MASTERE SPECIALISE REGULATION

DES CONTENUS NUMERIQUES

Promotion 2014 - 2016

DONNEES A CARACTERE PERSONNEL ET COMMUNICATIONS ELECTRONIQUES EN MAURITANIE :

UNE REGULATION PAR L'AUTORITE DE REGULATION MULTISECTORIELLE (ARE) OU PAR UNE AUTORITE ADMINISTRATIVE INDEPENDANTE (AAI) A CREER ?

Mamadou Alpha KANE

Conseiller Juridique auprès du
Conseil National de Régulation
De l'Autorité de Régulation Multisectorielle
De Mauritanie (ARE)

DONNEES A CARACTERE PERSONNEL ET COMMUNICATIONS ELECTRONIQUES EN MAURITANIE :

UNE REGULATION PAR L'AUTORITE DE REGULATION MULTISECTORIELLE (ARE) OU PAR UNE AUTORITE ADMINISTRATIVE INDEPENDANTE (AAI) A CREER ?

Mamadou Alpha KANE
Conseiller Juridique auprès du
Conseil National de Régulation
De l'Autorité de Régulation Multisectorielle
De Mauritanie (ARE)

- Juin 2016 -

« L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques »

- Article Loi n° 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifiée par la Loi N ° 2004-801 du 06 Août 2004) –

« Je ne connais pas d'être vivant, de cellule, tissu, organe, individu et peut être même espèce, dont on ne puisse pas dire qu'il stocke de l'information, qu'il traite de l'information, qu'il émet et qu'il reçoit de l'information »

- Michel Serres -

Lauréat de l'Ecole Normale Supérieure,

Agrégé en philosophe post-moderne,

Diplômé en études navales, mathématiques, communications, numérique, politique et écologie,

Historien des sciences et homme de lettres français,

Elu à l'Académie Française le 29 mars 1990

_____

DEDICACE

Je dédie cette thèse professionnelle à **mon Père Amadou Yaya KANE** alias **Amadou Kouro**, brillant Ingénieur en Télécommunications de son époque et Homme d'une extraordinaire qualité, malheureusement ravi, à la fleur de l'âge, à l'affection des siens.

J'aurais aimé, à mon arrivée dans le « monde des télécoms », avoir la chance que tu me prennes par la main et me guides, pas à pas !

J'aurais aimé, également, te remercier pour cela et pour tout le bien que tu as fait autour de toi !

La Mauritanie, en tout cas, te doit la reconnaissance de sa Nation toute entière pour avoir, avec les deux autres avec qui tu as formé le trio des premiers ingénieurs de télécommunications de toute l'Afrique, mis sur pied ce qui est devenu, bien longtemps après toi, MAURIPOST.

QU'ALLAH T'AIE EN SA MISERICORDE !

Je le dédie également à Bouna KANE, parce qu'il aurait aimé lire la dédicace faite à son petit frère.

QU'ALLAH T'ACCORDE TOUTE LA FELICITE POSSIBLE !

Mamadou Alpha Bouna KANE

Remerciements

A l'achèvement de la passionnante formation ayant occasionné la rédaction de la présente thèse professionnelle, mes plus sincères remerciements vont :

A l'Autorité de Régulation Multisectorielle (ARE) de Mauritanie, mon employeur, qui a eu l'extrême générosité de prendre en charge tous les frais afférents à cette formation et de prendre toutes les dispositions utiles pour me permettre de participer à toutes les sessions académiques dans d'excellentes conditions ; Merci aux quatre (4) présidents de l'institution aux Membres du Conseil National de Régulation, dont j'ai eu l'honneur et le privilège d'être le collaborateur, ainsi qu' à tout le personnel, qui m'ont tous soutenu,

A Monsieur Le Professeur Laurent Gille, le coordinateur et responsable pédagogique du Mastère, qui a été d'un apport et d'une disponibilité sans faille sur tous les plans ; Qu'il soit mon interprète auprès de Patricia Dumy, sa dévouée assistante administrative, Coco et Fatou, du restaurant administratif de TELECOM PARISTECH, qui ont agrémenté du mieux qu'ils ont pu nos séjours d'une touche typiquement « afro »,

A Monsieur Mathurin BAKO, le Président de l'ARCEP du Burkina Faso, qui force l'estime et l'admiration par sa grandeur d'esprit qui n'a d'égales que sa simplicité et son haut sens de la chaleur humaine ; Merci à lui, à l'éminent délégué Sanou Soumanan et à l'adorable Habiba Carole KANMUNI du service international pour la qualité jamais démentie de leur accueil,

A mes familles de Montreuil (Bouna Junior, Fati, Tonton beurre), de Gagny (Saidou « Ninyme » et Sala », de Villeneuve Saint Georges (La famille NIANG) et de Ouagadougou (Famille SAMAKE Adama de la Zone du Bois),

A celle et ceux qui ont pu légitimement se sentir, par moments, « délaissés » par moi, durant la longue période de rédaction du présent mémoire, pour leur compréhension et leur patience.

Et à Bouna et Haby, pour tout le bonheur qu'ils m'apportent, en attendant l'arrivée de leurs petits frères et sœurs, INCHAALLAH (!). /.

Mamadou Alpha KANE

Avertissement

Ce mémoire constitue le travail de fin d'études du Mastère Spécialisé en Régulation du Numérique délivré par TELECOM ParisTech, dans le cadre d'une formation organisée conjointement par TELECOM ParisTech, l'Arcep du Burkina Faso, l'Arcep de France et l'ANFR de France dans le cadre du réseau Fratel.

TELECOM ParisTech et les coorganisateurs de cette formation n'entendent donner aucune approbation ni improbation aux opinions émises dans ce mémoire: ces opinions doivent être considérées comme propres à leurs auteurs.

SOMMAIRE

PROBLEMATIQUE GENERALE

L'une des manifestations les plus tangibles de la vie en société, voire, tout simplement de la vie en communauté, réside dans le fait que, pour aspirer à un minimum d'affirmation de soi, de reconnaissance par ses semblables et d'épanouissement de quelque nature qu'il soit, tout individu est confronté à une savante et harmonieuse répartition de son temps, de ses activités et éventuellement de ses loisirs en deux (2) dimensions qui coexistent de manière complémentaire mais ne sont pas toujours conciliables ni équilibrées, l'une pouvant indifféremment, au gré des circonstances, empiéter sur les limites de l'autre. Il s'agit :

- de sa vie publique, dictée et fortement conditionnée par les contraintes inhérentes aux interactions de divers ordres, qu'il est forcément amené à avoir avec son environnement (Administration Centrale, Etat Civil, obligations professionnelles, mouvements politiques, associatifs ou tout simplement vie sur les réseaux sociaux) ;

- et de sa sphère privée ou intime, que soit, personne ne doit avoir le droit ni la moindre raison de « violer », du simple fait que cette dimension n'est pas censée intéresser le reste des membres de sa communauté, soit, il choisit expressément, pour une raison ou une autre qu'il n'a d'ailleurs pas à justifier, de soustraire à la connaissance du public (affaires familiales, conjugales, vie sexuelle, informations d'ordre médical, religieux ou philosophique, pour ne citer que cela).

C'est ainsi que toute personne, que ce soit dans le cadre de l'exercice de ses droits, devoirs ou obligations, que dans celui de sa vie privée, peut échanger, interagir, commercer et poser des actes de tous ordres tout en choisissant à son entière guise – dans la majorité des cas, en tout cas – de le faire :

- de manière directe, c'est-à-dire physiquement et sans interface quelconque ;

- de manière virtuelle, mais sans avoir à décliner son identité ou d'autres données qui lui sont propres (c'est le cas des inscriptions sur les réseaux sociaux et des participations à des forums ou sites de rencontres anonymes) ;

- de manière réelle, en déclinant ou non les informations qui lui sont intrinsèques, mais en utilisant toutes les commodités (et parfois inconvénients ou contraintes) des interfaces et supports qu'offrent aujourd'hui les progrès de l'informatique, en général et du numérique, en particulier.

Mais quel que soit le choix opéré, un fait est constant et certain, c'est que tous les échanges, conversations et actes réalisés de l'une des trois (3) façons précitées ont ceci de commun que non seulement ils constituent des sources d'informations intarissables mais que, surtout, ils laissent tous des traces, des preuves et des historiques de leur accomplissement,

éléments qui peuvent, par conséquent, faire l'objet de traçages, de reconstitutions, d'archivages et / ou d'exploitations à bon ou mauvais escient.

Ce constat, que l'on peut qualifier de triste ou d'heureux, en fonction des enjeux des informations ci-dessus évoquées et des intérêts antagonistes qu'elles peuvent présenter pour les personnes auxquelles elles se rapportent et pour celles qui, pour diverses raisons, peuvent être amenées à les exploiter, n'est spécifique ni à un espace géographique déterminé ni à une société donnée ; c'est un fait universel qui interpelle les citoyens et pouvoirs publics du monde entier, surtout si l'on sait que les informations, qui constituent de nos jours la première ressource d'une nouvelle forme d'économie planétaire qui se met en place, sont aussi sujettes que les individus qu'elles concernent aux flux transfrontaliers (échanges entre ressortissants et / ou administrations de pays différents par internet, téléphone, fax ou correspondances sur supports papiers).

Aujourd'hui que la Mauritanie est à la croisée des chemins de la révolution « du mobile » et de son inévitable corollaire, l'avènement du « numérique », qui y fait ses premiers pas et alors qu'au même moment, son Administration essaie de relever le pari de son informatisation à grande échelle - projet de mise en place d'équipements et de procédures de certifications de signatures électroniques, notamment - plusieurs questions peuvent, voire doivent se poser à ses pouvoirs publics et interpeller la masse de ses citoyens avertis :

- quant à non seulement la sécurité des divers supports informatiques et ce qu'il convient d'appeler la « liberté informatique » des individus, en général ;

- mais aussi et surtout, de façon plus pointue, quant à la protection des données à caractère personnel de ces derniers, de plus en plus produites, acheminées, exploitées, conservées ou détruites au moyen des supports évoqués plus haut.

Le gouvernement mauritanien, en effet, vient de poser les bases légales appelées à régir la sphère « des relations électroniques » que ses citoyens peuvent être amenés à entretenir, qu'il a dénommée « Société Mauritanienne de l'Information » (SMI), à travers les quatre (4) textes de lois suivants, dont les deux (2) premiers, seulement, ont été promulgués à ce jour, les deux (2) autres restants étant encore en attente d'être adoptés par les chambres parlementaires.

Il s'agit d'une loi d'orientation, qui délimite le cadre général et les principes directeurs de cette cyber-société, d'une loi sur la cybercriminalité, d'un projet de loi sur les transactions électroniques et d'un projet de loi sur la protection des données à caractère personnel.

- La Loi N ° 2016-006 du 20 janvier 2016, portant Loi d'Orientation de la Société Mauritanienne de l'Information (SMI), vise à mettre en place les bases juridiques et institutionnelles pouvant permettre l'intégration du pays au processus de mondialisation, auquel il ne peut échapper, par la création d'un environnement propice au développement

des technologies de l'information et de la communication (TICs), pour une meilleure inclusion effective de ses citoyens dans les échanges mondiaux.
Il faut noter qu'il s'agit d'une loi-cadre dont la principale finalité réside dans la cohérence de l'ensemble du dispositif juridique composé des normes spécifiques à chaque type de composante ou activité « TIC », que l'Etat entend règlementer de manière séparée et plus approfondie ;

- La Loi N ° 2016-007 du 20 janvier 2016, relative à la Cybercriminalité, se fixe pour but de définir et sanctionner les « nouveaux faits et comportements répréhensibles » qui seront, inéluctablement, engendrés par l'utilisation des nouveaux moyens d'échanges d'informations et de communications.

Il porte donc sur tous les crimes et délits pouvant être commis à l'aide des technologies de l'information et de la communication ;

- Le projet de Loi sur les transactions électroniques traduit fortement le constat, qui a été fait que si, durant les deux (2) dernières décennies, seuls les banques, hommes d'affaires, commerçants et quelques rares privilégiés faisaient usage des outils électroniques dans le cadre de leurs professions et activités respectives, il en va autrement aujourd'hui car de plus en plus de citoyens, de ménages et d'agents économiques, de milieux, activités et profils des plus variés, pour ne pas dire tout le monde, n'effectuent plus leurs diverses transactions (e-commerce) et formalités administratives (demandes, déclarations auprès de certaines administrations et ambassades) qu'au moyen de supports, voies et instruments de de traitements et paiements électroniques. Ce texte consacre d'ores et déjà sept (7) innovations importantes dans le corpus légal mauritanien, que sont :

- la prise en compte, comme moyen de preuve, de l'écrit électronique et de la signature électronique, au même titre que l'écrit sur support papier ;

- la création d'une autorité de certification, aux fins de sécuriser les transactions électroniques ;

- les règles de détermination de la responsabilité du commerçant électronique ;

- l'interdiction de la publicité non sollicitée par messagerie électronique ;

- les règles de détermination de la responsabilité des différents acteurs concernés par les transactions électroniques, en distinguant, d'un côté, les prestataires techniques que sont les opérateurs de communications électroniques et les hébergeurs de contenus et, de l'autre, les éditeurs de services de communication au public en ligne ;

- la protection du cyberconsommateur par l'encadrement de la publicité par voie électronique ;

- et, enfin, la dématérialisation des formalités et procédures administratives.

- Le projet de Loi sur la protection des données à caractère personnel, pour finir, qui, tel que l'indique son libellé, traite de toutes les données liées à la dimension privée de la vie des citoyens, en vue de protéger ces derniers contre toutes sortes d'atteintes aux éléments qui sont, de par leur nature, leurs manifestations et leurs conséquences, intimement, strictement et exclusivement rattachés à leurs personnes.

Ce projet de loi, encore au stade de discussion au niveau des chambres parlementaires au moment où nous tentons de nous livrer à la présente réflexion, constitue le fil directeur des développements autour desquels elle s'articulera, étant donné qu'au moins un aspect nous semble ici mériter la plus grande attention : La désignation et les critères objectifs de qualification, de fonctionnement et d'attribution de prérogatives de l'entité à laquelle ou, en cas de compétences partagées, des organes auxquels sera confiée la lourde responsabilité de la régulation des données à caractère personnel.

_____

INTRODUCTION

Le choix de l'intitulé du sujet dont nous venons de succinctement tenter de dégager la problématique, ci-dessus, n'est pas fortuit.

Nous avons choisi ce thème de réflexion parce que, d'abord, les données personnelles se situent, de notre point de vue, au croisement des systèmes électroniques, qu'elles mettent de plus en plus en jeu et, d'au moins, l'une des missions les plus basiques des régulateurs traditionnels, à savoir la régulation des infrastructures et canaux de transmission des différents types d'informations, ne serait-ce que parce que lesdites informations (voix, sons, images, texte, data) empruntent le plus souvent, pour des raisons pratiques, des équipements et technologies faisant partie d'un ensemble, d'une activité plus large sujette, elle, à une certaine normalisation (régulation des opérateurs de communications électroniques).

Le choix de ce sujet s'explique également par le fait que :

- D'un côté, l'on peut être tenté de déduire de certaines compétences octroyées par la Loi aux autorités de régulations traditionnelles (ARN) - en matière de droits et protection des utilisateurs de réseaux et services de communications électroniques - et du capital

expérimental que ces dernières ont acquis, qu'il revient naturellement à ces institutions de « rajouter à leur arc la corde des données à caractère personnel » ;

- Et, de l'autre, il faille se rendre à l'évidence qu'avec les perpétuelles avancées des droits et libertés individuels, il n'est pas forcément aisé à des autorités de régulation de communications électroniques « de type classique » d'arriver à concilier des enjeux et problématiques aussi variés que ceux qui sont inhérents aux secteurs industriels, donc commerciaux, qu'ils ont historiquement toujours régulés (télécommunications, poste, eau et électricité, pour citer le cas de la Mauritanie) avec les enjeux et problématiques, aussi complexes les uns que les autres, qui tournent, non autour des services dispensés à la population, mais autour de la protection d' intérêts exclusivement liés à l'intimité des citoyens, à moins que ne soit, au préalable, opérés de grands bouleversements organisationnels des institutions impliquées.

Il faut cependant noter, dans cet ordre d'idées, que même si à priori nous n'avons eu écho qu'une telle pratique avait cours dans une partie donnée du monde, nous nous sommes posé la question de savoir s'il n'existait pas une option intermédiaire, consistant à ce que les pouvoirs publics mauritaniens décident que les questions de régulation des données à caractère personnel relèvent d'un organe ad hoc qui ne siègerait qu'au cas par cas.

Mais avant d'aborder une à une ces différentes pistes, il ne nous semble pas inutile, au préalable, de revenir sur le concept clé de « données à caractère personnel », de manière à essayer de mettre en évidence, d'une part, toutes les corrélations possibles entre ces données, qui ne sont pas toujours forcément électroniques en elles-mêmes et les communications électroniques dont les opérateurs assurent le service et, d'autre part, le périmètre des différentes interactions possibles entre ces derniers, les régulateurs de communications électroniques, les autorités administratives indépendantes exclusivement dédiées à la protection des données à caractère personnel et éventuellement certains services de l'Etat intéressés par ces questions.

De la synthèse des lectures croisées des législations des pays qui ont servi de base comparative[1] à ce travail, il ressort que dans tous ces pays, la Loi répute constituer une donnée à caractère personnel toute information relative à une personne physique identifiée ou identifiable, de manière directe ou indirecte, par la seule référence à un numéro d'identification ou à un plusieurs éléments qui lui sont propres, étant bien compris que l'identité à laquelle font allusion les textes de lois en question peut s'entendre de l'identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.

A cette définition, assez extensive, il faut apporter une précision importante : Une donnée à caractère personnel peut être soit « ordinaire » ou « banale », à l'image du nom d'une personne, ce qui n'amoindrit cependant en rien son caractère personnel, mais l'on retrouve également, dans le vaste océan des données à caractère personnel celles qui revêtent un caractère « sensible », désignées à juste titre par l'appellation « données sensibles » ; c'est le cas des données faisant état, par exemple, des origines raciales ou ethniques, des opinions politiques, philosophiques ou religieuses, de l'état de santé ou de la vie sexuelle des personnes.

Ensuite faut-il rappeler que les données personnelles, qui sont présentes partout, sous forme d'énormes répertoires et sont, à juste titre, qualifiées par Mme Meglena Kuneva[2], déjà en 2009, de «nouveau pétrole de l'internet » et de « nouvelle monnaie du monde numérique", constituent de grands enjeux car elles présentent certaines caractéristiques et peuvent faire l'objet de toutes sortes de manipulations très variées par divers acteurs.

Du point de vue des caractéristiques, ce n'est certainement pas un hasard si la donnée se trouve aujourd'hui au cœur du numérique car, comme l'explique M. Laurent GILLE[3], la valeur d'une information, donc celle de la donnée qui la matérialise, la renferme ou dont on peut la déduire, se fonde, entre autres éléments, qu'il a développés, mais qui ne nous paraissent pas directement liés à l'aspect personnel qui nous intéressent, sur :

- son origine, sa signature ;
- sa propriété, sa détention, sa protection, sa confidentialité ;
- sa recherche, son accès, sa facilité de traitement ;
- et son utilisation, sa portée, ses usages

Les manipulations pouvant porter sur les données personnelles portent la qualification légale de « traitement » - nous y reviendrons dans le corps du document, en précisant les dispositions légales qui les règlementent – et comprennent toutes celles qui consistent en

[1] Législations mauritanienne, burkinabè, sénégalaise, ivoirienne et française traitant des données personnelles (Voir extraits des textes pertinents au niveau des parties du document relatives au contexte mondial et au contexte mauritanien).
[2] Commissaire Européenne à la consommation, en 2009.
[3] Professeur d'Economie à Télécom ParisTech, « La donnée au cœur du numérique : Questions », page 23.

une opération quelconque sur lesdites données, que cette opération se fasse manuellement ou de manière automatisée. Elles vont, ainsi, de la simple collecte à l'effacement ou la pure destruction d'une donnée, en passant par sa consultation, sa communication ou sa modification.
A noter que dans la plupart des cas, les traitements de données personnelles ou les données nouvelles qui peuvent en résulter se font ou sont transcrits sur des fichiers, créés sur supports papiers, informatiques ou numériques, sachant que constitue un fichier (voir développements infra) tout « ensemble structuré et stable de données à caractère personnel, accessible selon des critères déterminés ».

