Durée de conservation des données collectées*

Le requérant envisage conserver les données collectées pour une durée de 10 ans aux fins de gestion et d'exploitation des activités de l'entreprise conformément aux dispositions réglementaires en vigueur **(article 11 de la directive n°07/2006-14 du 31 octobre 2006 portant lutte contre le blanchiment des capitaux au Bénin et l'article 35 de la directive N°02/2015/CM/UEMOA relative à la lutte contre le blanchiment de capitaux et le financement du Terrorisme)**.

L'Autorité note que la durée de conservation des données est en adéquation avec la finalité du traitement envisagé.

### *II-6. Interconnexion de bases de données avec certaines banques et autres institutions financières nationales*

MTN Mobile Money indique dans son dossier qu'il a aussi interconnecté au Bénin sa base de données clients avec celles de certaines banques et autres institutions financières.

L'APDP rappelle au réquérant, que conformément aux dispositions de l'article 407. 5 du code du numérique « les traitements de données… » doivent être soumis à l'autorisation préalable de l'APDP avant leur mise en œuvre.

### *II-7. Interconnexion de bases de données avec le Ghana :*

#### ***Catégories de données concernées par l'interconnexion***

Le réquérant indique que les données identification KYC des abonnés (Nom et Prénoms, Numéro de pièce d'identité, Date de naissance, Adresse…) sont celles retenues pour être transférées au Ghana y compris des informations financières.

#### ***Durée de conservation de l'interconnexion avec le Ghana :***

Elle a une durée de conservation permanente et illimitée. MTN Mobile Money justifie la durée d'interconnexion pour des besoins de transfert des données au fil de l'eau et de restauration des données sans délai en cas de sinistre.

### *II-8. Sous-Traitance*

Le requérant indique qu'il utilise les services d'un sous-traitant dénommé "ERICSSON" qui assure la gestion de la base de données entre autres.

### *II-8. Sécurité*

#### ***Sécurité physique des locaux abritant les équipements***

Un protocole formalisé d'accès aux locaux et salles informatiques hébergeant les équipements de traitement et de sauvegarde des données collectées est mis en œuvre par le requérant.

En effet, l'accès au bâtiment s'effectue par badge. Un registre des entrées et sorties est renseigné par le requérant.

### ***Sécurité logique des données***

L'étude du système mis en place révèle que des mesures de sécurité pour assurer la confidentialité, l'intégrité et la disponibilité des données ont été prises.

Néanmoins, le réquérant doit se conformer aux dispositions de l'article 426 du code du numérique en ses points 1,3 et 4.

Elle recommande toutefois au réquérant de prévoir des mesures idoines permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci le plus rapidement possible en cas d'incident physique, technique ou de sinistre.

## ***III- Examen de la demande de transfert des données collectées***

MTN Mobile Money sollicite l'autorisation de l'Autorité aux fins de transfert des données à caractère personnel de ses clients vers SCANCOM LIMITED au GHANA qui n'est autre qu'une filiale du Groupe MTN.

Pour cette demande, il y a lieu de se référer à l'analyse précédente sur les points ci-après : consentement et principe de légitimité, droits d'accès, d'opposition, de rectification, de suppression, durée du traitement et mesures de sécurité liées au transfert.

Il est également nécessaire d'examiner : la finalité, la proportionnalité et les garanties dans le pays destinataire.

### ***III-1 Finalité***

Le transfert électronique des données à caractère personnel des clients de MTN Mobile Money sur des serveurs basés au Ghana, vise l'hébergement, la redondance, la continuité de service et la récupération de celles-ci en cas de sinistre.

Le transfert des données envisagé est donc justifié au regard de la finalité.

### ***III-2 Proportionnalité***

Les données transférées concernent les logs de transaction et la liste des abonnés de MTN Mobile Money.

L'APDP considère que ces données faisant l'objet de transfert sont adéquates, pertinentes et non excessives au regard des finalités.

### *III-2 Garantie dans le pays destinataire*

Conformément aux dispositions de l'article 391 alinéa 1er du code du numérique, « le transfert de données à caractère personnel faisant l'objet d'un transfert vers un État tiers ou une organisation internationale ne peut avoir lieu que lorsque l'Autorité constate que l'État ou l'organisation internationale en question, assure un niveau de protection équivalant à celui mis en place par les dispositions du présent livre (livre 5ième) ».