Quant aux acteurs pouvant être impliqués à un niveau ou l'autre de tout processus tournant autour des données personnel, ce sont :

- Le responsable de traitement, qui est la personne physique ou morale (autorité publique, organisme ou service) qui détermine les finalités (raisons justifiant le traitement) et les moyens utilisés ;
- Le sous-traitant : toute personne physique ou morale traitant des données à caractère personnel pour le compte du responsable du traitement. Le sous-traitant :
- agit sous l'autorité et les instructions du responsable de traitement
- doit apporter des garanties suffisantes
- La personne concernée, c'est-à-dire celle à qui se rapportent des données à considérer ;
- Le destinataire : Il s'agit de la personne physique ou morale qui reçoit les données ;
- Eventuellement[4] le Correspondant Informatique et Liberté (CIL), personne physique jouant le rôle de l'Autorité de protection des données à caractère personnel, qui appartient à la structure du responsable de traitement et s'assure que les procédures, droits et obligations relatifs aux données personnelles sont scrupuleusement respectés ;
- Et, enfin, l'institution, la commission ou l'organe chargé, au sein de chaque pays doté d'une loi spécifique au domaine, de la protection des données personnelles.

Pour mieux appréhender les questions essentielles formant la pierre angulaire et les différentes déclinaisons des données à caractère personnel, nous nous proposons, dans une première partie de faire un survol préliminaire de l'état de l'encadrement de cette dimension intuitu personae dans le contexte mondial, en faisant une brève comparaison des systèmes mis en mis en place en Europe et Afrique (I), comparaison qui devrait pouvoir nous renseigner sur la tendance générale à « réguler » les services pouvant « acheminer » des données personnelles eux-mêmes (voix, images, vidéos, signes, texte, datas) ou à ne réguler que les opérateurs mettant ces services à la disposition du public et les autres acteurs qui pourraient éventuellement être impliqués dans « les flux de données personnelles » (II).

[4] Eventuellement le CIL car ce ne sont pas toutes les législations qui mettent en place cet organe.

La deuxième partie, entièrement consacrée au contexte mauritanien, traitera des mécanismes mis en place par les textes de lois et de leur « moins évidente » application effective dans le contexte socio-culturel local (I), puis tentera de mettre à jour les interférences et conflits de compétences ou d'autorités qui, à notre avis, seront inévitables, non seulement du fait d'un défaut d'anticipation, au moment où ont été légiférés certains textes portant sur l'Autorité de Régulation Multisectorielle (ARE), relativement à la protection des usagers et utilisateurs de services, mais aussi parce qu'ultérieurement à la création de l'ARE mais antérieurement à la décision du Gouvernement de se nantir d'une loi sur la protection des données personnelles, une structure étatique dotée de « super pouvoirs », à notre sens, plus intrusifs que de raison, est venue enrichir le paysage administratif mauritanien (II)[5]. /.

---

[5] Il est d'usage que la rédaction de tout ouvrage scientifique, en général, ou de tout ouvrage académique, en particulier, respecte certaines normes de présentation, relatives, notamment, au format du corps de texte qui en forme le contenu. Il en va ainsi de la proportion des différentes parties traitées, qui doivent être équilibrées autant que faire se peut. Dans le cas présent, compte tenu de l'importance des éléments développés dans notre première partie, dont « l'amputation » viderait considérablement le sujet de son intérêt, et de la réalité du cadre d'étude de la deuxième partie, qui offre beaucoup moins de « matière », il serait possible que le deuxième volet de cette thèse professionnelle soit malencontreusement moins fourni que le premier ; nous l'assumons mais nous en excusons tout de même sincèrement. /.

PREMIERE PARTIE – LE CONTEXTE MONDIAL

Cette première partie aurait pu s'intituler tout simplement « Le contexte occidental », non parce que seul l'occident est concerné par les différentes problématiques des données à caractère personnel, loin s'en faut, mais pour les deux (2) principales raisons suivantes :

- D'abord, parce que les gouvernements des pays en voie de développement, surtout préoccupés de réduire le fossé économique et technologique entre leurs pays et les pays développés, ont légitimement pu être contraints, jusqu'à une époque très récente, de se focaliser sur d'autres « priorités » que la protection des données à caractère personnelles ;

- Ensuite, parce c'est l'Occident qui, le premier, a été « bénéficiaire » ou « victime » d'une numérisation aussi rapide qu'incontrôlable des différentes sociétés qui le composent, cette numérisation ayant complètement chamboulé, entre autres éléments, les pratiques sociales, donc, forcément les libertés publiques, ce qui explique que depuis plusieurs décennies s'est posée la question du statut et de l'avenir de la vie privée dans ce monde numérique qui n'arrête pas de repousser les limites de ses frontières (passage d'une informatique structurelle ou administrative à une informatique « privée individuelle » et, dans le même temps, à une informatique « publique de réseaux ».

Mais vu que le propre des données, quel que soit le caractère qu'elles peuvent revêtir (public ou personnel), est que non seulement elles ne subissent plus les contraintes de la moindre fixation géographique mais elles viennent - à l'image d'un ruisseau qui alimente une rivière, cette rivière se déversant dans un fleuve et ce dernier se jetant dans la mer - alimenter l'océan infini des BIG DATA, qui ne connaît ni frontières, ni cycles horaires, c'est à dessein que nous maintiendrons donc le libellé « mondial » qui illustre, on ne peut mieux les flux de données pouvant échapper à tout espace, toute autorité étatique et même à leurs auteurs.

I – Encadrement par les ARN traditionnelles ou par des AAI indépendantes à créer? (ELEMENTS FACTUELS ET DE DROIT COMPARE)

Il n'est pas aisé de répondre à la question de savoir s'il est préférable que les données à caractère personnel soient régulées par les autorités de régulation classiques, en l'occurrence les régulateurs de communications électroniques ou par des autorités administratives indépendantes à créer, chaque Etat déterminant souverainement sa politique de libertés publiques et individuelles, d'un côté et chaque peuple, chaque société, chaque communauté partageant, parmi tant d'autres, certaines valeurs indéfectibles qui leur sont communes et plus précieuses que tout.
C'est la raison pour laquelle, à défaut de pouvoir trouver une réponse tranchée toute trouvée à notre préoccupation, nous nous livrerons, dans un souci de contenance pratique, à une comparaison factuelle et juridico-légale des systèmes de protection des données

personnelles tels qu'ils sont mis en place en Europe et tels qu'ils commencent à être adaptés en Afrique. Peut-être se dégagera-t-il ainsi une piste à privilégier sur l'autre ou peut-être, tout simplement, que la confrontation des différents systèmes révèlera des failles susceptibles de nous inspirer une autre approche de régulation, voire une solution intermédiaire.

A. L'Europe & les DP

1. Les textes européens : Actes législatifs

Les institutions européennes ayant vocation à produire des textes sont :

• **La Commission Européenne**, dont dépend une direction générale spécialement chargée, entre autres, pour ce qui touche à notre sujet :

- de la règlementation du secteur des communications électroniques ;
- de la promotion des biens et services numériques et de leur diffusion dans la société ;
- de l'internet et sa chaine de valeur.

C'est la Commission, qui dès 2010, a adopté la fameuse « Stratégie Numérique pour l'Europe » assise sur un plan d'exécution quinquennal.

• **Le Conseil**, au sein duquel siègent les ministres chargés du secteur des communications électroniques de chaque Etat Membre et qui a été le théâtre, au mois d'octobre 2013, de la première réunion des chefs d'Etats consacrée au numérique.

• **Le Parlement**, enfin, composé des représentants de tous les Etats membres au prorata de l'importance de leurs populations respectives.
Il comprend deux (2) commissions chargées de questions cruciales pour le monde des communications électroniques, à savoir :

- ITRE : Commission de l'industrie, de la recherche et de l'énergie (Committee on Industry, Telecoms, Research & Energy) ;
- IMCO: Commission chargée du Marché Intérieur et de la protection du consommateur (Internal Market and Consumer Protection).

La régulation du secteur des communications électroniques est organisée, à l'échelle européenne (à l'instar de l'encadrement de tous les autres domaines et activités relevant de la règlementation communautaire) autour de quatre catégories de textes supranationaux :

Les règlements, les directives, les décisions et les recommandations et avis.

Pour rappel, ces instruments, qui peuvent porter sur les mêmes contenus, thématiques et objectifs, ne se différencient que par leurs portées et degrés de forces contraignantes respectifs.

Le règlement, ainsi, a une portée générale, est obligatoire dans toutes ses dispositions et est directement applicable, donc sans transposition préalable, dans chaque Etat Membre de l'Union Européenne, exactement à l'image d'une loi, au niveau national.

La directive, elle, lie également tous les Etats Membres de l'Union Européenne concernés par son contenu, à ceci près que sa finalité est de parvenir un résultat précis sur une thématique donnée au niveau des états qu'elle vise; c'est la raison pour laquelle il est laissé à chaque Etat le soin, la compétence et la liberté de choisir librement ses propres formes et outils de transposition de ladite directive dans son dispositif national légal ou règlementaire.

La décision, de son côté, est une norme obligatoire dans tout son contenu, comme le règlement, à la différence qu'elle n'a pas de portée étendue; elle n'a d'effet que vis-à-vis des Etats destinataires qu'elle désigne nommément.

Quant aux recommandations et avis, ce sont des normes, qui, tel que le laissent déduire leurs intitulés, n'ont aucune force contraignante à l'égard des Etats auxquels ils s'adressent.

Une fois ce rappel fait, les principaux textes européens voués à l'encadrement des données à caractère personnel, sont, chronologiquement :

- **Dès 1995** : ***La Directive sur la Protection des données personnelles*** ; il s'agit d'une directive multisectorielle applicables aux acteurs / opérateurs de tous les domaines d'activités.

- **En 2002** : ***La Directive « Vie privée et communications électroniques »*** ; Elle vient poser des règles pour régir le traitement des données à caractère personnel dans le cadre des services de communications électroniques, à l'exception des contenus audiovisuels et du commerce électronique. Elle vise donc les opérateurs de communications auxquels elle impose :

- une totale confidentialité des communications et des données associées ;
- des conditions strictes pour le traitement des données de trafic et des données de localisation des utilisateurs de mobiles ;
- un droit à une facturation détaillée et la liberté de paraître ou non dans les annuaires ;
- des mesures sur l'affichage des numéros des lignes appelantes ;
- des mesures sur le traitement des communications non sollicitées.

- **En 2006** : ***La Directive « Conservation des Données de Trafic et de Localisation »***

Cette directive fait obligation aux opérateurs d'effacer les données de trafic et de localisation de leurs abonnés, sauf pour « des intérêts légitimes » tels que la lutte contre le terrorisme et des questions de sécurité nationale, par exemple.
Elle introduit, par contre, une obligation de conservation des données autres que celles de trafic et de localisation pour la téléphonie fixe et mobile et l'accès Internet, avec un

minimum de 6 mois et un maximum de 2 ans, mais introduit en même temps, fort heureusement, des mesures de protection et de sécurité des données.

- **En 2012**, enfin, ***Le Projet de Règlement européen sur la Protection des données personnelles***, abrogeant et remplaçant la Directive de 1995.

Ce projet de règlement, qui constitue une révision du cadre juridique instauré dix-sept (17) ans plus tôt, a largement été suscité par l'accroissement continu des services en ligne observé à l'époque ; Il avait pour objectifs essentiels :

- Le renforcement du droit de contrôle accordé aux résidents européens sur leurs données personnelles ;
- Le renforcement des obligations de tous les organismes traitant des données personnelles, qu'ils soient privés ou publics.

N.B. : Une date mérite d'être notée : 2009 ; il s'agit de l'année qui a vu la naissance de l'ORECE (Organe des Régulateurs Européens des Communications Electroniques), créé par le règlement 1211/2009.

2. Principes fondamentaux découlant de la législation européenne

Avertissement préliminaire (!) :

Pour toute la suite de cette partie qui présente la manière dont est mise en œuvre la protection des données à caractère personnel de manière concrète en Europe, nous nous appuierons uniquement sur la législation française qui nous servira non seulement de base justificative que d'élément d'illustrations, par souci de commodité.

Cette assimilation, voire cette confusion volontaire des textes communautaires avec les textes européens peut choquer tout observateur puriste - nous nous en excusons – mais nous sommes d'avis qu'à défaut de « tomber sous le sens », elle peut procéder d'un certain bon sens, étant donné que :

- Primo : L'une des raisons principales de la création de l'espace européen est justement la production d'un cadre légal et juridique harmonisé ; la norme française ne saurait donc contredire la règle communautaire ;
- Secundo : Non seulement la France est une nation pionnière et référence incontestable en matière de droits individuels et libertés publiques, mais c'est le pays dont la culture juridique est la plus proche de celle des pays africains francophones, notamment du droit mauritanien qui ne présente de particularités notoires que dans certains domaines fortement marqués par l'emprunte du FIQH[6] (Statut personnel, droit de la famille).

[6] FIQH désigne le droit musulman, principalement découlant de la CHARI-A (LOI ISLAMIQUE)

Les termes « Loi française » et « législation européenne » seront donc indistinctement utilisés l'un pour l'autre, pour désigner la substance des mêmes règles.

_____

Trois (3) principes fondamentaux découlent des textes européens relatifs à la protection des données personnelles : le principe de légalité, le principe de finalité et le principe de proportionnalité.

a – Le principe de légalité

La légalité étant le caractère de ce qui est légal, donc conforme au droit, aucun traitement sur une donnée personnelle ne saurait transgresser la Loi qui s'y applique.
En d'autres termes, pour qu'un traitement soit possible, il doit, d'abord avoir été défini (voir par une Loi qui en précise les modalités d'exécution.

Or que qualifie la législation européenne de traitement ?
La réponse nous est donnée par l'article 2, alinéa 3 de la Loi N ° 78-17 du 6 janvier 1978 relative à l'Informatique, aux Fichiers et aux Libertés[7] (Modifié par Loi n°2004801 du 6 août 2004 art. 1 JORF 7 août 2004).

Au terme de cet article, « Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou L'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

Relativement aux procédés légalement autorisés pour opérer un traitement, l'article 6, 1° de la même loi (Modifié par la LOI n°2016-41 du 26 janvier 2016 art. 193), nous enseigne qu'un traitement ne peut porter que sur des données à caractère personnel que si « Les données sont collectées et traitées de manière loyale et licite ».

La combinaison des articles 2, alinéa 3 et 6, 1° nous édifie donc sur le caractère légal du traitement des données, sous réserves, bien entendu, des conditions exclusives mentionnées ci-dessus.

b – Le principe de finalité

[7] Pour la suite, Loi « I & L » désignera la Loi N ° N ° 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Il découle de l'article Article 6, 2° de la Loi « I & L » (Modifié par la LOI n° 2016-41 du 26 janvier 2016 art. 193), qui dispose que les données à caractère personnelles « sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités » mais que « Toutefois, un traitement ultérieur de données à des fins statistiques ou à des fins de recherche scientifique ou historique est considéré comme compatible avec les finalités initiales de la collecte des données, s'il est réalisé dans le respect des principes et des procédures prévus au présent chapitre, au chapitre IV et à la section 1 du chapitre V ainsi qu'au chapitre IX et s'il n'est pas utilisé pour prendre des décisions à l'égard des personnes concernées ».

En guise d'illustration, « les informations collectées dans le cadre de la gestion locative ne doivent pas être réutilisées à d'autres fins, sans que les personnes concernées en aient été informées et mises en mesure de s'y opposer »[8].

c – Le principe de proportionnalité

Ce principe est mis en évidence par l'article 6, 3° de la Loi « I & L » (Modifié par la LOI n° 2016-41 du 26 janvier 2016 art. 193), qui énonce qu'un traitement ne peut porter sur des données personnelles que si ces données sont « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ».

Remarque importante: Un traitement ne peut porter sur des données à caractère personnel s'il n'a, au préalable, reçu le consentement de la personne concernée, sauf si sa finalité est constituée par l'une des situations suivantes :

- Le respect d'une obligation légale incombant au responsable du traitement ;
- La sauvegarde de la vie de la personne concernée ;
- L'exécution d'une mission de service public dont est investi le responsable ou le destinataire du traitement ;
- L'exécution, soit d'un contrat auquel la personne concernée est partie, soit de mesures précontractuelles prises à la demande de celle-ci ;
- La réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le destinataire, sous réserve de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée. (Article 7 Loi « I & L » Modifié par Loi n°2004-801 du 6 août 2004 art. 2 JORF 7 août 2004).

[8] Me Frédéric Forster, Cabinet ALAIN BENSOUSSAN AVOCATS, « La Protection de la Vie Numérique », page 26.

3. Matérialisation et conséquences des règlements et directives européens

Le champ d'application matériel des textes européens (cf. Point précédent) englobe tous les traitements, automatisés (via des supports informatiques ou numériques) ou non automatisés (manuels), de données à caractère personnel qui sont contenues ou susceptibles d'être répertoriées dans des fichiers.

Quant à leur champ d'application géographique, les textes en question ont vocation à lier tous les responsables de traitement situés sur l'un quelconque des territoires des pays parties aux règlements et directives européens se rapportant aux données personnelles.

Il faut signaler, cependant, que ces règles s'appliquent même à un responsable de traitement non résident dans l'espace européen, toutes les fois que ce responsable « hors Union Européenne » a recourt à des moyens de traitement situés sur le territoire d'un Etat européen, auquel cas il est fait obligation à ce «responsable établi à l'étranger » de désigner un représentant basé, lui, sur le territoire dont les moyens de traitement ont été utilisés (Article 5, 2° de la Loi N ° 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, Modifié par Loi n°2004801 du 6 août 2004 art. 1 JORF 7 août 2004).

Cela dit, les textes évoqués ci-haut concrétisent essentiellement trois (3) droits fondamentaux de la protection des données à caractère personnel: Le droit d'accès, le droit d'opposition et le droit de rectification.

a – Droit d'accès et / ou de questionnement

Ce droit est posé par l'article 39 de la Loi N ° 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Modifié par Loi n°2003239 du 18 mars 2003 art.22 ; Modifié par Loi n°2004-801 du 6 août 2004 art.5 JORF 7 août 2004).

Il dispose que « Toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel en vue d'obtenir :

1° La confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;
2° Des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires ou aux catégories de destinataires auxquels les données sont communiquées ;
3° Le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un État non membre de la Communauté européenne ».

b – Droit d'opposition

Ce droit est consacré par l'Article 38 de la Loi « I & L » (Modifié par Loi n°2004801 du 6 août 2004 art. 5 JORF 7 août 2004).

Au terme de l'alinéa 1er de cette disposition, « Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

L'alinéa 2 de cet article apporte une précision complémentaire tenant au fait que toute personne physique peut également « s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur ».

L'alinéa 3, quant à lui, constitue un régime dérogatoire aux règles édictées par le premier (1er) alinéa, en soulignant qu'il ne s'applique pas « lorsque le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement ».

c - Droit de rectification / Droit au déréférencement (Article 40 nouveau)

Les droits de rectification et déréférencement sont instaurés par l'article 40 créé par Loi n°2004-801 du 6 août 2004 modifiant la Loi « I &L » (art. 5 JORF 7 août 2004)

Il énonce d'abord (alinéa 1er), que « 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 est interdite ».

Mais il instaure également une garantie d'exécution, en faveur de toute personne en droit d'exiger une rectification ou un déréférencement, puisque son alinéa 2 spécifie que « Lorsque l'intéressé en fait la demande, **le responsable du traitement doit justifier**, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'alinéa précédent ».
L'alinéa 3 conforte cette garantie : Il indique, en effet, qu' « En cas de contestation, la charge de la preuve incombe au responsable auprès duquel est exercé le droit d'accès sauf lorsqu'il est établi que les données contestées ont été communiquées par l'intéressé ou avec son accord ».

*** Remarque sur le déréférencement:**

Le déréférencement, que l'on peut définir comme étant l'action d'ôter ou supprimer le lien entre une donnée et son auteur - la personne qui l'a produite – ou sa cible (la personne à laquelle elle se rapporte), peut être entourée d'un certain flou quant à son acception et, de ce fait, sujette à polémique.

Il est intéressant de noter, à ce sujet, l'analyse de Geoffrey Delcroix[9], de la Commission Nationale Informatique et Libertés"

Selon ce spécialiste des données personnelles, le déréférencement n'a pas forcément pour effet l'effacement des références ou des informations sur lesquelles il porte.
A l'appui de son raisonnement, si l'on considère internet, même s'il est procédé à un déréférencement, les contenus, qui ne présentent plus de références à leur(s) auteur(s) ou à leur(s) cible(s) n'en disparaissent pas pour autant ; ces « contenus restent accessibles directement sur le site ou par l'intermédiaire d'autres mots clés de recherche » que leurs références initiales.

4. Mise en œuvre pratique d'une protection efficace des données personnelles

4.1 – Les mesures en elles-mêmes

Sur le plan pratique, la sécurité des données personnelles, dont sont responsables le "Responsable de traitement" et "le sous-traitant", repose sur trois (3) actions ou mesures :
Une action préventive, une action ou mesure procédurale obligatoire et une action informative.

a – La mesure préventive

Elle consiste :
- à assurer la sécurité matérielle et technique des traitements pouvant être réalisés sur ces données par, d'abord, une évaluation des risques potentiels que présentent les modalités de traitement adoptées ;
- et ensuite, une fois les risques identifiés, à mettre en œuvre des règles techniques et organisationnelles appropriées pour empêcher aussi bien l'altération, la perte ou la destruction des données que toute forme illicite de traitement.

b – La mesure procédurale obligatoire

Cette mesure commande à tout responsable de traitement et / ou à son sous-traitant de notifier à l'autorité de contrôle toute violation de données personnelles, au plus tard, 24 heures après en avoir pris connaissance ; Cette notification doit répondre à deux (2) exigences :
- il faut que le contenu de la notification ait été au préalable défini (déclinaison du principe de la légalité des infractions et des peines qui veut qu'un magistrat ne puisse appliquer une peine qui n'ait déjà été prédéfinie par la Loi) ;

---

[9]Geoffrey Delcroix, Chargé des études prospectives de la CNIL, Pôle innovation et prospective, dans sa Présentation « Labo CNIL », page 3.

- la trace documentaire de ladite violation doit être conservée (en guise de justificatif ou preuve).

c – La mesure informative

La personne dont la ou les données ont été violées ayant légitimement le droit de savoir que ses données, l'autorité de contrôle, une fois qu'elle a reçu la notification de la violation dénoncée, peut imposer que soit informée la personne concernée. Là également, la communication doit sacrifier à la condition que son contenu ait été prédéfini.

Mais dans le cas où elle dispose des preuves que des mesures de protection technologiques appropriées ou mesures correctives été appliquées aux données et que ces dernières ont effectivement recouvré leur intégrité, l'autorité de contrôle peut juger non nécessaire la communication de la violation à la personne concernée.

4.2 – Point sur les failles de sécurité

Tel que cela a été signalé plus haut, le responsable de traitement et le sous-traitant doivent observer des mesures préventives matérielles et techniques aux fins de garantir l'intégrité des données personnelles.
Cet impératif et les responsabilités qui en découlent posent donc la problématique cruciale des failles de sécurité. Or le propre d'une faille de sécurité d'un système donné, c'est de rendre possible une intrusion en son sein, donc une violation des éléments qu'il est censé sécuriser.
Se posent alors trois (3) questions :

A quoi correspondent légalement et techniquement une faille ou violation ?
Qui est en responsable ?
Comment l'éviter ou, si elle se produit, comment la "gérer" ?

a – De la détermination de la violation d'une donnée personnelle

a – 1 Acceptions du concept de « violation de donnée personnelle

Les différentes acceptions du terme « violation de données personnelles », qui est expliqué par les textes légaux plus du point de vue de ses conséquences que sous l'angle de la définition distincte et explicite de la « violation » en elle-même, peuvent néanmoins être déduites, de la combinaison de certaines dispositions du code pénal français et de la Loi « I & L ».

Le code pénal français, en l'occurrence son article 226-17, ne donne pas, en effet, la définition d'une violation de donnée personnelle, mais fixe la sanction attachée à son accomplissement. Il dispose, en effet, que « Le fait de procéder ou de faire procéder à un

traitement de données à caractère personnel, sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 … [….] … est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. »

Il faut signaler que le code pénal français, en plus du traitement réprimé par son article 226-17, assimile également la divulgation, non autorisée, d'information à caractère secret ou de données à caractère personnel à une violation de donnée personnelle.
Son article 226-13 prévoit ainsi que « La révélation d'une information à caractère secret par une personne qui en est dépositaire, soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende ».
Son article 226-22, toujours dans le même ordre d'idées, met en place le garde-fou suivant : « 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 est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende. La divulgation prévue à l'alinéa précédent est punie de trois ans d'emprisonnement et de 100 000 Euros d'amende lorsqu'elle a été commise par imprudence ou négligence. Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit. »

La Loi « I & L », à la différence de la loi pénale qui en donne un champ d'application plus large, restreint la définition d'une violation de donnée à caractère personnel au seul domaine de la fourniture au public de services de communications électroniques ; Faut-il en déduire qu'aux yeux du législateur « Informatique & Liberté », les opérateurs et / ou sous-traitants de communications électroniques se rendent plus souvent que les autres acteurs potentiels coupables de violations de données personnelles ?
Toujours est-il que l'article 34 bis, I, alinéa 2 de la Loi « I & L », créé par l'Ordonnance n°2011-1012 du 24 août 2011 (art.38), dispose qu'il faut entendre par violation de données à caractère personnel « toute violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de services de communications électroniques ».

Le paragraphe II met à la charge du fournisseur de services de communications électroniques impliqué l'obligation d'avertir sans délai la CNIL et celle, si ladite violation peut porter atteinte aux données violées ou à la vie privée d'un abonné ou d'une autre personne physique, d'avertir également, sans délai, l'intéressé.
Ce paragraphe apporte cependant une dérogation à l'obligation de notification mentionnée ci-dessus : Ladite obligation tombe si la CNIL a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation.

Le paragraphe III et dernier de l'article pose une règle originale, tenant à ce que chaque fournisseur de services de communications électroniques tienne à jour un inventaire (reporting) des violations de données à caractère personnel, en détaillant les modalités de leur commission, leurs effets et les mesures correctives qu'il y a apportées, sous réserve de conserver ce registre ainsi constitué à la disposition de la CNIL.

a – 2 Interdiction de violer les données personnelles

Deux (2) dispositions de la Loi « I & L » ont spécifiquement été édictées pour éviter la moindre violation d'une donnée à caractère personnel :

- Son article 34 (Modifié par Loi n° 2004-801 du 6 août 2004 art. 5 JORF 7 août 2004), au terme duquel « 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 ».
Il faut souligner le caractère extrêmement important de son alinéa final, qui fait état des prescriptions techniques auxquelles doivent se conformer les traitements mentionnés au 2° et au 6° du point II de l'article 8 (traitements régis par décrets pris après avis de la CNIL), c'est-à-dire :
+ Les traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle
+ et Les traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé ;
- Et son article 35 (Modifié par Loi n° 2004-801 du 6 août 2004 art. 5 JORF 7 août 2004), qui non seulement engage la responsabilité personnelle du responsable de traitement mais érige sa responsabilité au rang d'une véritable « responsabilité du commettant » quand il recourt à un sous-traitant pour un traitement à effectuer.
Il dispose, en effet, que « Les données à caractère personnel ne peuvent faire l'objet d'une opération de traitement de la part d'un sous-traitant, d'une personne agissant sous l'autorité du responsable du traitement ou de celle du sous-traitant, que sur instruction du responsable du traitement » et rajoute que « Toute personne traitant des données à caractère personnel pour le compte du responsable du traitement est considérée comme un sous-traitant » au sens de la Loi « I & L ».
C'est la raison pour laquelle, toujours, selon le même article (alinéa 3), le sous-traitant est également assujetti à des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité mentionnées à l'article 34, même si cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

C'est également ce qui justifie (alinéa 4) que tout contrat liant un sous-traitant à un responsable du traitement doit comporter l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données et doit expressément prévoir que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

b – Des personnes impliquées par la violation d'une donnée personnelle

A priori, si l'on en croit les dispositions de l'article 34 bis, I, alinéa 2 de la Loi « I & L » qui n'envisage une violation de donnée à caractère personnel que dans le cadre de la fourniture au public de services de communications électroniques, ce sont les fournisseurs de services de communications électroniques au public qui sont visées par une quelconque violation des données personnelles.
Il s'agit en premier chef des opérateurs de communications électroniques, qui, rappelons-le, offrent des services de téléphonie fixe ou mobile, acheminent des données et fournissent l'accès à internet à travers des réseaux fixes, mobiles et satellitaires.

Mais les dispositions de l'article précité ne nous permettent pas d'écarter une autre catégorie d'acteurs, notamment les fournisseurs de services de communication au public en ligne ; il s'agit, par exemple :

- des éditeurs de services de vidéos à la demande (VOD) ;
- des exploitants de plateformes de jeux en ligne ;
- des exploitants de réseaux sociaux (LinkedIn, Facebook, Twitter…)
- des éditeurs de journaux et programmes télévisés en ligne

Mais il s'agit, également, par extension, de certains professionnels dont les activités nécessitent qu'ils collectent forcément des données personnelles de leurs clients, tels que :

- les banquiers ;
- les assureurs ;
- et les autres entités privées qui exploitent d'une manière ou d'une autre des réseaux informatiques sur lesquels sont soit acheminés soit archivés des données personnelles.

Sur la base de l'article 34, les responsables de traitement ne sont donc pas directement concernés. Mais cela suffit-il à en déduire qu'ils ne peuvent, en aucun cas, être responsables d'une violation de donnée personnelle ?
Me Forster[10], spécialiste du droit des télécommunications et des technologies avancées, semble le penser.

[10] Me Frédéric Forster, « La Protection de la Vie Numérique », page 106.

Mais nous nous posons tout de même la question de savoir si un responsable de traitement, qui, par définition détermine les finalités et les moyens des traitements et doit en principe être d'une probité à toute épreuve, ne pourrait être amené, pour raison quelconque, à se rendre coupable d'une violation de donnée à caractère personnel consistant, par exemple, en une divulgation non autorisée d'information à caractère secret (?).

Il n'en demeure pas moins, il faut le rappeler, que le code pénal français (cf. article 226-13), lui, fait nommément état de « la révélation d'une information à caractère secret par toute personne qui serait dépositaire, soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire… ».

c – Prise en charge de la violation d'une donnée personnelle

La prise en charge des violations de données personnelles ne se fait seulement après coup, une fois l'acte consommé ; Il s'agit, avant tout, de créer un cadre et des procédures propices à leur évitement.

c – 1 Actions à entreprendre pour éviter ou réduire les risques de violations

Les mesures suivantes doivent en principe empêcher la commission de la moindre violation au sein d'une entreprise ou d'une administration :

- Informer par tout moyen et tout support (notes, circulaires, réunions) la personne responsable de l'état du droit (conséquences) et de l'état de l'art sur les données personnelles ;
- Réaliser un audit juridique et technique des procédures de protection des données personnelles de l'entreprise en prévoyant des mesures de correction.

c – 2 Gestion de la violation proprement dite

Une fois qu'une violation de donnée s'est révélée au sein d'une entreprise ou d'une entité quelconque, les personnes compétentes doivent au plus vite procéder :

- à un inventaire des données violées ;
- à la transmission de l'inventaire à la CNIL (ou veiller à ce que la CNIL puisse avoir libre accès à l'inventaire) ;
- Mettre en place un outil et une méthodologie de remontée de toutes informations pertinentes et d'alertes.

4.3 – Les sanctions apportées à la non-information des personnes concernées et aux traitements irréguliers

Des sanctions pécuniaires très sévères peuvent être appliquées aux entreprises se livrant à une obstruction, une dissimulation ou une rétention d'éléments constitutifs de violation(s) de données à caractère personnel.

C'est ainsi qu'une entreprise qui ne met pas en place, en son sein, un service "Droit d'accès", qui ne répond pas à des demandes légitimes formulées par des personnes – ses employés, notamment – se sachant ou se pensant sujettes à un traitement illicite de données personnelles ou qui exige, en contrepartie de réponses aux demandes qui lui sont faite, de percevoir des frais pour les réponses aux informations demandées, s'expose à une amende de 250 000 € ou pouvant aller jusqu'à 0,5 % de son chiffre annuel mondial.

Encore plus dissuasives, une amende de 500 000 € ou 1 % de son chiffre d'affaires annuel mondial peut être infligée à toute entreprise qui se livrerait à l'un des manquements suivants à l'endroit des personnes vis-à-vis desquelles elle n'a pas été diligente par rapport à leurs demandes :

- Défaut d'information, transmission d'informations incomplètes ou non suffisamment transparentes ;
- Empêchement, entrave, obstruction d'accès, défaut de rectification des données, défaut de communication des informations aux destinataires ;
- Non-respect du droit à l'oubli numérique ou de l'effacement de données ;
- Défaut de communication de copie des données sous forme électronique ;
- Défaut de mise à jour de la documentation intéressant les personnes concernées ou transmission de données non mises à jour ;
- Défaut de définition ou définition insuffisante des obligations des responsables conjoints.

Le plus haut degré dans l'échelle des sanctions, portant le niveau d'amende à l'encontre de toute entreprise défaillante ou négligente en matière de protection des données à caractère personnel à 1 000 000 € ou 2 % de son chiffre d'affaires annuel mondial, est réservé aux manquements les plus graves, qui sont les suivants :

- Les traitements de données effectués soit sans base juridique, soit obtention du consentement des personnes auxquels ils se rapportent ;
- Les traitements de catégories particulières de données (données sensibles, par exemple) en violation des dispositions légales et règlementaires ;
- Le non-respect d'une opposition formulée par une personne concernée ;
- Le non-respect des conditions du profilage ;
- Le non-respect des obligations "d'accountability"[11], de Privacy by Design [12] ou de Privacy Impact Assessment (Analyse d'impact);

[11] Mise en conformité d'une entreprise à la réglementation Informatique et libertés grâce à un ensemble de règles contraignantes, d'outils et de bonnes pratiques correspondantes. Le terme désigne également la mise en place d'un mécanisme permettant de démontrer l'efficacité des mesures prises et l'effectivité de la protection des données.

- L'absence de désignation d'un représentant ;
- Les traitements des données en violation du règlement ;
- L'omission de signaler ou notifier une violation de données ou l'inexécution, en temps utile, d'une mesure corrective ;
- L'absence de réalisation d'une analyse d'impact ;
- L'absence de désignation d'un délégué à la protection des données ;
- Le fait de réaliser ou de donner l'instruction de réaliser un transfert vers un pays non autorisé ;
- Le non-respect de l'obligation de répondre à l'autorité de contrôle.

B. Les Données Personnelles en Afrique

Alors que la question de la protection des données personnelles est d'actualité dans la plupart des pays africains (Algérie, Cameroun, Congo, Mali, Niger, Togo , Tchad , pour ne citer que ceux-là), seule une dizaine d'entre eux sont aujourd'hui dotés d'une loi de protection des données à caractère personnel, sachant que même dans l'affirmative, certains de ces derniers n'ont cependant pas d'autorités dédiées à l'encadrement des actes, produits, services et activités mettant ou pouvant mettre en jeu ces nouvelles valeurs de la vie numérique des individus.

C'est ici le lieu - devant « rendre à César ce qui appartient à César » - de souligner que c'est le Burkina Faso qui est le pionnier de la protection des données à caractère personnel en Afrique (de l'Ouest !), en se dotant, depuis 2004, d'une loi spécifique en la matière, loi dont l'article 26 est relatif à la création d'une autorité qui y est dédiée.

Ce sont d'ailleurs les expériences de coopération entre le Burkina, la France et l'Organisation Internationale de la Francophonie (OIF) qui ont inspiré la création[13], à Montréal, en 2007, de

---

[12]Conception de produits et des services en prenant en compte dès leur conception les aspects liés à la protection de la vie privée et des données à caractère personnel. Il implique également le respect de ces valeurs tout au long du cycle de vie du produit ou service concerné.

[13] Source : « Eléments de présentation de l'AFAPDP », Page 1 ; Mastère Reg Num - Télécom Paris Tech, 2015, par Floriane Leclercq, Chargée de Mission à l'AFAPDP

l'Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP)[14], en réponse à :

- une demande d'assistance des pays pour mettre en place des lois et autorités
- une demande de coopération pour mieux sécuriser les données en cas de transferts à l'étranger (en l'absence de cadre protecteur international).

A ce jour, douze (12) pays africains, dont certains sont membres de l'AFAPDP[15] se sont dotés d'un arsenal juridique voué à la protection des données à caractère personnel[16]. Ce sont, par ordre chronologique d'adoption de législation spécifique :

- Le Cap Vert (Loi datant de 2001, **mais toujours pas d'autorité à ce jour !**) ;
- Le Burkina Faso* (Loi datant de 2004 + Commission de l'Informatique & des Libertés) ;
- La Tunisie* (Loi de 2004 + Instance nationale de protection) ;
- Maurice* (Data Protection Act de 2004 + Data Protection Office) ;
- Le Sénégal* (Loi de 2008 + Commission de protection) ;
- Le Bénin* (Loi datant de 2009 + Commission Nationale de l'Informatique & des Libertés) ;
- Le Maroc* (Loi de 2009 + Commission Nationale pour le contrôle des « DACP » ;
- Le Gabon* (Loi de 2011 + Commission nationale de protection) ;
- Le Ghana (Data Protection Act de 2012 + Data Protection Commission (DPC);
- Le Mali (Loi de 2013 mais **Autorité de protection en cours d'installation**) ;
- La Côte d'Ivoire* (Loi datant de 2013 ; **Protection des données personnelles assurée par l'Autorité de régulation des télécommunications et des TIC (ARTCI)** ;
- Madagascar (Loi de 2014 mais **Commission de protection en cours d'installation**).

[14] Le Burkina, le Bénin, le Gabon, le Maroc, Maurice, le Sénégal et la Tunisie sont membres ; il était question que la Côte d'Ivoire adhère en 2015.
[15] Les pays membres de l'AFAPDP sont marqués par un astérisque.
[16] Source : Site web de l'AFAPDP, http://www.afapdp.org/pays.

B - 1. Les textes africains

La législation africaine traitant de la protection des données à caractère personnel sera succinctement abordée sous l'angle de deux (2) principaux textes supranationaux et celui des lois spécifiques des trois (3) pays qui nous ont servi de base de comparaison : Le Burkina Faso, la Côte d'Ivoire et le Sénégal, le cadre légal et règlementaire mauritanien étant réservé à la deuxième partie de ce document.

B – 1.1 – Les textes supranationaux

Deux textes ont vocation à créer un cadre légal harmonisé dans le traitement des données personnelles au niveau de l'espace communautaire africain :

- « l'Acte additionnel A/SA1 1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la Communauté Economique des Etats de l'Afrique de l'Ouest » (CEDEAO), signé à Abuja, le 16 février 2010 par les chefs d'Etats et de Gouvernements de treize (13) pays[17], sur les quinze (15) que compte l'Organisation.
- et la « Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel », signée par les chefs d'Etats et de Gouvernements ou Représentants dûment autorisés, adoptée à Malabo, le 27 juin 2014 par la 23ème Session Ordinaire de la Conférence de l'Union Africaine (UA).

B – 1.2 –– Les lois nationales africaines choisies comme cadre de comparaison

Les lois burkinabè, ivoirienne et sénégalaise reprenant les mêmes principes généraux et posant, en substance, les mêmes règles que celles qui sont édictées par la législation européenne, notamment française, en la matière, nous ne reviendrons dans leurs détails que si certains de leurs aspects ou spécificités nous paraissent particulièrement pertinents ou, éventuellement divergents en leurs formes ou contenus ; Reprendre textuellement leurs dispositifs respectifs relèverait en effet, nous semble-t-il, plus d'un simple « remplissage » que d'une analyse pourvue d'intérêt réellement instructif, critique ou professionnel.

---

[17] Seuls la Guinée et le Niger ne sont pas signataires ; Nos pays de référence (éléments de droit comparé), c'est-à-dire le Burkina, la Côte d'Ivoire et le Sénégal sont par contre signataires.

a - Résumé de la Loi burkinabè

La loi burkinabè portant protection des données à caractère personnel est la Loi N ° 010-2004/AN du 20 avril 2004.

Elle a « pour objet de protéger, au Burkina Faso[18], les droits des personnes en matière de traitement de données à caractère personnel, quels qu'en soient la nature, le mode d'exécution ou les responsables » (Article 1er).