Il ressort du dossier que les données collectées seront transférées à SCANCOM LIMITED Ghana, filiale du groupe MTN qui dispose d'une autorisation délivrée par l'Autorité du Ghana « Ghana Data Protection Commission » Sous le N° DC15100000274S en date du 06/10/2018 et qui Expire le 05/10/ 2020.
L'APDP en prend acte

**Par ces motifs,**

**enjoint au réquérant d'avoir à :**

- **déclarer auprès de l'Autorité l'interconnexion de sa base de données à celle des banques et autres Institutions financières nationales conformément aux dispositions de l'article 407.5 du code du numérique;**

- **inviter également les Institutions financières interconnectées à sa base de données à se rapprocher de l'Autorité aux fins d'accomplir les formalités liées audit traitement.**

**rappelle que :**

- **le traitement déclaré ne saurait être détourné de ses finalités ;**

- **le responsable du traitement ou son représentant veille au respect des mesures de sécurité conformément aux dispositions de l' article 426 ;**

- **un registre des activités du traitement soit tenu, conformément aux dispositions de l'article 435 du code du numérique ;**

- **un rapport d'activités, en application des dispositions de l'article 387 du code du numérique soit adressé annuellement à l'Autorité ;**

- **sa responsabilité est engagée, en cas de manquement aux dispositions de l'article 451 du code du numérique.**

**Sous réserve de ce qui précède,**

**Autorise, la mise en œuvre du traitement automatisé des données à caractère personnel des clients de MTN Mobile Money et le transfert des données les concernant.**

**Conformément aux dispositions des articles 462 et 489 de la loi portant code du numérique en République du Bénin, l'APDP se réserve le droit de procéder à des contrôles ultérieurs aux fins de s'assurer du respect par le requérant des termes et conditions de la présente délibération.**

Le Président,

**Etienne Marie FIFATIN**

**Délibération n° 2018-006 /AT/APDP du 27 décembre 2018 portant autorisation de collecte et de traitement des données alpha numériques et biométriques des propriétaires et présumés propriétaires de parcelles dans la Commune d'Abomey-Calavi**

L'Autorité de Protection des Données Personnelles (APDP), réunie en séance plénière, sous la présidence de M. Etienne Marie FIFATIN ;

Etant également présents, les Conseillers :

- BIO TCHANE MAMADOU Ismath ;
- BENON Nicolas ;
- YEKPE Guy-Lambert ;
- ABOU SEYDOU Amouda ;
- OKE Soumanou ;
- TCHOBO Valère ;
- LEKOYO Imourane.

**Vu** la loi no 90-32 du 11 décembre 1990 portant Constitution de la République du Bénin ;

**Vu** la loi n° 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin ;

**Vu** le décret n° 2015-533 du 06 novembre 2015 portant nomination des membres de la Commission Nationale de l'Informatique et des Libertés (CNIL), deuxième mandature ;

**Vu** le décret n° 2016-513 du 24 août 2016 portant nomination de Madame Félicité AHOUANDOGBO née TALON en qualité de Commissaire du Gouvernement près la Commission Nationale de l'Informatique et des Libertés (CNIL) ;

**Vu** le décret n° 2016-606 du 26 septembre 2016 modifiant le décret n° 2015-533 du 06 novembre 2015 portant nomination de Madame Ismath BIO TCHANE et de Monsieur Onésime Gérard MADODE, en qualité de membres de la Commission Nationale de l'Informatique et des Libertés (CNIL) ;

**Vu** le règlement intérieur de la Commission Nationale de l'Informatique et des Libertés (CNIL) en date du 05 janvier 2011 ;

**Vu** la lettre n° 21/2065/C-AC/DC/SG/DAU/SAC en date du 19 septembre 2018 par laquelle le Maire de la Commune d'Abomey-Calavi a saisi l'APDP d'une requête aux fins d'autorisation de collecte et de traitement des données alpha-numériques et biométriques des propriétaires et présumés propriétaires de parcelles dans sa Commune ;