Elle n'exclut de son champ d'application que trois (3) catégories de traitements :

- les copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique en vue du stockage automatique intermédiaire et transitoire des données à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations (Article 9) ;
- Les traitements de données ayant pour fin le suivi thérapeutique ou médical individuel des patients (Article 11) ;
- les traitements permettant d'effectuer des études à partir des données recueillies à l'occasion des suivis thérapeutiques ou médicaux individuels, à condition, bien entendu, que non seulement ces études soient réalisées par les personnels assurant ces suivis, mais qu'elles soient destinées à leur usage exclusif (article 11).

Au terme de son article 5, « Tout traitement de données à caractère personnel doit avoir reçu le consentement de la ou des personnes concernée(s), sauf dérogations prévues par la loi ».

Quelles sont ces dérogations ?

Les dérogations annoncées par l'article 5 sont constituées par :

- les copies temporaires qui sont faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique en vue du stockage automatique intermédiaire et transitoire des données à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations (Article 9);
- Les traitements de données ayant pour fin le suivi thérapeutique ou médical individuel des patients et les traitements permettant d'effectuer des études à partir des données ainsi

[18] L'article 8, in fine, précise cependant que la Loi ne s'applique pas aux données « qui ne sont utilisées qu'à des fins de transit ».

recueillies si ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif (Article 11) ;
- La collecte de données nécessaires à la constatation d'une infraction (Article 13, in fine) ;
- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis (Art.21);
- le traitement est nécessaire à la sauvegarde de la vie de la personne concernée ou de celle d'un tiers (Art.21);
- le traitement porte sur des données rendues publiques par la personne concernée (Art.21) ;
- le traitement est nécessaire, soit à l'exécution d'un contrat auquel la personne concernée est partie, soit à des mesures précontractuelles prises à la demande de celle-ci (Art.21);
- le traitement est nécessaire à la constatation d'une infraction, d'un droit, à l'exercice ou à la défense d'un droit en justice (Art.21);
- les traitements nécessa1res aux fins de médecine préventive, de diagnostics médicaux, d'administration de soins ou de traitements, de gestion des services de santé, à condition qu'ils soient mis en œuvre par un membre d'une profession de la santé ou par une autre personne à laquelle s'impose, en raison de ses fonctions, le secret professionnel (Art.21).

Remarque : Equivoque (éventuelle) de l'article 6

Au plan purement juridique, même si le bien-fondé de la norme et la volonté du législateur burkinabè ne sont pas remis en cause – loin de nous cette idée – la formulation de l'article 6 nous laisse tout de même un peu perplexe quant à sa portée qui, de notre point de vue, présente le risque d'être mal interprétée.
Il dispose, en effet, que « Toute personne a le droit de connaître et de contester les informations et les raisonnements utilisés dans les traitements, automatisés ou non, dont les résultats lui sont opposés ».
Quid, alors, de la méconnaissance de données utilisées dans un traitement dont les résultats ne lui seraient pas opposés ? N'a-t-elle pas le droit d'en prendre connaissance ?

Cela dit, quel organe est garant de la protection des données personnelles ?

Ce sont les articles 26 à 28 de la Loi burkinabè qui donnent la réponse.

L'article 26 institue une Autorité de contrôle dénommée Commission de l'Informatique et des libertés (CIL), dotée d'un pouvoir règlementaire et d'un pouvoir de sanction, qui a pour but, entre autres, d'informer toutes les personnes concernées de leurs droits et obligations, en plus de contrôler les applications de l'informatique aux traitements des données à caractère personnel.
Afin de pouvoir mener à bien ses missions, cette commission est érigée en autorité administrative indépendante au sein de laquelle siègent neuf (09) membres répartis comme suit (article 27):

- un magistrat, membre du Conseil d'Etat, élu par ses pairs en assemblée générale ;
- un magistrat, membre de la Cour de cassation, élu par ses pairs en assemblée générale ;
- deux députés désignés par le Président de l'Assemblée nationale ;

- deux personnalités désignées par les associations nationales œuvrant dans le domaine des droits humains ;
- deux personnalités désignées par les associations nationales de professionnels de l'informatique ;
- une personnalité désignée par le Président du Faso en raison de sa compétence ;

L'originalité du mode de fonctionnement de cette commission réside dans le fait que ses membres, tous nommés pour un mandat de cinq (5) ans, renouvelable une fois, n'exercent pas de fonction à titre permanent, à l'exception de leur président (Article 28) ; il s'agit donc, vraisemblablement, d'une commission revêtant une nature assez particulière, pour ne pas dire hybride : Officielle et formelle, sur le plan institutionnel, mais ad' hoc, sur le plan fonctionnel.
S'agissant de ses attributions (articles 37 à 45) et des sanctions pénales[19] (…Sic…) qu'elle peut prononcer à l'encontre des contrevenants (articles 46 à 55), elles sont, dans leurs grandes lignes, les mêmes que celles dont dispose la CNIL française.

b – Résumé de la Loi ivoirienne

La loi ivoirienne relative aux données personnelles est la « Loi N ° 2013-450 relative à la protection des données à caractère personnel », du 19 juin 2013.

L'article 3 de ladite loi dispose que sont soumis à ses dispositions :

« [……..]…….

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

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

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

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

[19] Là encore, une question de style peut choquer tout juriste puriste qui ne concevrait que la sanction pénale ne soit que du ressort du juge et non d'une AAI qui, elle, peut infliger des sanctions privatives et pécuniaires mais seulement avec la qualification « sanctions administratives ».

Ce que nous trouvons particulièrement intéressant, dans la délimitation du champ d'application de cette loi, c'est que son article 3 souligne qu'elle vise également l'Etat et les collectivités locales au même titre que tous les autres acteurs potentiels pouvant traiter, faire traiter ou utiliser des données personnelles ; il s'agit là, à notre avis, d'une précision loin d'être inutile car elle a pour mérite de conforter aussi bien les citoyens que tout organe appelé à œuvrer à la protection des données, surtout dans un environnement social et politique dans lequel l'Etat serait - au grand dam d'une démocratie encore chancelante - tout puissant.

Sont, par contre, exclus du champ d'application de cette loi, au terme de son article 4 :

- les traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données ne soient pas destinées à une communication systématique à des tiers ou à la diffusion ;
- les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises. ».

Le consentement préalable exprès de toute personne dont les données personnelles font l'objet d'un traitement est ici également de mise (article 14), sous réserves des mêmes dérogations (art.14 également) que celles qui sont prévues par la Loi burkinabè.

Relativement à l'organe compétent en matière de protection des données personnelles, c'est l'article 46 de la loi ivoirienne qui en confie nominativement la mission à « l'Autorité administrative indépendante en charge de la Régulation des Télécommunications et des Technologies de l'Information et de la Communication », en chargeant cette institution de veiller à ce que les « traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions » de la Loi N ° 2013-450 et de ses décrets d'application.

Ses attributions et pouvoirs de sanctions administratives et financières « supplémentaires », listés en détail par les articles 47 à 52, sont les mêmes que celles dont jouit la Commission burkinabè.

Remarque : Le mode de désignation, les caractéristiques et formes juridiques, les qualifications, missions et conditions d'emploi du Correspondant à la Protection des Données à Caractère Personnel (équivalent du CIL français) ont fait, en Côte d'Ivoire, l'objet d'une fixation par voie règlementaire (Arrêté N° 511 MPTICICAB du 11 novembre 2014 portant définition du profil et fixant les conditions d'emploi du Correspondant à la Protection des Données à Caractère Personnel).

c - Résumé de la Loi sénégalaise

La loi sénégalaise relative aux données personnelles est Loi n° 2008 – 12 du 25 janvier 2008 sur la Protection des données à caractère personnel, en abrégé « LDCP ».

Son article premier (1er), alinéa 1er dispose qu'elle « a pour objet de mettre en place un dispositif permettant de lutter contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel ».

Mais l'alinéa 2 du même article précise, toutefois, qu' « elle prend également en compte les prérogatives de l'Etat, les droits des collectivités locales, les intérêts des entreprises et de la société civile ».

Il est intéressant de constater qu'à l'image de la loi ivoirienne, le texte sénégalais, notamment son article 2, alinéa 1er, spécifie qu'il s'applique à « Toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel… » effectués, entre autres, « ….par l'Etat, les collectivités locales….. ».

Intéressant, d'abord, car cette disposition constitue, en soi, un moyen de renforcer les garanties de protection individuelle, mais intéressant, ensuite, car, notre point de vue, la confrontation de cette même disposition avec les prérogatives étatiques de l'alinéa 2 de l'article 1er peut conduire, dans nombre de cas, à la levée, voire la neutralisation pure et

simple de la protection de certaines données, au nom des prérogatives de l'Etat, surtout si l'on sait que cette notion juridique constitue, un peu partout, souvent un « fourre-tout » extensible à souhait en fonction des circonstances et des objectifs des actions gouvernementales.

Ceci dit, la loi sénégalaise opère les mêmes exclusions de son champ d'application que la loi ivoirienne, à savoir :

- les traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données ne soient pas destinées à une communication systématique à des tiers ou à la diffusion (Article 3, 1°) ;
- les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises (Article 3, 2°).

Sur le plan organique et institutionnel, la protection des données à caractère personnel relève de l'entité suivante : la Commission de Protection des Données à Caractère Personnel dite «Commission des Données Personnelles » en abrégé la « CDP », instituée par l'article 5 de la Loi N ° 2008 – 12.

La CDP est une autorité administrative indépendante chargée de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la loi précitée et a pour charge d'informer les personnes concernées et les responsables de traitement de leurs droits et obligations, en plus de s'assurer que les technologies de l'information et de la communication ne comportent pas de menace au regard des libertés publiques et de la vie privée.

Au terme de l'article 6 de la loi, la CDP est composée de onze (11) membres nommés [20]par Décret[21], en raison de leur compétence juridique et/ou technique ; il s'agit :

- de trois (3) personnalités désignées par le Président de la République ;
- d'un (1) député désigné par le Président de l'Assemblée nationale ;
- d'un (1) sénateur désigné par le Président du Sénat ;
- d'un (1) représentant des organisations patronales désigné par le Ministre chargé des organisations professionnelles;
- d'un magistrat membre du Conseil d'Etat désigné sur proposition du Président du Conseil d'Etat ;
- un magistrat membre de la Cour de Cassation désigné sur proposition du Premier Président de la Cour de Cassation ;
- un avocat désigné par le Bâtonnier de l'Ordre des avocats du Sénégal ;
- un représentant des organisations de défense des droits de l'homme désigné par le Ministre de la Justice, Garde des sceaux, sur proposition du Haut-Commissariat aux droits de l'Homme et à la Promotion de la Paix ;
- et du Directeur de l'Agence De l'Informatique de l'Etat (ADIE).

L'alinéa 3 et final de cet article 6 peut cependant, comme l'article 1er, alinéa 2 relatif aux « prérogatives de l'Etat », susciter quelque appréhensions sur la supposée indépendance de la CDP.
Il dispose, en effet, qu'« un Commissaire du Gouvernement, désigné par le Premier ministre, siège auprès de la Commission des Données Personnelles » et que ce dernier, qui « est convoqué à toutes les séances de la Commission, dans les mêmes conditions que les membres de celle-ci », « Il informe la Commission sur les orientations du gouvernement et sur les motivations de l'administration concernant la mise en œuvre des traitements…. »….même s'il « ne prend pas part au vote ».

S'agissant du mode de fonctionnement de la CDP, le législateur sénégalais a opté pour le système burkinabè. L'article 8 de la loi sénégalaise indique en effet qu'à « l'exception du Président, les membres de la Commission des Données Personnelles n'exercent pas leur fonction à titre exclusif ».

Ses attributions et pouvoirs de sanctions administratives et financières, identiques, dans leurs contenus, à ceux des organes burkinabè et ivoirien, sont listés par les articles 16, 25, 27 et 29 à 31 de la loi sénégalaise.

---

[20] Le mandat des membres de la CDP, qui sont inamovibles, est de 4 ans, renouvelable une fois (article 8 de la Loi).
[21] Les premiers membres de cette commission ont été nommés par le Décret N° 2011-929 du 29 juin 2011.

Pour finir, la loi sénégalaise de protection des données personnelles présente une innovation par rapport aux textes burkinabè et ivoirien : l'exposition possible, en cas de transgression de ses règles, à une triple sanction. Son article 75 énonce, en effet, que les infractions à ses dispositions « sont prévues et réprimées par le Code pénal ainsi que par la loi relative à la cybercriminalité ».

B - 2. Principes fondamentaux découlant des textes africains

Pour les raisons déjà évoquées plus haut – cadre des lois africaines passées en revue d'inspiration française) – nous ferons l'économie de toutes les règles qui résultent des dispositifs-clés de référence.

Nous rappelons, si besoin est, qu'aussi bien, les principes de légalité, finalité et proportionnalité, que les différents droits rattachés aux données personnelles (droits d'accès/questionnement, d'opposition et de rectification / déréférencement) et mesures procédurales de mise en œuvre d'une protection effective de ces données, qui ont été transposées au niveau national par chaque Etat concerné, sont consacrés par

- l'Acte additionnel A/SA1 1/01/10 de la CEDEAO 16 février 2010, relatif à la protection des données à caractère personnel;
- et la Convention de l'Union Africaine du 27 juin 2014 sur la cyber sécurité et la protection des données à caractère personnel.

La brève rétrospective de l'état des lieux du cadre législatif global africain et de celui des pays ouest africains ciblés dans le cadre de notre comparaison, fait ressortir que sur les douze (12) pays membres de l'AFAPDP :

- tous sont dotés d'une loi de protection des données personnelles ;
- huit (8) ont mis en place des autorités dédiées à la protection des données personnelles ;
- deux (2) pays, en l'occurrence le Mali et Madagascar, dont les lois remontent respectivement à 2013 et 2014, n'ont toujours pas achevé la mise en place de leurs autorités de protection des données personnelles ;

- un (1) seul pays, la Côte d'Ivoire, a fait le choix de confier la protection des données personnelles à son autorité de régulation des télécommunications et des TIC (ARTCI) ;

- un (1) seul pays, le Cap Vert, semble avoir délibérément choisi de ne pas se doter d'une autorité en charge de la question, puisque la loi qu'il a adoptée pour régir la matière date de 2001, c'est-à-dire bien avant le Burkina, qui n'a légiféré que trois (3) ans plus tard.

En plus de la tendance majoritaire à mettre en place un organe dédié à la mission de protection des données personnelles, un autre constat se fait jour : De nos trois pays de comparaison, seule la Côte d'Ivoire a institué « un correspondant à la protection des données à caractère personnel » - équivalent du correspondant Informatique & Libertés français (CIL), non seulement en le prévoyant par une disposition légale expresse (article 12) mais en lui consacrant un acte règlementaire pour en définir les profils, qualifications et missions (Arrêté N ° 511 MPTICICAB du 11 novembre 2014).

II – Régulation des données personnelles ou régulation des opérateurs et autres acteurs impliqués ?

De même que tel que nous l'avions signalé, au niveau de l'introduction de cette étude, il n'était pas forcément aisé à des régulateurs traditionnels de communications électroniques de concilier leurs enjeux et problématiques avec ceux tenant à la sphère intime des citoyens, ces derniers ont des préoccupations et intérêts très différents de ceux des opérateurs de communications électroniques, des opérateurs économiques de tous ordres, qu'ils soient producteurs de biens ou prestataires de services.

Mais un fait est constant, c'est qu'au centre des activités de tous ces acteurs se trouvent forcément les données personnelles puisque tantôt certains d'entre eux permettent leur génération, leur acheminement et leurs échanges, tantôt les autres font de leur collecte l'une des conditions principales de leurs offres, voire de la personnalisation de leurs biens et services.

A partir du moment où les entreprises commerciales ou manufacturières, les prestataires de services, les fournisseurs de solutions technologiques et fournisseurs de divers services de communications électroniques surpassent de très loin, en nombre, les opérateurs de communications électroniques, nous pouvons légitimement nous poser la question de savoir si la régulation doit aujourd'hui être envisagée sous l'angle exclusif des contenus, c'est-à-dire s'il faut réguler les données à caractère personnel elles-mêmes, en encadrant les comportements des personnes auxquelles elles se rapportent, ou s'il faut plutôt ne réguler que les opérateurs et autres acteurs qui, à l'occasion de leurs activités, se retrouvent en quelque sorte « les dépositaires temporaires » ou « conservateurs » de ces données.

A. Voix, sons, images, vidéos, signes, texte, Internet & datas

Plusieurs intervenants, pour ne pas dire tous les acteurs du monde actuel des technologies de l'information et de la communication, sont, à des degrés divers, interpelés et impliqués par les données à caractère personnel.

1. Les opérateurs face aux données personnelles

La voix, les sons, les images, les vidéos, les signes et les textes constituent, tant juridiquement que techniquement, des données dont toute émission, toute transmission ou toute réception définit, dans toutes les législations, une communication électronique.

Partant de cette base et de celle de la définition d'un opérateur de communications électroniques (Personne qui exploite un réseau de communications électroniques ouvert au public ou fournit un service de communications électroniques), c'est tout naturellement que ce dernier, qui occupe une place centrale dans l'industrie des communications (téléphonie fixe et mobile, services de messagerie, fourniture d'accès internet), soit assujetti à un ensemble de règles strictes tendant à préserver les droits et assurer la protection des utilisateurs de réseaux et services de communications électroniques, en général, et la protection des données à caractère personnel de ces derniers, en particulier.

C'est la raison pour laquelle les autorités de régulation du secteur des communications électroniques ont toujours veillé, en application de leurs lois respectives, à ce que les opérateurs soumis à leur contrôle, respectent strictement :

- le secret des correspondances des usagers de leurs services ;
- le principe de neutralité vis-à-vis du contenu des messages transmis entre ces derniers ;
- et la protection de leurs données à caractère personnel.

Les opérateurs doivent donc, par conséquent, mettre en place à la fois :

- un dispositif de conservation[22] / anonymisation et d'effacement des données de trafic et de navigation des utilisateurs dès la fin de leurs communications ;
- un dispositif et des mesures de protection des personnes contre les sollicitations commerciales.

Deux exceptions atténuent cependant les dispositions ci-dessus mentionnées, à savoir La permission, qui leur est accordée, de :
- conserver des données pour les besoins de leurs facturations ou du maintien de la sécurité de leurs réseaux ;
- et de traiter des données en vue de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée (SVA) à leurs clients et prospects.

Concrètement, les données susceptibles d'être conservées par les opérateurs sont les suivantes :
▪ Les données techniques permettant d'identifier les utilisateurs ;
▪ Les données intrinsèques aux équipements terminaux utilisés ;
▪ Les caractéristiques, dates, horaires et durées des communications ;
▪ Les spécifications des services complémentaires demandés et / ou consommés par les utilisateurs ainsi que les données relatives aux fournisseurs de ces services (SVA) ;
▪ Les données pouvant établir l'origine (lieu) des communications ;

[22] Les opérateurs peuvent, toutefois, préserver les données qui peuvent permettre d'identifier une personne ayant contribué à la création d'un contenu.

▪ Les données de localisation des communications, d'identification des appelants et des destinataires en vue de procéder à des facturations.

N.B. : Conformément à la législation, un opérateur ne peut conserver les données ci-dessus évoquées au-delà de la durée nécessaire à l'accomplissement des tâches qui ont justifié leur conservation.
C'est ainsi que les données servant à sa facturation, qu'il ne peut communiquer qu'à des tiers directement concernés par la facturation ou au recouvrement, doivent forcément être effacées à l'expiration de la période de contestation éventuelle ou du délai ouvert pour son recouvrement (1 an en France, par exemple).
Quant aux données pouvant avoir la moindre corrélation sur la sécurité des réseaux, leur durée de limitation maximale est beaucoup plus réduite (elle ne peut excéder un trimestre, en France).

Bien entendu, les opérateurs sont déliés de toute obligation lorsque, par exemple, ladite protection peut constituer une entrave à certaines actions menées dans le cadre de la sécurité publique (terrorisme), de la défense nationale (souveraineté de l'Etat), de procédures judiciaires (recherche ou constatation d'infractions) ou à l'exercice de certains droits (droits d'auteurs) auxquels cas toute protection peut être légitimement levée sur requête de (ou des) autorité(s) compétentes.
Maintenant que le lien entre les opérateurs de communications électroniques et les données personnelles est mis en évidence, il faut peut-être revenir sur la justification historique de la régulation de ces exploitants de réseaux ouverts au public et fournisseurs de services de services de communications électroniques, pour se rendre compte que de même que la régulation sectorielle qui les encadrait, à l'origine assise sur une concurrence par les infrastructures - qui permettaient aux opérateurs d'exercer leur pouvoir de marché et créer des effets de domination - s'est ensuite orientée vers une concurrence par les services, internet est venu considérablement changer les donnes avec l'avènement de nouveaux

acteurs[23] (fournisseurs de services de communications électroniques, concepteurs de plateformes d'intermédiation, développeurs d'applications) et services personnalisés.

2. Les données à caractère personnel, « stars » ou victimes d'internet ?

M. Patrick WAELBROECK[24] expliquait de la manière suivante, dans une étude conjointe réalisée en mai 2013 pour le compte du Commissariat général à la stratégie et à la prospective, la nouvelle configuration de ce que nous appellerons « l'écosystème des communications électroniques » induite par internet : « Englobant progressivement à la fois les marchés issus des télécommunications classiques (et notamment le service téléphonique, principal service rémunérateur) et les marchés d'intermédiation, internet pose principalement la question de la dissociation réseau-service/contenu ».

C'est donc dire à quel point les opérateurs classiques, qui avaient une parfaite maîtrise en amont et en aval de tout le leur « cycle de production » économique, de leurs infrastructures aux produits finis aux consommateurs, se sont très rapidement vu ravir des parts considérables de leurs marchés (niches) par des nouveaux concurrents qui non seulement, pour certains excellent dans leurs segments d'intervention, mais arrivent à les concurrencer, voire les dépasser (fournisseurs d'accès, de contenus et de services à valeur ajoutée).

Les infrastructures traditionnelles faisant place à de nouvelles technologies (supports, plateforme, terminaux) et les services classiques « s'effaçant » ou à tout le moins, s'amenuisant progressivement pour laisser la place à de nouveaux usages, la régulation du secteur en question, pour être efficiente, se doit donc, puisque toute régulation, par définition, s'attache à mettre en place le cadre d'une saine concurrence, d'évoluer en conséquence et s'adapter à ce nouveau « paysage numérique » qui se met en place.

---

[23] De nombreux autres acteurs collectent et traitent également des données personnelles dans le cadre de leurs interactions avec leurs clientèles ou administrés, à l'exemple des banques, des assureurs ou des administrations mais présentent beaucoup d'enjeux de régulation qu'internet, qui retiendra donc notre attention.

[24] Professeur d'économie à Telecom ParisTech, Auteur de « Protection de la vie privée », dans « La dynamique d'internet Prospective 2030 », Étude réalisée pour le Commissariat général à la stratégie et à la prospective, Mai 2013, Page 86.

M. WAELBROECK ne dit pas autre chose, quand il soutient[25] que puisque « La régulation s'intéresse aux marchés, à leurs défaillances éventuelles » et que, « les formes de concurrence qui se développent sur internet bousculent la conception classique du marché », « le futur de la régulation doit aussi affronter de nouveaux objets[26] et de nouveaux acteurs qui ne faisaient pas traditionnellement partie du champ habituel de la gouvernance des secteurs industriels ».

Avec le boom des plateformes d'intermédiation auquel l'on assiste, Internet nous met aujourd'hui en présence, comme il le souligne, de « mécanismes automatiques ou asservis (via l'internet des objets) » et constitue le cadre d' « échanges interpersonnels et communautaires » dont le but est d' « orienter une partie des consommateurs vers certains contenus, voire certaines applications, certains services ou certaines formes de consommations ».

Les plateformes d'intermédiation, autres formes de support et terminaux (smartphones, objets connectés) posent une problématique cruciale au regard de notre sujet : ils sont, pour leur fonctionnement, alimentés de données en tous genre et se « nourrissent » littéralement de données à caractère personnel.

Se pose alors la double question, qui interpelle forcément la régulation, de la confiance que les individus peuvent avoir en ces outils technologiques et celle, incidemment, de leur « dépendance », non seulement à ces mêmes instruments mais aussi vis-à-vis des personnes avec lesquelles les plateformes les mettent en relation (firmes, prestataires de services divers, partenaires, voire administrations).

En effet, de la même manière qu'un Etat doit renoncer à une partie de sa souveraineté dans le cadre d'un traité international qui est la condition de son accueil au sein d'un groupe supranational ou d'un ensemble mondial, « exister » sur internet, suppose et requiert, aujourd'hui, d'accepter de restreindre certains pans de sa souveraineté personnelle (éléments de sa vie privée, nombre de données à caractère personnel), voire de renoncer à

[25] Etude précitée
[26] Objets connectés (biométrie, traceurs, compteurs intelligents, notamment)

toute intimité et ce, même malgré la possibilité technique de se fabriquer une (ou plusieurs) fausse(s) identité(s) ou vie(s) numérique(s) et celle de faire héberger ses données « en soi-disant toute sécurité[27] » .

Antonio Casilli[28] avance, à ce propos, que « Le partage de contenus est une motivation essentielle des utilisateurs des technologies communicantes actuelles » et que « Ces contenus incluent, entre autre, de l'information sur l'usager lui-même, des contenus qui incluent des informations sur leur émetteur, ses préférences et ses comportements, de sorte à attirer des choix homophiles ». Il conclut, en en déduisant que « La constitution de structures de réseaux est donc inséparable de la question du dévoilement de soi et par conséquent de la négociation de la vie privée ».

Citons, en guise d'illustration, un exemple éloquent de « l'effritement » de l'intimité et de l'exposition des données personnelles des usagers des nouvelles technologies.

Il s'agit d'un cas de violation manifeste de la vie privée, donc des données personnelles des individus, matérialisé les télévisions connectées de SAMSUNG, relaté par le Journal « LIBERATION », dans sa parution du 09 février 2015[29] :

Selon cet article, intitulé « Votre télévision vous enregistre-t-elle à votre insu ? (Big Brother is watching you), les télévisions connectées de Samsung, qui sont contrôlées par les voix de leurs propriétaires, enregistrent, une fois qu'elles sont allumées, l'ensemble des conversations de ces derniers, avant de les envoyer à une tierce entreprise.

L'auteur soutient que les termes et conditions de la dernière TV connectée de Samsung sont les suivants : «Soyez conscients que, si les mots que vous prononcez (à portée de la télévision) incluent des données sensibles ou personnelles, ces dernières seront, avec

---

[27] Cloud Computing ou « Informatique en nuage ».

[28] Sociologue, Maître de Conférences en Humanités Numériques à Telecom ParisTech, Auteur de « Vie privée dans un monde dense », dans « La dynamique d'internet Prospective 2030 », Étude réalisée pour le Commissariat général à la stratégie et à la prospective, Mai 2013, Page 135

[29] Article publié sur internet par Hugo Pascual
http://www.liberation.fr/sciences/2015/02/09/votreteleviseurvousenregistretilavotreinsu_1198872

l'ensemble des autres données, enregistrées et transmises à un tiers par le biais du dispositif de reconnaissance vocale».

Il explique que lorsque la télévision est allumée, une petite icône représentant un microphone s'affiche à l'écran pour signaler que le poste est à l'écoute, mais que s'il advenait que celui ou celle qui l'a allumée oublie que cette fonction est en marche et tienne une conversation dans le champ d'action du micro, Samsung l'enregistrerait avant de la sauvegarder sur un serveur et de partager les données avec une tierce entreprise.

Pour finir, l'auteur souligne le paradoxe de la déclaration de SAMSUNG, qui prétend prendre très au sérieux la vie privée de ses consommateurs, auxquels sont offertes de nombreuses possibilités de se retirer de ce service, alors que la marque reconnaît cependant que «Samsung does not retain voice data or sell it to third parties. If a consumer consents and uses the voice recognition feature, voice data is provided to a third party during a requested voice command search» Traduction : «Samsung ne garde ou ne vend aucune donnée vocale à une tierce partie. Si les consommateurs consentent et utilisent le système de reconnaissance vocale, les données seront fournies à une tierce partie lors du procédé impliquant une commande vocale».

L'on sait également, aujourd'hui, que les usagers d'internet ne sont plus que de simples consommateurs passifs d'informations et données en tous genres; ils ont aujourd'hui un rôle actif, puisqu'en fournissant eux-mêmes des données publiques ou personnelles (capteurs et connexions liés à leurs professions, leurs domiciles ou leurs corps), des traces de ses connexions (cookies), des informations et des contenus (interactions P2P), ils concourent à un certain rééquilibrage de l'offre et de la demande.

L'une des conséquences que nous pouvons déduire des réalités du nouvel internet et des bouleversements qu'il opère, c'est que les données à caractère personnel, peuvent, sans encadrement énergique, être mises à mal, non seulement par une diversité d'acteurs et de domaines confondus, qui doivent capter toute l'attention aussi bien des individus que des organes auxquels sera confiée la protection des données rattachées à ces individus

(intervenants des domaines des nouvelles technologies et des communications électroniques, du commerce physique comme électronique, du marketing et de certains établissements financiers dédiés aux patrimoines des individus, tels que les banques et les assurances, pour ne citer que ceux-là).

Nous pouvons citer, à titre d'exemple, l'importance des mesures qui doivent être prises dans le cadre des transactions électroniques pour, d'un côté, protéger les utilisateurs qui fournissent leurs données personnelles et, de l'autre, lutter contre la fraude aux moyens de paiements utilisant des réseaux bancaires ou interbancaires, qui impliquent et exposent à la fois :

- les réseaux interbancaires eux-mêmes ;
- les banques affiliées à ces réseaux ;
- les commerçants qui utilisent des terminaux nécessaires à la validation des paiements
- les acheteurs potentiels, qui se trouvent être clients des banques et des commerçants,

dont les données peuvent être interceptées, piratées et détournées.

3. Point récapitulatif sur la géolocalisation et les cookies[30]

Daniel Kaplan, dans son ouvrage « Informatique, libertés, identités »[31] publié en avril 2010 par la Fédération Internet Nouvelle Génération (FING), constate « le déséquilibre profond entre les énormes capacités de surveillance et de traçage des individus, par les autorités comme par les entreprises, d'une part, et le peu de pouvoir qu'ont les individus eux-mêmes sur leurs propres données, d'autre part ». Cet auteur touche ainsi du doigt une question qui devient de plus en plus préoccupante : celle de la géolocalisation.

---

[30] La prospection par mails, SMS, MMS, courriers sur supports papiers et autres modes publicitaires a volontairement été éludée car bien qu'intrusive et dérangeante, elle ne présente pas, de notre point de vue, les risques redoutés par l'exploitation malveillante des données personnelle de ses destinataires.

[31] « Informatique, libertés, identités », avril 2010, Fyp Editions,

Hubert Guillaud[32], rédacteur en chef d'InternetActu.net et responsable de la veille à la FING, rappelait, quant à lui, lors d'une présentation sur le web des données, qu'il a faite à l'occasion de Semaine européenne des l'Open Data (..Sic..), les propos d'un certain Clive Humby[33], datant de 2006 déjà, qui affirmait que "Les données sont le nouveau pétrole de l'économie" et ceux, non moins prédictifs de Tim O'Reilly et John Battelle[34], dont les convictions sur les données étaient les suivantes :

« Le web est un écosystème de bases de données interconnectées. Les données sont partout, sous forme d'énormes répertoires de données produisant elles-mêmes leurs propres données, car la façon même dont nous interrogeons ces données devient elle-même source de données. C'est d'ailleurs la première des données, la plus accessible, la plus importante. Celle de nos comportements en ligne, de nos historiques de navigations ».

Ces allégations, portant sur ce que d'aucuns appellent aujourd'hui « le nouvel or noir de l'internet» ou « la nouvelle monnaie du monde numérique », notamment Meglena Kuneva[35], ne traduisent pas autre chose que le phénomène des « cookies ».

3.1 – La géolocalisation

La géolocalisation, lorsqu'elle n'est pas motivée par des motifs légitimes bien limités, tels que la recherche d'un terroriste, de l'auteur d'une infraction ou d'un objet volé, présente un sérieux risque d'atteinte à la vie privée des individus en ce qu'elle peut permettre à des organismes privés ou administratifs, en la mettant en œuvre (employeurs, notamment), de connaitre avec précision :

- quels sont les habitudes et comportements des individus suivis ;
- quels sont les déplacements que des individus effectuent vers des lieux où ils ne sont pas censés se rendre ;

---

[32]« Vers un nouveau monde de données », 01/06/2012, http://www.internetactu.net/2012/06/01/versunnouveaumondededonnees/

[33] Clive Humby, Mathématicien, Expert consultant en fidélisation

[34] Spécialistes du BIG DATA, qui ont lancé la première conférence « Web 2.0 » au mois d'octobre 2014

[35] Commissaire européenne à la consommation en 2009.

- quels sont les établissements de santé que les personnes surveillées fréquentent, et donc, pour quelles raison elles s'y rendent ;
- quels sont les lieux de cultes fréquentés par une personne faisant l'objet de suspicion ;
- les détournements d'usages auxquels certaines personnes peuvent se livrer (un employé qui utilise les moyens de déplacement de son entreprise pour faire ses courses personnelles ;
- et, pour s'en arrêter là, l'appartenance politique d'une personne, en surveillant à quels mouvements politiques elle se rend.

Ce qu'il faut retenir principalement, c'est que la géolocalisation, qui est strictement encadrée[36] par les dispositions des articles 230-32 à 230-44 du code de procédure pénale française, doit, pour pouvoir être mise en œuvre, répondre à certaines conditions :

▪ Il peut y être fait recours, mais à la condition que ce soit en temps réel, c'est-à-dire ponctuellement et non de manière permanente ;

▪ l'acteur de la géolocalisation doit obtenir le consentement des personnes susceptibles d'y être soumises (des employés, notamment), sachant que ce consentement exprès doit systématiquement être actualisé chaque année ;

▪ le système de géolocalisation doit, par défaut, être désactivé (donc seulement en fonctionnement en cas de nécessité) ;

▪ Et, enfin, chaque activation doit nécessairement faire l'objet de l'information des personnes concernées.

3.2 – Les cookies

Laurent Gille fait deux (2) constats intéressants[37] à plus d'un titre, car décrivant bien quelques raisons pour lesquelles aussi bien des commerçants que des fournisseurs de contenus et services électroniques recourent aux cookies, ces fameux « témoins » de la navigation des internautes :

---

[36] La géolocalisation a fait l'objet, au niveau européen, de l'avis N ° 13/2001 du G29.
[37] Dans « La donnée au cœur du numérique : questions », pages 28 & 32.

Il commence par attirer l'attention sur le fait « Ce ne sont plus uniquement les produits qui sont jaugés, mais les êtres passés au crible de métriques de plus en plus nombreuses: nombre de connexions, d'amis, de followers, de messages envoyés ou reçus, nombre de fois où son profil aura été consulté, de pages ou sites web sur lesquelles son nom apparaît… ».
Il présente, ensuite, l'opposition de deux (2) conceptions, l'une, que nous qualifierons de juridique et l'autre, d'économique, mais toutes les deux aussi défendables l'une que l'autre :

▪ La donnée est une partie constitutive de la personne et ne peut être cédée sans son consentement ;
▪ La donnée est un ingrédient essentiel du fonctionnement du marché et ne peut être réservée si le risque encouru est disproportionné à la charge de son absence pour le marché.

Les cookies, qui ont été règlementées en France depuis 2011 et fait l'objet d'encadrement, au niveau européen, par la Directive N ° 2009/136, doivent répondre aux exigences suivantes :
- Ceux qui les conçoivent doivent informer les utilisateurs avant l'installation des programmes en question sur leurs terminaux ;
- Ils doivent, également, expliciter les finalités poursuivies par l'installation des cookies ;
- Et ils doivent, enfin, mettre à la disposition de tout utilisateur ne désirant pas que des cookies soient installés sur sa machine, des moyens d'opposition à ladite installation.

N.B. : Le recueil du consentement préalable à l'installation d'un cookie est obligatoire sauf dans deux (2) cas :
- S'ils facilitent la communication par voie électronique ;
- S'ils sont nécessaires à la fourniture d'un service de communication en ligne.

B. Problématique des Données Sensibles – Fondement du droit de la protection des données personnelles

Une donnée est la description élémentaire d'une réalité ; elle constitue, par exemple, une observation ou une mesure[38].

Or c'est en organisant des données collectées, comme l'a si bien démontré Serge ABITEBOUL[39], lors de sa leçon inaugurale au Collège de France le 8 mars 2012, que l'on obtient une information sensée et c'est en comprenant les informations qu'il est possible d'aboutir à des connaissances, c'est-à-dire à des « faits », considérés comme vrais et à des « lois », autrement dit des règles logiques.

De la masse, pour ne pas dire de « l'univers » incommensurable et inépuisable de données, nous pouvons opérer la séparation suivante :

Il y a d'abord les données qui sont relatives à tout ce qui est commun à la société – au sens sociologique du terme – qui peuvent et doivent, d'ailleurs, être partagées par tous, puisqu'elles sont « publiques » et concourent à l'information et à la connaissance dont nous parlions ci-dessus.

Et il y a ensuite les données propres à chaque individu, pris isolément, qui, comme le rappelait Laurent Gille[40], font partie intégrante de sa personne.

Contrairement aux données intéressant toutes les composantes possibles d'une communauté (particuliers, corporations éducatives et / ou professionnelles, artistiques, administrations civiles ou militaires, etc.), les données personnelles, bien que certaines d'entre elles soient utiles à un enrichissement de la « connaissance » collective et donc, profiter à la masse dans une optique purement didactique et scientifique, renseignent avant tout et surtout, sur des attributs intrinsèques des individus allant de leurs patrimoines, que légitimement, ils cherchent à préserver, à défaut de les faire fructifier, à leurs

[38] Serge ABITBOUL, Informaticien français, Professeur à l'ENS Cachan et directeur de recherche à INRIA ; Elu Membre de l'Académie des Sciences le 16 décembre 2008 pour ses travaux sur la gestion d'informations.
[39] Leçon inaugurale au Collège de France, 08 mars 2012.
[40] Cf. « La donnée au cœur du numérique : question », page 32.

caractéristiques physiques, morales, physiologiques et psychologiques, en passant par leurs habitudes et philosophies de vie, leurs loisirs mais aussi, éventuellement, leurs passés, généalogies et histoires de famille qu'ils peuvent avoir, également, des raisons légitimes, de garder confidentiels.

Au sein de cette dernière catégorie de données, communément regroupées sous le vocable « données personnelles » et faisant l'objet d'un encadrement légal (régime d'autorisation de traitements sous réserve du consentement des personnes concernées), il en est certaines, que, plus que les autres, les personnes auxquelles elles se rapportent tiennent coûte que coûte à tenir hors de portée de qui que ce soit ; il s'agit des données sensibles.

Revêtent la qualification légale de « données sensibles » (c'est le cas de toutes les législations abordées infra), toutes les données pouvant permettre d'établir les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale, ainsi que celles qui se rapportent à l'état de santé des personnes concernées par lesdites données.

Ce qui sous-tend logiquement, à notre avis, cette règle, c'est l'idée qu'aucune personne ne devrait, dans un Etat de droit, souffrir du moindre préjudice, ni de la moindre discrimination de quelques ordre et nature qu'elle soit, en raison de facteurs non objectifs tels que sa race, son affiliation politique, ses déficiences médicales ou sa religion (protégée par la liberté du culte dans les pays laïques), pour ne citer que ces éléments.

En France, à titre d'exemple, c'est l'article 8 / I, de la Loi « I & L », Modifié par LOI n°2016-41 du 26 janvier 2016 qui pose l'interdiction de «collecter ou de traiter » des données sensibles.

Etant donné que les données à caractère personnel « non sensibles » peuvent être traitées sous certaines conditions (consentement exprès préalable des personnes concernées et, selon le cas, déclaration du traitement envisagé à l'autorité de protection et / ou autorisation), il ne nous paraît pas faire de doute que les « données sensibles » - dont le traitement est purement et simplement interdit, sauf dans de rares cas limitatifs - constituent le fondement de la protection que les législateurs ont consacrée à leur égard, puis étendues à toutes les données qui pourraient revêtir le moindre caractère personnel.

Quelles sont les dérogations à l'interdiction de traiter des données sensibles ?