**Vu** le rapport du Conseiller Nicolas BENON de l'Autorité de Protection des Données Personnelles ;

Après en avoir délibéré en présence du Commissaire du Gouvernement Madame Félicité AHOUANDOGBO née TALON qui a fait ses observations ;

**IL EST EXPOSÉ CE QUI SUIT :**

## *I- Objet de la demande d'autorisation et responsable du traitement*

### *I-1. Objet*

Par lettre n° 21/2065/C-AC/DC/SG/DAU/SAC en date du 19 septembre 2018, le Maire de la Commune d'Abomey-Calavi a saisi l'APDP d'une requête aux fins d'autorisation pour procéder à la constitution d'une base de données à caractère personnel des propriétaires et présumés propriétaires de parcelles dans ladite Commune.

### *I-2. Responsable du traitement*

Est considéré comme Responsable du traitement, aux termes des dispositions de l'article 1er du livre préliminaire de la loi no 2017-20 du 20 avril 2018 :

**« Toute personne physique ou morale, l'autorité publique, le service ou tout autre organisme ou association qui, seul ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel et en détermine les finalités et les moyens ».**

En l'espèce, le Responsable du traitement est le Maire de la Commune d'Abomey-Calavi.

## *II- Examen de la demande d'autorisation du traitement*

### *II-1. Recevabilité*

A l'analyse, la requête du Maire d'Abomey-Calavi est recevable au regard des dispositions des articles 380 et 407 de la loi 2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.

### *II-2. Finalité*

Conformément aux dispositions de l'article 383 de la loi 2017-20 du 20 avril 2018 portant code du numérique, :

**« Les données à caractère personnel doivent être :**

- **collectées pour des finalités déterminées, explicites et légitimes et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables ».**

Le requérant indique que la finalité poursuivie par le traitement envisagé est de créer une base de données des propriétaires et présumés propriétaires de parcelles dans sa Commune afin d'assurer la traçabilité des cessions de parcelles et de lutter contre l'insécurité foncière.

### *II-3. Droits des personnes concernées*

#### *II.3.1- Droit à l'information préalable et respect du principe de consentement et de légitimité*

- ***Droit à l'information préalable***

Conformément aux dispositions de l'article 415 de la loi 2017-20 du 20 avril 2018 portant code du numérique :

**« Le responsable du traitement ou son représentant doit fournir à la personne dont les données font l'objet d'un traitement, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, au moins les informations suivantes :**

**- son identité et l'adresse de sa résidence habituelle ou de l'établissement principal et, le cas échéant, les coordonnées de son représentant … »**

L'Autorité note, au regard du formulaire renseigné par le requérant, que les personnes concernées bénéficient du droit à l'information préalable sur la base de questionnaires et d'affiches.

Elle rappelle cependant au requérant que cette modalité d'information n'est pas suffisante.

Le requérant est donc invité à recourir à d'autres moyens d'information complémentaires tels que les médias audiovisuels notamment pour les personnes concernées non-alphabétisées.

- ***Respect du Principe de consentement et de légitimité***

Conformément aux dispositions des articles 389 alinéa 1er, 390 et 415 points 8 et 10 de la loi portant code du numérique, le consentement des personnes concernées est requis.

L'Autorité note que le requérant a prévu et garanti le respect du principe de consentement préalable et de légitimité aux personnes concernées par le traitement envisagé.

L'Autorité en prend acte.

### *II.3.2- Droit d'accès et droit d'interrogation*

- ***Droit d'accès***

L'article 437 du code du numérique dispose que :

**« toute personne physique dont les données à caractère personnel font l'objet d'un traitement peut demander au responsable de ce traitement :**

1- les informations permettant de connaître et de contester le traitement de ses données à caractère personnel ;

2- la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de traitement, ainsi que des informations portant au moins sur les finalités du traitement, les catégories de données sur lesquelles il porte et les catégories de destinataires auxquels les données sont communiquées ;

3- la communication sous forme intelligible des données à caractère personnel qui la concernent ainsi que de toute information disponible quant à l'origine de celles-ci ;… ».