Il existe neuf (9) dérogations possibles à l'interdiction de traiter des données sensibles, dérogations « possibles » car n'étant envisageables que si la finalité des traitements l'exige pour certaines catégories de données (lorsqu'il faut impérativement effectuer à ces traitements) et parce qu'étant strictement encadrées ; Il n'est donc pas possible de mettre systématiquement en œuvre les dérogations en question. Il s'agit :

- des traitements pour lesquels la personne concernée a donné son consentement exprès, sauf dans le cas où la loi prévoit que même le consentement de la personne concernée ne peut lever l'interdiction de traitement ;
- des traitements nécessaires à la sauvegarde de la vie humaine, mais auxquels la personne concernée ne peut donner son consentement par suite d'une incapacité juridique ou d'une impossibilité matérielle ;
- des traitements mis en œuvre par une association ou tout autre organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical, si ces traitements portent uniquement sur des données en relation avec l'objet de ladite association ou dudit organisme et ne concernent que les membres de cette association ou de cet organisme ou, le cas échéant, des personnes qui entretiennent avec ladite association ou ledit organisme des contacts réguliers dans le cadre de leurs activités. Il faut noter que dans tous les cas, les données objet des traitements réalisés ne doivent pas être communiquées à des tiers, à moins que les personnes concernées n'y consentent expressément ;
- des traitements portant sur des données que la personne concernée a elle-même rendues publiques ;
- des traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- des traitements nécessaires aux fins de la médecine préventive, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de services de santé et mis en œuvre par un membre d'une profession de santé, ou par une autre personne à laquelle s'impose, en raison de ses fonctions l'obligation de secret professionnel (laborantin, assureur-santé par exemple) ;

- des traitements statistiques réalisés par les organes étatiques compétents ;
- des traitements nécessaires à la recherche, aux études et évaluations dans le domaine de la santé ;
- et, enfin, des traitements, automatisés ou non, justifiés par l'intérêt public (registres destinés à l'information du public, traitements de données médicales faits pour des situations d'urgence de santé publiques, telles que les épidémies, traitements intéressant la Sûreté de l'Etat, la Défense ou la Sécurité Publique, traitements relatifs à la recherche et la répression des infractions.

N.B. : (1) Les traitements justifiés par l'intérêt public font l'objet d'autorisations spéciales matérialisées par l'adoption d'actes administratifs (Décrets, Arrêtés).

(2) En France, les dérogations évoquées ci-dessus sont énumérées par les paragraphes II / 1° à 8° et IV de l'article 8 nouveau de la Loi « I & L ».

DEUXIEME PARTIE - LE CONTEXTE MAURITANIEN

I – Etat des lieux

Comme annoncé au niveau de la problématique générale qui sous-tend notre réflexion, c'est peu de dire que la Mauritanie n'en est encore toujours qu'à la phase conceptuelle de la protection[41] des données à caractère personnelle, tant il est vrai que le projet de Loi qui porte cet intitulé, ainsi qu' un second, qui lui, est voué à régir les transactions électroniques, sont encore, à ce jour, au stade de discussions au niveau des chambres parlementaires.

[41] Pour rappel, à ce stade, les textes promulgués ayant trait aux technologies de l'information et de la communication sont la Loi N ° 2016-006 du 20 janvier 2016 portant Loi d'orientation de la Société Mauritanienne de l'Information et la Loi N ° 2016-007 du 20 janvier 2016 relative à la cybercriminalité.

A – La collecte et le traitement éthiques prévus par les textes

(Projet de Loi relatif à la protection des données à caractère personnel[42])

L'article Premier (1er) du projet de Loi relatif à la protection des données à caractère personnel (PLPDP) indique qu'il « a pour objet de mettre en place un cadre normatif et institutionnel sur le traitement de données à caractère personnel, en vue de garantir de meilleurs services, de prévenir et de lutter contre les atteintes à la vie privée susceptibles d'être occasionnées par l'utilisation des Technologies de l'Information et de la Communication ».

Il précise, cependant, que ses dispositions ne sauraient faire échec à celles de la Loi N ° 2011 - 003 abrogeant et remplaçant la Loi N ° 96-019 du 19 juin 1996, portant code d'état civil et celles de ses textes d'application.

1. Champ d'application et exclusions

Au terme de son article 3, le PLPDP s'applique aux cinq (5) catégories de traitements suivants :

- tout traitement de données à caractère personnel, effectué par une personne physique, par l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé ;
- tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier, à l'exception des traitements à vocation personnelle ou domestique effectués par une personne physique et copies temporaires de transmission) ;
- tout traitement mis en œuvre par un responsable sur le territoire mauritanien ou en tout lieu où la loi mauritanienne s'applique ;
- tout traitement mis en œuvre par un responsable, établi ou non sur le territoire mauritanien, qui recourt à des moyens de traitement situés sur le territoire national, à l'exclusion des moyens qui ne sont utilisés qu'à des fins de transit ;

[42] Pour la suite, l'acronyme « PLPDP » désignera le Projet de Loi relatif à la protection des données à caractère personnel.

- tout traitement des données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt quelconque de l'Etat, sous réserve des dérogations que prévoit la présente la Loi et des dispositions spécifiques en la matière fixées par d'autres lois.

Echappent par contre au champ d'application du PLPDP, comme l'indique son article 4, les mêmes actes que ceux qui sont autorisés par les lois comparées dans notre première partie:

- les traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données ne soient pas destinées à une communication non autorisée à des tiers ou à la diffusion ;
- les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

2. Principes fondamentaux attachés aux traitements

Hormis l'exigence du consentement de la personne dont le traitement des données personnelles est envisagé (Article 5 PLPDP), sauf cas dérogatoire constitué par une obligation légale, l'exécution d'une mission d'intérêt public, l'exécution d'un contrat liant le concerné ou la sauvegarde de son intérêt ou de ses droits et libertés fondamentaux, les principes essentiels auxquels doit se conformer tout traitement de donnée personnelle sont, à l'identique de ce que prévoient les autres lois africaines et la loi française, les suivants :

- Le principe de légalité, érigé par l'article 6 du PLPDP ;
- Le principe de finalité (Article 7, alinéa 1er) ;
- Et le principe de proportionnalité (Article 7, alinéa 2).

Cela dit, l'alinéa 3 de l'article 7 du PLPDP interdit toute conservation de données plus longue que de nécessaire, à moins que la conservation ne soit prolongée à des fins historiques, statistiques ou de recherches en vertu des dispositions légales.

Relativement aux droits des personnes concernées, le PLPDP consacre le droit à l'information de ces dernières, qui fait l'objet de ses articles 9 et 50, ainsi que les droits d'accès (Articles 53 à 58), d'opposition (articles 59 et 60) et le droit de rectification et suppression (articles 61 à 63).

Pour ce qui est maintenant des données sensibles, leur interdiction est formalisée par l'article 12 du PLPSD qui dispose qu' « Il est interdit de procéder à la collecte et à tout traitement qui révèlent l'origine raciale, ethnique, linguistique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée ».
L'interdiction de traitement des données précitées souffre cependant des dix (10) exceptions suivantes:

- Leur manifeste mise à la disposition du public opérée par les personnes concernées elles-mêmes ;
- Le consentement écrit à un tel traitement, sur quelque support que ce soit, donné par les intéressés ;
- Les traitements nécessaires à la sauvegarde des intérêts vitaux des personnes concernées ou de toute autre personne, si ces dernières se trouvent dans l'incapacité physique, mentale ou juridique de donner leur consentement ;
- Les traitements nécessaires à la constatation, à l'exercice ou à la défense d'un droit en justice ;
- Les traitements occasionnés par une procédure judiciaire ou une enquête pénale concernant une personne concernée;
- Les traitements justifiés par un motif d'intérêt public, notamment à des fins historiques, statistiques ou scientifiques ;
- Les traitements nécessaires à l'exécution de contrats liant les intéressés ;

- Les traitements nécessaires au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ;
- Les traitements nécessaires à l'exécution d'une mission d'intérêt public, effectués par une autorité publique ou assignés par une autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées ;
- Et, enfin, les traitement effectués dans le cadre des activités légitimes d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale, sous réserve, toutefois, que les dits traitements se limitent aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers, liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

Il est intéressant de noter que selon les dispositions de l'article 14, seules les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales, ainsi que les auxiliaires de justice peuvent mettre en œuvre des traitements de données relatives à des infractions, condamnations pénales et mesures de sûreté.

Dans un autre registre, la double préoccupation des effets de publicité, dans le cadre des prospections directes et de la transmission de données personnelles à des tiers (cookies, par exemple) aux mêmes fins est prise en compte par le législateur mauritanien qui interdit, formellement, non seulement ces pratiques, sous réserve du consentement préalable des personnes ciblées (article 18, alinéa 1er) mais également la communication à des tiers ou l'utilisation des données personnelles dans un commercial.

3. Les différents régimes mis en place par le PLPDP

Les différents régimes de traitements de données personnelles aménagés par le PLPDP sont :
- Celui des dispenses de formalités, prévu à son article 32 ;
- Celui de déclaration, régi par ses articles 33 à 36 ;

- Celui de l'autorisation, encadré par les articles 37 à 39 ;
- Et le régime de l'autorisation sur avis de « l'Autorité de Protection des Données à Caractère Personnel » (Articles 40 à 42).

3.1 Les dispenses de formalités :

Elles concernent :

▫ En tout premier lieu, les traitements de données mis en œuvre par la personne physique qu'elles concernent à titre personnel ou domestique, sous réserve que ces données ne soient pas destinées à une communication non autorisée à des tiers ou à la diffusion et les copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises ;

▫ Ensuite les traitements à seule finalité de tenue de registres destinés à l'information du public ;

▫ S'ensuivent les traitements mis en œuvre par une association ou tout organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical dès lors que ces données correspondent à l'objet de cette association ou de cet organisme, qu'elles ne concernent que leurs membres et qu'elles ne doivent pas être communiquées à des tiers ;

▫ Et, enfin, les traitements réalisés avec le consentement écrit des personnes concernées.

3.2 Le régime de la déclaration

Il s'applique à tous types de traitements différents de ceux qui bénéficient de la dispense, évoqués ci-dessus et ne constituant pas l'une des opérations suivantes :

- les traitements des données à caractère personnel portant sur des données génétiques et sur la recherche dans le domaine de la santé ;

- les traitements des données à caractère personnel relatives aux infractions, condamnations ou mesures de sûreté ;
- les traitements des données à caractère personnel ayant pour objet une interconnexion de fichiers ;
- les traitements portant sur un numéro national d'identification ou tout autre identifiant de portée générale ;
- les traitements des données à caractère personnel comportant des données biométriques ;
- les traitements des données à caractère personnel ayant un motif d'intérêt public, notamment à des fins historiques, statistiques ou scientifiques.

3.3 Le régime de l'autorisation

Conséquemment au champ d'application du régime déclaratif, les traitements suivants ne peuvent être mis en œuvre qu'après avoir formellement été autorisés par l'Autorité de Protection des Données à caractère personnel :

- les traitements des données à caractère personnel portant sur des données génétiques et sur la recherche dans le domaine de la santé ;
- les traitements des données à caractère personnel relatives aux infractions, condamnations ou mesures de sûreté ;
- les traitements des données à caractère personnel ayant pour objet une interconnexion de fichiers ;
- les traitements portant sur un numéro national d'identification ou tout autre identifiant de portée générale ;
- les traitements des données à caractère personnel comportant des données biométriques ;
- les traitements des données à caractère personnel ayant un motif d'intérêt public, notamment à des fins historiques, statistiques ou scientifiques.

3.4 Le régime de « l'autorisation sur avis de l'Autorité de Protection des Données à Caractère Personnel »

Ce régime vise tous les traitements autorisés non par la Loi ni par l'Autorité de Protection des Données à Caractère Personnel, mais autorisés par actes règlementaires – donc par le Gouvernement – sur avis motivé de l'Autorité de Protection.
Les traitements dont il est question, opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité locale ou d'une personne morale de droit privé gérant un service public, portent spécifiquement sur :

- la sûreté de l'Etat, la défense ou la sécurité publique ;
- la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;
- le recensement de la population ;
- les données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci (Donc les données sensibles !);
- le traitement de salaires, pensions, impôts, taxes et autres liquidations
- la mise en œuvre du recouvrement des ressources de l'Etat.

4. Les obligations incombant aux responsables de traitements et à leurs sous-traitants

L'article 46, alinéa 1er du PLPDP rappelle que « Le traitement des données à caractère personnel est strictement confidentiel » et qu' « Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement, et seulement sur ses instructions ».
Il en découle plusieurs obligations édictées à l'égard des responsables de traitements et de leurs sous-traitants :
- une obligation de confidentialité (article 46) ;

- une obligation de sécurité (article 47) ;
- une obligation de conservation, limitée à la durée nécessaire, hormis les cas de conservations à des fins historiques, statistiques ou scientifiques (article 48) ;
- et une obligation de pérennité (article 49).

N.B. : La pérennité dont il est fait cas veut que tout responsable de traitement prenne toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées, ultérieurement, quel que soit le support technique utilisé.

Pour ce faire, le responsable du traitement est tenu de sauvegarder les données par la constitution de copies de sécurité, et si nécessaire, de convertir les données pour un stockage pérenne.

5. L'organe chargé de la régulation en matière de protection des données personnelles : l'Autorité de Protection de Données à Caractère Personnel (APDCP)[43]

C'est l'article 64 du PLPDP qui institue[44] l'instance mauritanienne chargée de la protection des données à caractère personnel.

Il énonce, en effet : « Il est créé une Autorité de Protection des Données à caractère personnel, chargée de veiller à ce que les traitements des données à caractère personnel, en Mauritanie, soient mis en œuvre conformément aux dispositions de la présente Loi.

L'Autorité de Protection des Données à caractère personnel est une personne morale de droit public, indépendante, dotée de l'autonomie financière et de gestion. Elle est rattachée au Premier Ministre.

Elle informe les personnes concernées et les responsables de traitement de leurs droits et obligations et s'assure que les Technologies de l'Information et de la Communication ne comportent pas de menace au regard des libertés publiques et de la vie privée ».

---

[43] Pour la suite, « APDCP » désignera l'Autorité mauritanienne de protection des données à caractère personnel.

[44] La Loi mauritanienne relative aux données à caractère personnel n'ayant toujours pas été promulguée, il coule de source que l'Autorité de protection qui y est dédiée, puisqu'elle tire sa source de création du texte en question, n'est matériellement pas encore créée.

L'APDCP est composée des sept (7) membres inamovibles suivants, choisis pour un mandat, renouvelable une fois, de quatre (4) ans (art.67), en raison de leur compétence juridique et/ou technique (article 65 PLPDP) :

- Trois (3) personnalités qualifiées pour leurs connaissances et expériences dans les domaines du droit, de l'informatique et/ou des nouvelles technologies de l'information, désignées par le Président de la République ;
- Deux (2) personnalités désignées sur propositions respectives du président de l'Assemblée Nationale et du président du Sénat ;
- Un (1) magistrat désigné sur proposition du Ministre chargé de la justice ;
- Un (1) représentant des organisations de défense des droits de l'homme, désigné sur proposition des organisations de la Société Civile.

A l'image du législateur sénégalais, le législateur mauritanien entend adjoindre à la structure ainsi composée un Commissaire du Gouvernement, désigné par le Premier Ministre, qui siège auprès de l'Autorité de Protection des Données à Caractère Personnel, sachant que ce représentant du Gouvernement doit être convoqué à toutes les séances de l'Autorité, dans les mêmes conditions que les membres de celle-ci et qu' il rend compte à cette dernière des orientations du gouvernement et motivations de l'Administration concernant la mise en œuvre des traitements, même s'il ne prend pas part au vote de l'instance.

Il est curieux de constater que l'article 66, alinéa 2 prévoit que l'APDCP disposera d'un personnel mis à sa disposition par l'État, même s'il prévoit également – fort heureusement – qu'elle pourra pourvoir au recrutement d'agents en fonction des besoins de son fonctionnement ; cette mise à disposition de fonctionnaires par l'Etat nous semble en effet assez paradoxale, au regard de l'indépendance et de l'autonomie proclamées par l'article 64, alinéa 2, vu que déjà trois (3) des membres de l'organe sont désignés par le Président de la République et un (1), proposé par le Ministre de la Justice.

Remarque : A l'exception du Président, les autres membres de l'instance n'exercent pas leurs fonctions à titre exclusif.

Il est par contre heureux que selon l'article 71 du PLPDP, les membres de l'APDCP jouissent d'une totale immunité pour les opinions émises dans l'exercice ou à l'occasion de l'exercice de leur fonction (alinéa 1er) et que dans l'exercice de leurs attributions, ils ne reçoivent d'instructions d'aucune autorité.

Pour finir cette présentation, les attributions de l'APDCP, listées par l'article 73 du PLDP, sont identiques, dans leur substance, à des celles de ses homologues africaines et française.
Il en va de même des modalités de contrôles qu'elle peut être amenée à opérer et de son pouvoir de sanctions administratives et pécuniaires (articles 74 à 83), ainsi que des dispositions pénales (84 à 98).

B – Application effective dans le contexte socio-culturel mauritanien – Délimitation d'un "périmètre Données personnelles et Vie privée" : Mission difficile, voire à priori "Impossible" sans une AAI dotée d'un pouvoir coercitif étendu

Le cadre théorique posé par les textes mauritaniens qui auront vocation, dans un futur proche, voire imminent, à régir la Société Mauritanienne de l'Information et les différentes manifestations des interactions dont elle sera le théâtre, en général, donc, par voie de conséquence, les données à caractère personnel, en particulier, est cohérent dans son ensemble.
Mais les pays en voie de développement, dont aussi bien les administrations que les populations sont encore en train de parachever, chacun à son rythme et selon les réalités de son propre contexte, l'appropriation, le mûrissement et la consolidation des acquis issus des processus de démocratisation politique, administrative, culturelle et sociale qu'ils ont lancés, pour la plupart d'entre eux, au cours de ces trois (3) dernières, sont confrontés à une difficulté récurrente : celle de la transposition et de l'application effective des cadres législatifs et règlementaires qu'ils adoptent, étant donné que ces normes, commandés ou

juste suggérés par la mondialisation et le nouvel ordre qu'elle implique, sont souvent d'inspiration étrangère.

Pour être édifié sur le fait que nombre d'obstacles constitueront un rempart contre les nombreuses et nobles missions de l'organe qui sera chargé de la protection des données personnelles en Mauritanie, une succincte introspection rétrospective dans le microcosme social mauritanien et un bref aperçu de ce que sont les relations sociales dans ce pays, aujourd'hui seront, à nos yeux, assez éloquents.

B - 1 Les vestiges du passé

La Mauritanie est un pays caractérisé par une tradition de très forte oralité, or ce qui caractérise une civilisation orale est la forte propension des individus qui en sont les dépositaires, c'est que « tout se dit, tout se transmet » de bouche à oreille et pratiquement rien ne se consigne.

Sans prétendre pouvoir établir des profils sociologiques ou anthropologiques d'une société à dominante orale – nous en laissons le soin à des voix et plumes plus autorisées en la matière – nous pouvons cependant tenter de fournir des éléments tenant à l'histoire et à la géographie qui pourraient expliquer l'origine de ce mode de transmission ancestrale de la mémoire des mauritaniens.

La Mauritanie, pays désertique sur la plus grande partie de son territoire, est essentiellement composée de quatre (4) ethnies, à savoir les ouolofs (ou wolofs), les soninkés, les peulhs et les maures[45].

Les ouolofs, qui se sont toujours consacrées à l'agriculture et à la pêche, ainsi que les soninkés connus pour être de grands cultivateurs, sont sédentaires ; c'est d'ailleurs la raison

[45] L'on retrouve également, au centre et à l'est du pays des bambaras (provenant, à l'origine, du Mali, pays frontalier de la Mauritanie, pour la plupart), mais si ne nous les avons pas cités, c'est parce qu'ils se sont fortement métissés, depuis plusieurs générations, avec les peulhs et les maures.

pour laquelle ils se sont installés, à leur arrivée dans le pays[46] , dans la Région du Fleuve Sénégal.

Les peulhs et les maures, quant à eux, sont restés, depuis les temps ancestraux et jusqu'à une période très récente des nomades invétérés, allant au gré de leurs commerces et des transhumances de leurs cheptels, toujours à la recherche de nouveaux pâturages.