L'Autorité note que le droit d'accès des propriétaires et présumés propriétaires de parcelles à leurs données personnelles est assuré par le Maire en rapport avec son partenaire technique. Ce droit s'exerce au moyen d'une demande verbale adressée au Responsable du Traitement qui instruit aussitôt son partenaire technique pour donner suite aux requêtes formulées par la personne concernée.

La communication des informations demandées en cas d'exercice de ce droit est instantanée selon le requérant.

L'Autorité recommande au requérant de prévoir pour les personnes concernées par le traitement, l'exercice du droit d'accès par une demande écrite datée, signée et transmise par voie postale ou électronique au Responsable du traitement ou à son représentant, conformément aux dispositions de l'article 437 alinéa 2 du code du numérique.

- ***Droit d'interrogation***

Conformément aux dispositions de l'article 439 du code du numérique :

**« toute personne justifiant de son identité a le droit d'interroger les services ou organismes chargés de mettre en œuvre les traitements automatisés dont la liste est accessible au public en vue de savoir si ces traitements portent sur des informations nominatives la concernant et, le cas échéant, d'en obtenir communication ».**

Dans le cas d'espèce, ce droit est non requis.

### *II.3.3- Droit d'opposition*

Prévu par les dispositions de l'article 440 de la loi 2017-20 du 20 avril 2018, ce droit est assuré aux personnes concernées par le Responsable du traitement.

L'exercice du droit d'opposition par les propriétaires et présumés propriétaires se fait auprès du Responsable du traitement.

L'Autorité en prend acte et rappelle que s'agissant du droit d'opposition, le délai de réponse ne saurait excéder les trente (30) jours qui suivent la réception de la demande.

### *II.3.4- Droit de rectification et de suppression*

Ces droits sont garantis par le requérant, conformément aux dispositions de l'article 441 du code du numérique.

L'Autorité en prend acte mais rappelle que le délai de réponse ne saurait excéder les quarante-cinq (45) jours qui suivent la réception de la demande.

### *II-4. Proportionnalité*

Conformément aux dispositions de l'article 383-4 :

« Les données collectées doivent être :

… ;

 adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ; … ».

En l'espèce, les personnes concernées par le traitement sont les propriétaires et présumés propriétaires de parcelles dans la Commune d'Abomey-Calavi.

Les données collectées sont :

Nom et prénoms, adresse, photo, empreintes digitales et autres informations relatives au titre de propriété foncière.

Lesdites informations sont recueillies directement auprès des personnes concernées.

L'APDP considère que les catégories de données objets du traitement sont adéquates, pertinentes et non excessives au regard des finalités poursuivies.

### *II-5. Durée de conservation des données collectées*

Aux termes des dispositions de l'article 383-6 de la loi no 2017-20 du 20 avril 2018, les données à caractère personnel collectées doivent être **«…Conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles elles sont traitée … »**

L'Autorité note que le Maire envisage de conserver les données collectées et traitées pour une durée illimitée.

Au regard de la finalité du traitement, l'APDP conclut que le caractère illimité de la durée de conservation desdites données à caractère personnel est justifié.

Elle rappelle toutefois que la conservation des données ne doit pas excéder la durée nécessaire à l'atteinte des finalités pour lesquelles elles sont collectées et traitées.

### *II-6. Traitement des données biométriques*

Le responsable du traitement justifie le recours à un système biométrique par la nécessité d'identifier de manière unique et sans équivoque les propriétaires et présumés propriétaires de parcelles de la Commune d'Abomey-Calavi.

Les données biométriques collectées sont les empreintes digitales. Elles sont collectées sur un (01) seul doigt (le pouce ou l'index ou le majeur) de la main droite.

L'Autorité estime qu'une telle collecte n'est pas excessive au regard de la finalité poursuivie.

### *II-7. Sous-traitance*

L'article 386 définit comme sous-traitant : « **Toute personne traitant des données à caractère personnel pour le compte du Responsable du traitement**… ».

Le requérant assurant lui-même le traitement déclaré avec l'appui technique de la Société SAM AY Sarl, l'Autorité considère au regard des éléments du dossier que, ce dernier n'est pas un sous-traitant au sens des dispositions de l'article suscité.