Leur mode de vie de l'époque (campements et bivouacs dans le désert), longues marches et processions étalées pendant de très longues durées, sans jamais rencontrer âme qui vive, font que lorsque des rencontres intra ou intergroupes se produisaient, elles donnaient lieu à d'interminables discussions, questions-réponses sur divers thèmes tels que l'état et la sécurité des routes – pour éviter les razzias et coupeurs de routes – la recherche de d'éléments de troupeaux égarés, perdus ou volés, les lieux les plus riches en pâturages, pour ne citer que ces exemples.

Aussi surprenant que cela puisse paraître, ces traits de caractère ont résisté aux siècles et ont même déteint sur les autres groupes sociaux, à la faveur des interpénétrations qui n'ont pas manqué de se faire dans tous les domaines de la vie, aussi bien par des alliances et liens de sang, que par l'existence d'autres centres d'intérêts communs.

B – 2 L'oralité, un code social constituant à la fois une vertu, un facteur d'inclusion et une présomption d'accomplissement social

En Mauritanie, les salutations prolifiques, les questionnements d'usage sur l'état de santé, la situation matérielle et les activités des uns et des autres, sans oublier de se renseigner sur leurs entourages, procède et participe de convenances sociales et d'une politesse traditionnelle, familière et coutumière voire rituelle non seulement admises, mais encouragées et généralisées. C'est ainsi que dans la société mauritanienne, certaines questions ou affirmations, qui choqueraient plus d'un, sous d'autres cieux, ne dérangent

[46] La Mauritanie, à l'origine ne serait qu'un vaste « No man's land » n'eût été les importantes activités caravanières sahéliennes et les conquêtes des empires almohades, almoravides et du Ghana, dont proviendraient les soninkés.

nullement ni la personne questionnée, ni un quelconque auditoire qui serait présent au moment où cette dernière serait interpelée.

Un autre trait de l'oralité mauritanienne réside dans le fait qu'une personne loquacité d'un individu est souvent assimilée et attribuée à sa sociabilité, sa capacité, même lorsqu'il ne se trouve pas dans les meilleures dispositions, à gérer son prochain avec une courtoisie « purement mauritanienne » et ce, en toutes circonstances, ce qui fait de lui « celui dont tout le monde cherche la compagnie » pour agrémenter les moments de détente et loisirs.

Un dernier attribut, non pas de la loquacité en tant que telle, mais de l'un de ses aboutissements – en l'occurrence la masse d'informations qui en résulte, le plus souvent – est que dans ce pays, l'appréciation que se font les gens du rang social ou du statut professionnel ou politique d'une personne dépend, dans une large mesure, des informations qu'il peut détenir sur des personnes, des faits ou des situations que forcément, il faut fréquenter une certaine « élite » pour y avoir accès.

Tout ceci pour dire que dans une société aujourd'hui encore très fortement marquée par cette empreinte indélébile de l'oralité, il relève, à notre avis, de la gageure que la protection des données personnelles devienne une réalité avec juste l'adoption de la Loi et la mise en place d'une autorité dédiée, sans, auparavant, abattre un énorme travail sur deux (2) plans au moins :

- Procéder à une sensibilisation de cette thématique importante, assidue et étendue à toutes les couches de la population ;

- Donner un contenu certain à la Loi et ses textes d'application en faisant des exemples concrets (sanctions à appliquer à tout contrevenant éventuel, qu'il s'agisse d'un responsable de traitement, d'un sous-traitant ou d'une personne sont les données personnelles sont traitées).

II – Interférences possibles et conflits d'autorités : L'autonomie d'une Autorité Administrative dédiée à la protection des données personnelles : REALITE OU UTOPIE ?

Au vu des éléments qui doivent caractériser toute autorité administrative indépendante (AAI), en l'occurrence une véritable indépendance et une autonomie complète, pour que ses prérogatives puissent s'exercer pleinement et sur la base de ce qui ressort de l'examen de certains textes mauritaniens – notamment ceux qui encadrent les activités de l'Autorité de Régulation Multisectorielle (ARE) et ceux de l'Agence Nationale du Registre des Populations et des Titres Sécurisés (ANRPTS), nous sommes sceptique quant au succès total de la mission de l'APDCP ; cette dernière, qui est en principe, d'après le texte légal qui la crée, est l'unique et exclusive entité appelée à s'assurer de la protection des données personnelles des citoyens mauritaniens, ne manquera pas, dans les faits, de se retrouver sur le terrain en concurrence avec deux autres institutions.

A – Prérogatives de l'ARE tirées de la règlementation sur les communications électroniques et du Projet de Loi mauritanienne sur la protection des données à caractère personnel : INTERACTIONS ENTRE L'ARE ET D'AUTRES AAI

Notre première inquiétude quant à l'indépendance de l'APDCP est soulevée la Loi N ° 2013-025 du 15 juillet 2013 portant sur les communications électroniques, dont le chapitre XII, relatif aux droits et protections des utilisateurs de réseaux et services de communications électroniques, comprend une section qui traite de la vie privée des usagers (section 1 du chapitre, articles 83 à 89) et une autre section, spécifique, elle, au traitement des données à caractère personnel (section 2 du chapitre, articles 90 à 95).

L'article 83 de la Loi N° 2013-025 enjoint aux opérateurs et leurs employés de « respecter le secret des correspondances par voie de communications électroniques et les conditions de la protection de la vie privée et des données nominatives des usagers, sous réserve des obligations relatives aux prescriptions exigées par la Défense Nationale et la Sécurité Publique et les prérogatives de l'autorité judiciaire ».

L’article 84, alinéa 1er, interdit, quant à lui, sur toute l’étendue du territoire national: l'interception, l'écoute, l'enregistrement, la transcription et la divulgation des correspondances émises par voie des communications électroniques sans autorisation préalable délivrée par le Procureur de la République ou par un juge d'instruction.

Reprenant en cela le PLPDP, l’article 89 dispose que « L'utilisation de systèmes automatisés d'appel et de messageries, de télécopieurs ou de courriers électroniques à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable ».

Pour citer quelques exemples spécifiques à la section de la Loi N ° 2013-025 qui encadrent le traitement des données à caractère personnel, dans le cadre de la fourniture au public de services de communications électroniques et des réseaux qui prennent en charge les dispositifs de collecte de données et d'identification. retenons que :

- l’article 91 pose le principe que « les opérateurs doivent effacer ou rendre anonyme toute donnée relative au trafic », sauf pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales et pour les besoins de l'ordre public, la défense nationale et la sécurité publique (article 92) ;
- l’article 93 prévoit que « pour les besoins de la facturation et du paiement des prestations de communications électroniques, les opérateurs peuvent, jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement, utiliser, conserver et, le cas échéant, transmettre certaines catégories de données techniques à des tiers concernés directement par la facturation ou le recouvrement » (alinéa 1er),

et qu’ils « peuvent en outre réaliser un traitement des données relatives au trafic en vue de commercialiser leurs propres services de communications électroniques ou de fournir des services à valeur ajoutée, si leurs clients y consentent expressément et pour une durée déterminée. Cette durée ne peut, en aucun cas, être supérieure à la période nécessaire pour

la fourniture ou la commercialisation de ces services », tout comme « Ils peuvent également conserver certaines données en vue d'assurer la sécurité de leurs réseaux » (alinéa 2).
- l'article 95, enfin, précise que les données susceptibles d'être conservées et traitées par les opérateurs « portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux », et ne sauraient en aucun cas, « porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications ».

Notre deuxième appréhension résulte, elle, de l'article 58, alinéa 1, 1° du PLPDP, qui dispose que lorsqu'un traitement intéresse la sûreté de l'Etat, la défense nationale ou la sécurité publique, le droit d'accès doit être exercé par une demande adressée à l'Autorité de Protection des Données à caractère personnel, qui désigne l'un de ses membres appartenant ou ayant appartenu à la Cour Suprême pour mener les investigations nécessaires mais que ce magistrat « peut se faire assister d'un agent de l'Autorité de Régulation Multisectorielle ».

Il ne fait pas de doute que même si l'Autorité de Régulation Multisectorielle ne constitue pas forcément de menace ou de facteur de blocage à l'action de l'APDCP, il n'en demeure pas moins que le législateur a tout même créé les conditions d'un conflit de compétences manifeste ou, à tout le moins, d'empiètements de l'une des institutions sur l'autre, surtout que l'on sait que les communications électroniques et services qui y sont rattachés constituent la chasse gardée « souveraine et exclusive » du régulateur multisectoriel.

B – Traitement et exploitation des données – Intérêt Général Versus Intérêts Individuels & Vie Privée - Cas de l'ANRPTS / ETAT CIVIL : FICHIER CENTRAL ? CONTRÔLE ET SUPERVISION OU SURVEILLANCE ?

L'Agence Nationale du Registre des Populations et des titres sécurisés est créée par la Loi N ° 2011-003 du 12 janvier 2011 abrogeant et remplaçant la Loi N ° 96-019 du 19 juin 1996 portant Code de l'Etat Civil.

Cette loi, au terme de son article premier (1er), « organise et détermine les conditions et les procédures obligatoires de déclaration, d'enregistrement des évènements d'Etat Civil ainsi que celles relatives à la délivrance des actes sécurisés qui en découlent », de même qu' « elle s'applique à tous les citoyens Mauritaniens et aux étrangers résidents ou de passage en Mauritanie ».

Son article 2, alinéa 1er, énonce qu' «« il est institué un « Regsitre National des Populations » (RNP) qui contient l'ensemble des éléments biographiques et biométriques qui identifient un individu » et l'alinéa 2 du même article précise qu' « il intègre les informations relatives à la naissance, au mariage, au divorce et au décès ainsi que les empruntes digitales, les données de reconnaissance faciale, la photographie et toutes autres données ou mentions utiles à l'identification d'une personne » ».

Il faut d'abord signaler la masse exorbitante d'informations et de données que, dans la pratique, collecte l'ARNPTS.
Nombre de fois, pour nombre de pièces dont ils demandaient à se faire servir des extraits ou expéditions, des citoyens se sont vu notifier que la délivrance des documents demandés était subordonnée à la présentation de documents et justificatifs de données pourtant déjà en possession de l'institution, puisqu'ils émanaient de ses services.
Ce « déluge d'informations requises (!)» nous fait penser à quelques réflexions Gilles Dounès[47] au sujet des données personnelles: « L'enjeu principal est la maitrise, au sens de la compréhension, la plus pointue possible, des individus et des groupes par des institutions qui ont un intérêt à pouvoir influer sur ces comportements, qu'il s'agisse de commerçants grands ou petits, de gouvernements qu'ils soient totalitaires ou démocratiques, ou même de groupes sectaires comme DAESH qui peuvent tout à fait à terme avoir accès à ce type de technologie et surtout à leur exploitation ».

[47] Gilles Dounès est Directeur de la Rédaction du site MacPlus.net qui couvre l'actualité d'Apple depuis septembre 1997.
Il est le co-auteur avec Marc Geoffroy d'iPod Backstage, les coulisses d'un succès mondial, paru en 2005 aux Editions Dunod.

« « Un jour peut-être, il faudra se poser la question de savoir pourquoi une simple application sur Smartphone (lampe de poche, jeux ...) a besoin d'accéder à l'historique de vos appareils, de vos applications, de votre position spatiale, à vos photos personnelles, votre camera, votre micro d'enregistrement, à vos SMS… La liste est souvent longue… Un nouveau marché se profile à l'horizon : « payer pour ne pas communiquer ses métadonnées» ».

C'est dire combien les principes de finalité et de proportionnalité semblent, dans ce cas précis, ignorés, pire « bafoués ».

En effet, la première mesure administrative que l'ANRPTS a prise, lors de sa création, a été un recensement de toute la population au niveau des guichets de ses centres d'accueil des citoyens (CAC)[48].

S'étant appropriée le rôle et la fonction traditionnels des mairies (Etat Civil), elle a repris à son compte l'une des prérogatives les plus souveraines de la Direction Générale de la Sûreté, la délivrance des passeports et est en train, à ce jour, de mettre en place des moyens techniques et dispositifs destinés à éditer les permis de conduire qui relèvent, pour l'instant, du Ministère de l'Equipement et des Transports.

Cela dit, quatre (4) dispositions de la Loi organique 2011-003 (qui a créé l'ANRPTS) nous paraissent représenter des violations manifestes des principes sous-tendant la protection des données à caractère personnel ; il s'agit de ses articles 31, 32, 38 et 48.

L'article 31 dispose qu' « Aucune rectification ne peut être apportée aux actes d'état civil, après leur délivrance, que sur décision judiciaire ayant force de la chose jugée » et qu' « en aucun cas, les rectifications ne peuvent porter sur :

Le Numéro National d'Identification (NNI) ;

Les dates de naissances, de mariage, de « Talaq » [49] ou de « Tatliq »[50] et des décès ».

---

[48] Les centres d'accueil des citoyens sont les agences décentralisées de l'ANRTPS, à la tête de chacune d'entre elles se trouvant un chef de centre ayant la qualité d'Officier d'Etat Civil.

[49] Divorce prononcé unilatéralement par le mari

[50] Divorce prononcé par le CADI ou Juge de juridiction musulmane

L'article 32, in fine, ensuite, énonce que sauf exception édictée par la Loi, « aucune contestation n'est recevable auprès du Responsable du centre d'Accueil des Citoyens ».

Si l'on en croit l'article 38, si une femme mère célibataire ou veuve décède avant d'avoir procédé à la déclaration de naissance de son enfant, ce dernier « est déclaré par toute personne diligente qui lui choisit un prénom », mais « le nom de famille de l'enfant est attribué par l'officier d'état civil ».

Les actes de « TALAQ » et de « TATLIQ » (divorce) doivent énoncer, selon la lettre de l'article 48 de la Loi N ° 2011-003, entre autres éléments :

- la situation de la femme « par rapport à la grossesse »
- et « « les fondements et références sur lesquels l'acte de « TALAQ » ou « TATLIQ » a été établi » ».

CONCLUSION PONCTUELLE : QUESTIONNEMENTS / ENSEIGNEMENTS A TIRER / PERSPECTIVES EVENTUELLES ?

La discussion théorique autour de laquelle s'est articulée notre réflexion, l'opportunité de confier la protection des données à caractère personnel au régulateur multisectoriel mauritanien (l'ARE), à une instance ad' hoc ou à une autorité administrative indépendante à créer nous semble loin d'être terminée, tellement l'approche que nous avons choisie pour la mener, c'est-à-dire un regard croisé sur l'analyse des différents systèmes règlementaires d'encadrement des données personnelles, leurs applications possibles ou effectives et l'observation de quelques pratiques en rapport avec le sujet, met en évidence les limites, voire les incapacités d'un quelconque régulateur à assurer, à lui seul, la mise en place et la pérennité d'un cadre adéquat à la protection des données personnelles.

C'est la raison pour laquelle, pouvons-nous, tout au plus, essayer « d'esquisser » une synthèse de quelques enseignements que nous pouvons en tirer et des implications, en matière de politique(s) des données à caractère personnelles qu'ils appellent selon nos convictions.

Nous avons vu, dans le corps de texte de notre étude, que la régulation des communications électroniques est passée par plusieurs phases, s'étant d'abord focalisée sur les infrastructures, avant de s'intéresser à la concurrence qui se joue sur les services des opérateurs, et qu'aujourd'hui, les régulateurs ont pris conscience des nombreux et cruciaux enjeux représentés par les contenus confondus de ces services, de plus en plus pointus, personnalisés et affinés.
Or le corollaire logique de la spécialisation et de la segmentation des activités sujettes à la régulation est une spécialisation tout aussi poussée des régulateurs.
Il faut malheureusement constater, à ce sujet que l'Autorité de Régulation Multisectorielle mauritanienne (l'ARE) qui a certes capitalisé, de sa création en 2001, à nos jours, une expertise certaine dans la régulation des secteurs dont elle a la charge (communications électroniques, poste, eau et électricité), ne dispose ni d'équipes spécialisées dans la traque des contrevenants du numérique, en général, et de l'internet en particulier (capacité à établir des croisements et recoupements en matière de cookies, par exemple), ni de laboratoires équipés en conséquence.
Nous supposons que ce n'est pas le cas du régulateur ivoirien, qui lui, s'est vu rajouter la compétence de régulation des données personnelles.

Dans le même ordre d'idées, il est déplorable que les textes organiques relatifs à la composition des membres de l'Autorité de Protection des Données à caractère personnel se soient contentés d'adjoindre à cette dernière des « personnalités qualifiées pour leurs connaissances et expériences dans les domaines du droit, de l'informatique et/ou des nouvelles technologies de l'information », sans lui associer une structure mise en place et fonctionnelle depuis plus d'une décennie et équipée de spécialistes férus de l'informatique et des nouvelles technologies : la Direction Générale de la Modernisation de l'Administration.

Cette question de renforcement des compétences étant posée, citons ici trois (3) constats majeurs sur la réalité, pas toujours bien cernée par le grand public, des données personnelles, avant de proposer les quelques pistes que nous suggère la thématique.

▫ Tel que le souligne Daniel Kaplan[51] , de la Fédération Internet Nouvelle Générale (FING), il existe un déséquilibre profond entre les énormes capacités de surveillance et de traçage des individus, par les autorités (cas des pouvoirs exorbitants de l'ANRPTS, cité dans notre étude) et le peu de pouvoir qu'ont les individus eux-mêmes sur leurs propres données d'autre part.

[51] Voir article de Daniel Kaplan, dans « Informatique, Libertés, Identités », « La valeur de la vie privée, c'est de nous permettre d'avoir une vie publique ! », http://fing.org/?InformatiqueLibertesIdentites.

▫ La régulation s'opère selon les mêmes lois et critères qui président à la « sélection naturelle des espèces ». C'est ce que s'évertue à démontrer le Professeur Jean FRAYSSINET[52] quand il soutient que dans un contexte donné, des formes variées de régulation sont en compétition (c'est le cas de l'ARE, de l'ANRPTS et de l'APDCP à venir !) avec leurs caractéristiques propres et seules les plus adaptées l'emportent.
Par conséquent, il ne faut pas envisager la régulation sous l'angle d'une compétition mais plutôt sous celui d'une franche et fertile interaction des différents acteurs concernés, chacun d'entre eux et chaque niveau de régulation ayant leur importance.

▫ La protection des données personnelles des individus, en général et celle de leurs identités numériques dans une société informatisée, en particulier, ne peut être assurée que par une savante alchimie entre les pratiques, la technique, la législation, l'éducation, l'éducation et encore l'éducation « numérique », aussi bien des citoyens que de leurs dirigeants.

Ci-après trois (3) pistes, parmi tant d'autres, que les pouvoirs publics devraient, à notre sens, intégrer :

■ « Démocratiser » la technologie, c'est-à-dire faire en sorte que le « pouvoir » des technologies soit partagé entre les Administrations et les administrés, en fournissant à ces derniers les moyens éducatifs, techniques et matériels de se mettre au même niveau que les services administratifs et les organisations qui veulent en savoir plus sur eux.

Il s'agit par exemple, dans un contexte comme celui dans lequel l'ANRPTS est toute puissante, de « surveiller les surveillants ! »[53] , c'est-à-dire exiger de ceux qui obtiennent des informations des individus, de donner en retour des informations sur eux-mêmes et sur leurs pratiques (Une sorte de « donnant-donnant », régulé par les autorités publiques et/ou par l'intelligence collective des citoyens-consommateurs).
Les spécialistes de l'institut Demos écrivent, dans une étude relative au sujet, que "la question n'est pas de savoir si nous entrons dans une société dominée par la surveillance, mais s'il en résulte davantage, ou moins, de contrôle des individus sur leur propre vie, ainsi que sur les décisions d'intérêt collectif." ;

---

[52] Jean Frayssinet, Agrégé des Universités, Faculté de Droit d'Aix-en-Provence, Expert en protection des données personnelles, Membre de la Commission de contrôle des fichiers d'INTERPOL.
[53] GROUPE "INFORMATIQUE & LIBERTES 2.0 ?", « LE NOUVEAU PAYSAGE DES DONNEES PERSONNELLES :QUELLES CONSEQUENCES SUR LES DROITS DES INDIVIDUS ? », Note de travail, Janvier 2009, par Daniel Kaplan, Charles Nepote, Vincent Toubiana et 9 autres auteurs, IDENTITES ACTIVES.NET, FING.

■ Articuler la régulation des données à caractère personnel autour de la convergence des organes de régulation existants - l'ARE et la seconde (pseudo-régulateur de fait), l'ANRPTS, dans notre cas – en ne perdant pas de vue, comme attire dessus l'attention Patrick WAELBROECK qu'il ne peut y avoir de « convergence des instances de régulation sans refonte importante des mécanismes de régulation » ;

■ Envisager la nécessaire création d'une structure permanente consacrée au « Numérique » comprenant en son sein un pool de métiers liés à la recherche, la veille, la formation, la sensibilisation et la production législative et/ou réglementaire dans le domaine du numérique et de l'internet.