### *II-8. Sécurité*

#### ***Sécurité physique des locaux abritant les équipements***

Un protocole formalisé d'accès aux locaux et salles informatiques hébergeant les équipements de traitement et de sauvegarde des données collectées est envisagé par le requérant.

L'accès au bâtiment se fait par l'usage d'un verrou de sûreté. De plus, la sécurité des lieux est assurée par des gardiens.

L'Autorité fait remarquer que les dispositifs de sécurité d'accès au bâtiment abritant les équipements sont insuffisants, en raison du caractère sensible des données stockées.

Par conséquent, il est instamment demandé au requérant de renforcer le niveau de sécurité physique des locaux abritant les équipements de traitement des données collectées par la mise en œuvre d'un système d'accès numérique et de surveillance (vidéosurveillance).

- ***Sécurité logique des données***

L'étude du système mis en place révèle que des mesures adéquates et suffisantes sont prises pour assurer la sécurité et la confidentialité des données.

Au nombre de ces mesures, le requérant déclare avoir prévu le respect des principes de :

- authentification des systèmes (accès par mot de passe) ;
- confidentialité des données (privilège d'accès sur droit d'accord) ;
- intégrité (chiffrement des données).

L'Autorité en prend acte mais recommande au requérant d'utiliser des mots de passe de plus de huit (08) caractères comprenant, non seulement, des lettres mais aussi, des chiffres et des caractères spéciaux renouvelables selon la politique informatique de la structure.
Néanmoins, le requérant s'oblige à respecter toutes les mesures prévues par les dispositions de l'article 426 de la loi 2017-20 du 20 avril 2018.

**Par ces motifs,**

1. **enjoint au requérant d'avoir à :**

   - **tenir un registre (sous forme écrite ou électronique) des activités de traitement effectuées sous sa responsabilité, conformément aux dispositions de l'article 435 du code du numérique ;**

   - **produire à l'Autorité un rapport annuel des activités objets de la présente délibération, conformément aux dispositions de l'article 387 du code du numérique.**

2. **recommande au requérant de :**

   - **assurer également l'information préalable aux moyens des médias audiovisuels, notamment pour les personnes non-alphabétisées concernées par le traitement ;**

   - **prévoir pour les personnes concernées par le traitement, l'exercice du droit d'accès par une demande écrite datée, signée et adressée au Responsable du traitement ou à son représentant par voie postale ou électronique, conformément aux dispositions de l'article 437 alinéa 2 du code du numérique ;**

- **respecter le délai de réponse aux requêtes des personnes concernées par le traitement dans l'exercice de leurs différents droits, conformément aux dispositions des articles 437, 440 et 441 de la loi 2017-20 du 20 avril 2018 portant du code du numérique en République du Bénin.**

3. **rappelle que :**

   - **le traitement exécuté ne saurait être détourné des finalités déclarées ;**

   - **la responsabilité du requérant est engagée, en cas de manquement aux dispositions du Livre Ve du code du numérique.**

**Sous réserve de ce qui précède,**

**Le Maire de la Commune d'Abomey-Calavi est autorisé à mettre en œuvre le traitement des données visé dans la présente délibération.**

**Conformément aux dispositions des articles 462 et 489 de la loi portant code du numérique en République du Bénin, l'APDP se réserve le droit de procéder à des contrôles ultérieurs aux fins de s'assurer du respect par le requérant des termes et conditions de la présente délibération.**

Le Président,


**Etienne Marie FIFATIN**

**AUTORITE DE PROTECTION DES DONNEES A CARACTERE PERSONNEL**

Rue 6.076 « Immeuble El MARZOUK Joël »

Tel : (+229) 21 32 57 88 / 69 55 00 00
01 BP : 04837 Cotonou
Email: contact@apdp.bj
https://www.apdp.bj

**Prévu par l'article 481 de la loi n°2017-20 du 20 avril 2018 portant code du numérique en République du Bénin.**

Rue 6.076 « Aïdjèdo, Immeuble El MARZOUK Joël »
COTONOU

Tél. 21 32 57 88 / 69 55 00 00
01 BP : 04837
Site web : https://www.apdp.bj
Email : contact@apdp.bj