■ Envisager, enfin, dans le cas où la proposition précédente prendrait corps, puisque c'en est une conséquence directe, le recours à l'autorégulation par ladite structure permanente.

Cette proposition s'explique surtout par le fait que, de l'avis général, notamment de l'AFAPDP, les tendances pour l'avenir, auxquelles l'Afrique, dans sa globalité et la Mauritanie ne sauraient échapper, vont :

- Au renforcement des outils de mise en conformité (régulation en amont) et des pouvoirs de contrôle à postériori et des sanctions ;

- Au renforcement des mécanismes d'harmonisation et de coopération internationale ;

- Au travail en commun avec d'autres régulateurs du monde numérique.

En définitive, nous pouvons soutenir que quelle soit la tournure sous laquelle la thématique des données à caractère personnel est présentée, sa problématique ne se résume qu'à une seule question : Comment concilier démocratie, technologie et droits des personnes ?

Si nous devions, pour notre part, émettre une conclusion ponctuelle sur l'encadrement des données personnelles en Mauritanie, elle consisterait :

- Soit à amender les textes législatifs et règlementaires organiques de l'Agence Nationale du Registre de la Population et des Titres Sécurisés, de manière à donner toute leur légitimité, toute leur contenance et toute leur force aux leviers théoriquement réservés à l'Autorité de Protection des Données à Caractère Personnel ;

- Soit à consacrer le principe de compétences partagées entre toutes les Autorités existantes (ARE, Autorités des Marchés Publics, des Transports, de la Presse et de l'Audiovisuel, etc.) en délimitant, pour chacune d'entre elles, un champ d'application strictement confiné des

questions de données personnelles qui les interpellent. Dans ce cas, bien entendu, chaque structure aura son propre département « Protection des données personnelles » du secteur qu'elle régule ;

- Soit, enfin, créer une commission Ad' hoc qui se réunirait non seulement selon une périodicité convenue (une fois par semaine ou par mois) et de manière ponctuelle, en fonction du signalement des atteintes et violations avérées des données à caractère personnel d'une certaine gravité.

Cette commission serait constituée par une équipe comprenant, idéalement, des experts juristes et techniciens de tous les régulateurs et de tous les départements ministériels.

Au terme de cette brève étude, qui ne fait que lancer les bases de futures discussions que nous espérons fertiles en Mauritanie, il subsiste une question inévitable : Malgré tous les efforts d'encadrement et de protection qui sont et ne finiront jamais d'être mis en œuvre de par le monde, la vitesse à laquelle s'accroissent les capacités de traitements et la performance toujours plus accrue des outils et supports qui rendent possibles ces traitements n'auront-ils pas pour résultat un jour, « la mort des données personnelles ?

En attendant d'avoir une réponse à cette question, une chose est certaine : Toute personne représente, en réalité, le meilleur régulateur de ses propres données, car elle doit s'attacher à une génération, une exploitation, une conservation et une communication efficaces et sûres de ses données.

- ANNEXE UNIQUE -

PROJET DE LOI RELATIF AUX DONNEES A CARACTERE PERSONNEL

REPUBLIQUE ISLAMIQUE DE MAURITANIE

Honneur-Fraternité-Justice

Le Premier Ministère

PROJET DE LOI SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

EXPOSÉ DES MOTIFS

Depuis la mise en place d'institutions démocratiques garantissant les libertés individuelles et le respect de la vie privée des citoyens, aucune disposition juridique n'envisageait l'encadrement de la protection des données à caractère personnel.

Ce contexte a ainsi créée un vide juridique empêchant toute forme de sanction sur les atteintes à la vie privée mais aussi laissant les citoyens dans l'insécurité pour toutes les données liées à leur vie privée.

Ce projet de texte ne remet pas en cause le cadre aménagé par la Lloi N° 2011-003 abrogeant et remplaçant la loi n° 96-019 du 19 juin 1996 portant Code de l'état civil, ni le régime prévu s par le Décret n° 2010-150 portant création, organisation et fonctionnement de l'Agence Nationale du Registre des Populations et des Titres Sécurisés (ANRPTS).

Une législation spécifique dans ce domaine aura pour vocation de fixer le cadre juridique global de la mise en œuvre de toute forme de traitement de données à caractère personnel, en posant de manière expresse les différents mécanismes et les droits des personnes concernées par le traitement de ces données.

Ce projet de loi a pour objectif de :

- renforcer la sécurité publique et les droits des citoyens ;
- Protéger contre les atteintes à la vie privée.

Telle est l'économie du présent projet de loi soumis à votre approbation.

Le Premier Ministre

Yahya Ould Hademine

REPUBLIQUE ISLAMIQUE DE MAURITANIE

Honneur-Fraternité- Justice

PRESIDENCE DE LA REPUBLIQUE

Visa :

DGLTE/JO

Projet de loi n° _____ relative à la protection des données à caractère personnel.

CHAPITRE PREMIER : DES DISPOSITIONS GENERALES

Section 1 : De l'objet de la présente Loi

Article Premier

Sans préjudice des dispositions de la Loi n° 2011-003 abrogeant et remplaçant la Loi n° 96-019 du 19 juin 1996, portant code d'état civil et ses textes d'application, la présente Loi a pour objet de mettre en place un cadre normatif et institutionnel sur le traitement de données à caractère personnel, en vue de garantir de meilleurs services, de prévenir et de lutter contre les atteintes à la vie privée susceptibles d'être occasionnées par l'utilisation des Technologies de l'Information et de la Communication.

Elle pose les conditions dans lesquelles tout traitement portant sur des données à caractère personnel, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des citoyens.

Section 2 : Des définitions

Article 2

Au sens de la présente Loi, on entend par :

1. **Communication électronique :** toute émission transmission, ou réception de signes, de signaux, d'écrit, d'images ou de son par voie électromagnétique, telle que définie par la loi n°2013-025 portant sur les communications électroniques.
2. **Code de conduite :** tout ensemble de règles, notamment les chartes d'utilisation, élaboré par le responsable du traitement, en conformité avec la

présente Loi, afin d'instaurer un usage correct des ressources informatiques, de l'Internet et des communications électroniques de la structure concernée et homologué par l'Autorité de Protection des Données à caractère personnel ;

3. **Consentement de la personne dont les données à caractère personnel font l'objet d'un traitement :** toute manifestation de volonté expresse, non équivoque et libre, par laquelle la personne concernée ou son représentant légal, accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique ;
4. **Copies temporaires :** données copiées temporairement dans un espace dédié, pour une durée limitée dans le temps, pour les besoins du fonctionnement du logiciel de traitement ;
5. **Donnée à caractère personnel :** toute information, quel que soit son support et de quelque nature qu'elle soit, y compris le son et l'image, relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ;
6. **Donnée génétique :** toute information concernant les caractères héréditaires d'un individu ou d'un groupe d'individus apparentés ;
7. **Donnée sensible :** toute information relative aux opinions ou activités religieuses, philosophiques, politiques, syndicales, à la vie sexuelle, à la race, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives ;
8. **Donnée dans le domaine de la santé :** toute information concernant l'état physique et mental d'une personne donnée ;
9. **Fichier de données à caractère personnel** : tout ensemble structuré de données à caractère personnel, accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ;
10. **Interconnexion des données à caractère personnel :** la mise en relation de données à caractère personnel traitées, pour une finalité déterminée, avec d'autres données traitées à des finalités identiques ou non ;
11. **Pays tiers :** tout Etat autre que la République Islamique de Mauritanie ;

12. **Responsable du traitement :** la personne physique ou morale, publique, privée ou tout autre structure ou association qui, seule ou conjointement avec d'autres, prend la décision de collecter et de traiter des données à caractère personnel ;
13. **Sous-traitant :** toute personne physique ou morale, publique ou privée, tout autre organisme ou association qui traite des données pour le compte du responsable du traitement ;
14. **Traitement des données à caractère personnel :** toute opération ou ensemble d'opérations effectuées à l'aide de procédés automatisés ou non, et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction.

Section 3 : Du champ d'application

Article 3

Le champ d'application de la présente Loi sur les données à caractère personnel comprend :

1. tout traitement de données à caractère personnel, effectué par une personne physique, par l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé ;
2. tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier, à l'exception des traitements mentionnés à l'article 4 de la présente Loi ;
3. tout traitement mis en œuvre par un responsable sur le territoire mauritanien ou en tout lieu où la loi mauritanienne s'applique ;
4. tout traitement mis en œuvre par un responsable, établi ou non sur le territoire mauritanien, qui recourt à des moyens de traitement situés sur le territoire national, à l'exclusion des moyens qui ne sont utilisés qu'à des fins de transit ;
5. tout traitement des données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, même liées à un intérêt quelconque de l'Etat, sous réserve des dérogations que prévoit la

présente Loi et des dispositions spécifiques en la matière fixées par d'autres lois ;

Article 4

Les dispositions de la présente Loi sur les données à caractère personnel ne s'appliquent pas :

1. aux traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques, à condition toutefois que les données ne soient pas destinées à une communication non autorisée à des tiers ou à la diffusion ;
2. aux copies temporaires faites dans le cadre des activités techniques de transmission et de fourniture d'accès à un réseau numérique, en vue du stockage automatique, intermédiaire et transitoire des données et à seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

CHAPITRE II : DES PRINCIPES FONDAMENTAUX RELATIFS AUX TRAITEMENTS DES DONNEES PERSONNELLES

Section 1: Des principes de base relatifs au traitement des données à caractère personnel

Article 5

Le traitement des données à caractère personnel effectué sans le consentement de la personne concernée, est interdit.

Toutefois, il peut être dérogé à cette exigence du consentement, lorsque le traitement est nécessaire :

1. au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
2. à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;
3. à l'exécution d'un contrat auquel la personne concernée est partie ;
4. à la sauvegarde de l'intérêt ou des droits et libertés fondamentaux de la personne concernée.

Article 6

La collecte, l'enregistrement, le traitement, le stockage et la transmission des données à caractère personnel doivent se faire de manière licite, loyale et non frauduleuse.

Article 7

Les données à caractère personnel doivent être collectées pour des finalités déterminées, explicites et légitimes et ne peuvent pas être traitées ultérieurement de manière incompatible avec les finalités prédéfinies.

Elles doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et traitées ultérieurement.

Elles doivent être conservées pendant une durée qui n'excède pas la période nécessaire aux finalités pour lesquelles elles ont été collectées ou traitées.

Au-delà de cette durée, les données à caractère personnel ne peuvent faire l'objet d'une conservation qu'en vue de répondre spécifiquement à un traitement à des fins historiques, statistiques ou de recherches en vertu des dispositions légales.

Article 8

Les données à caractère personnel collectées doivent être exactes et, si nécessaire, mises à jour. Toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et traitées, soient effacées ou rectifiées.

Article 9

Le traitement des données à caractère personnel s'effectue conformément au principe de transparence qui implique une information obligatoire de la part du responsable de leur traitement..

Article 10

Les données à caractère personnel sont traitées de manière confidentielle et sont protégées conformément aux dispositions de l'article 47 de la présente Loi, notamment lorsque le traitement comporte des transmissions de données dans un réseau.

Article 11

Tout traitement de données à caractère personnel effectué pour le compte du responsable du traitement doit être régi par un acte juridique consigné par écrit qui lie le sous-traitant au responsable du traitement et qui prévoit notamment que le sous-traitant n'agit que sur la seule instruction du responsable du traitement et que les obligations prévues par la présente Loi incombent également à celui-ci.

Dans le cadre de la sous-traitance pour des activités liées au traitement de données, toute personne participant à l'exécution de la mission est soumise à l'obligation de confidentialité.

Section 2 : Des principes spécifiques au traitement de certaines catégories de données à caractère personnel

Article 12

Il est interdit de procéder à la collecte et à tout traitement qui révèlent l'origine raciale, ethnique, linguistique ou régionale, la filiation, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, la vie sexuelle, les données génétiques ou plus généralement celles relatives à l'état de santé de la personne concernée.

Article 13

L'interdiction fixée à l'article précédent ne s'applique pas pour les catégories de traitement suivantes :

1. Lorsque le traitement des données à caractère personnel porte sur des données manifestement rendues publiques par la personne concernée elle-même ;
2. Lorsque la personne concernée a donné son consentement par écrit, quel que soit le support, à un tel traitement ;
3. Lorsque le traitement des données à caractère personnel est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique, mentale ou juridique de donner son consentement ;
4. Lorsque le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
5. Lorsqu'une procédure judiciaire ou une enquête pénale concernant la personne concernée est ouverte ;
6. Lorsque le traitement des données à caractère personnel s'avère nécessaire pour un motif d'intérêt public notamment à des fins historiques, statistiques ou scientifiques ;
7. Lorsque le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ;
8. Lorsque le traitement est nécessaire au respect d'une obligation légale ou réglementaire à laquelle le responsable du traitement est soumis ;

9. Lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public, ou est effectué par une autorité publique, ou est assigné par une autorité publique au responsable du traitement ou à un tiers, auquel les données sont communiquées ;
10. Lorsque le traitement est effectué dans le cadre des activités légitimes d'une fondation, d'une association ou de tout autre organisme à but non lucratif et à finalité politique, philosophique, religieuse, mutualiste ou syndicale. Toutefois, le traitement doit se rapporter aux seuls membres de cet organisme ou aux personnes entretenant avec lui des contacts réguliers liés à sa finalité et que les données ne soient pas communiquées à des tiers sans le consentement des personnes concernées.

Article 14

Le traitement des données à caractère personnel relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être mis en œuvre que par :

1. les juridictions, les autorités publiques et les personnes morales gérant un service public, agissant dans le cadre de leurs attributions légales ;
2. les auxiliaires de justice pour les stricts besoins de l'exercice des missions qui leur sont confiées par la Loi.

Article 15

Le traitement des données à caractère personnel à des fins de santé n'est légitime que :

1. lorsque la personne concernée a donné son consentement ;
2. lorsqu'il porte sur des données manifestement rendues publiques par la personne concernée ;
3. lorsqu'il est nécessaire à la défense des intérêts vitaux de la personne concernée ou d'une autre personne, dans le cas où celle-ci se trouve dans l'incapacité physique, mentale ou juridique de donner son consentement ;
4. lorsqu'il est nécessaire à la réalisation d'une finalité fixée par la loi ;
5. lorsqu'il est nécessaire à la promotion et à la protection de la santé publique, au moyen d'un dépistage, par exemple ;
6. lorsqu'il est nécessaire à la prévention d'un danger certain ou à la répression d'une infraction pénale déterminée ;

7. lorsqu'il est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
8. lorsqu'il est nécessaire à des fins de médecine préventive, de diagnostics médicaux, de l'administration de soins ou de traitements, soit à la personne concernée, soit à son parent ou lorsque les services de santé agissent dans l'intérêt de la personne concernée.

Article 16

Les données à caractère personnel relatives à la santé sont collectées auprès de la personne concernée. Elles ne peuvent être collectées auprès d'autres sources qu'à condition que la collecte soit nécessaire aux fins du traitement ou que la personne concernée ne soit pas en mesure de fournir les données elle-même.

Article17

Le traitement des données à caractère personnel réalisé aux fins de journalisme, de recherche ou d'expression artistique ou littéraire est admis, lorsqu'il est mis en œuvre aux seules fins d'expression littéraire et artistique ou d'exercice, à titre professionnel, de l'activité de journaliste ou de chercheur, dans le respect des règles déontologiques, législatives ou réglementaires de ces professions.

Les dispositions de la présente Loi ne font pas obstacle à l'application des dispositions des lois relatives à la presse écrite ou audiovisuelle et du code pénal.

Article 18

Il est interdit de procéder à la prospection directe à l'aide de tout moyen de communication utilisant, sous quelque forme que ce soit, les données à caractère personnel d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir de telles prospections.

Les données à caractère personnel ne sont communiquées à des tiers, ou utilisées à des fins de prospection, que dès lors que la personne concernée a formellement exprimé son accord.

Article 19

Aucune décision de justice impliquant une appréciation sur le comportement d'une personne, ne peut avoir pour fondement un traitement automatisé des données à caractère personnel destiné à évaluer certains aspects de sa personnalité.

Aucune décision, produisant des effets juridiques à l'égard d'une personne, ne peut être prise sur le seul fondement d'un traitement automatisé des données à caractère personnel destiné à définir le profil de l'intéressé ou à évaluer certains aspects de sa personnalité.

Section 3 : Des principes spécifiques au transfert des données à caractère personnel vers un pays tiers

Article 20

Le responsable d'un traitement ne peut transférer des données à caractère personnel vers un pays tiers que si cet Etat assure un niveau de protection suffisant de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font ou peuvent faire l'objet.

Article 21

L'Autorité de Protection des Données à caractère personnel publie et tient à jour la liste des Etats qu'elle considère comme offrant un niveau de protection suffisant de la vie privée, des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel.

Article 22

Avant tout transfert des données à caractère personnel vers un pays tiers ne figurant pas sur cette liste, le responsable du traitement doit préalablement informer l'Autorité de Protection des Données à caractère personnel.

Le transfert de données à caractère personnel ne peut se faire que selon les conditions et règles de procédure arrêtées par l'Autorité de Protection des Données à caractère personnel.

Article 23

Le caractère suffisant du niveau de protection d'un pays tiers s'apprécie en fonction, notamment, des mesures de sécurité qui y sont appliquées, conformément à la présente Loi, des caractéristiques propres du traitement, telles que ses finalités, sa durée ainsi que de la nature, de l'origine et de la destination des données traitées.

Article 24

Le responsable d'un traitement peut transférer des données à caractère personnel vers un pays tiers ne répondant pas aux conditions prévues à l'article 21 de la présente Loi, si le transfert est ponctuel, non massif et que la personne à laquelle se rapportent les données a consenti expressément à leur transfert ou si le transfert est nécessaire à l'une des conditions suivantes :

1. à la sauvegarde de la vie de cette personne ;
2. à la sauvegarde de l'intérêt public ;
3. au respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice ;
4. à l'exécution d'un contrat entre le responsable du traitement et l'intéressé.

Article 25

L'Autorité de Protection des Données à caractère personnel peut autoriser, sur la base d'une demande dûment motivée, un transfert ou un ensemble de transferts de données vers un pays tiers n'assurant pas un niveau de protection adéquat, lorsque le responsable du traitement offre des garanties suffisantes au regard des dispositions de la présente Loi. Ces garanties peuvent notamment résulter de clauses contractuelles appropriées ou des règles internes dont il fait l'objet.

.

Section 4 : Des interconnexions des fichiers comportant des données à caractère personnel

Article 26

L'interconnexion de fichiers portant sur des données à caractère personnel constitue un traitement au sens du point 14 de l'article 2 de la présente Loi.

Article 27

L'interconnexion de fichiers relevant d'une ou de plusieurs personnes morales gérant un service public, et dont les finalités correspondent à des intérêts publics différents, doit faire l'objet d'une autorisation de l'Autorité de Protection des Données à caractère personnel.

Il en est de même pour les traitements mis en œuvre par l'Etat aux fins de mettre à la disposition des usagers de l'Administration un ou plusieurs services à distance dans le cadre de l'administration électronique.

Article 28

L'interconnexion de fichiers relevant de personnes privées et dont les finalités principales sont différentes, est également soumise à autorisation de l'Autorité de Protection des Données à caractère personnel.

Article 29

Toute interconnexion des fichiers doit permettre d'atteindre des objectifs légaux ou statutaires présentant un intérêt légitime pour les responsables des traitements et des bénéficiaires ou usagers.

Elle ne peut pas entraîner de discrimination ou de réduction des droits, libertés et garanties pour les personnes concernées, ni être assortie de mesures de sécurité appropriées et doit tenir compte du principe de pertinence des données faisant l'objet de l'interconnexion.

Article 30

La demande d'autorisation d'interconnexion comprend toutes les informations nécessaires sur :

1. la nature des données à caractère personnel relatives à l'interconnexion ;
2. la finalité pour laquelle l'interconnexion est considérée nécessaire ;
3. la durée pour laquelle l'interconnexion est souhaitée ;
4. et toute autre information utile à la prise de décision.

Article 31

La demande d'autorisation d'interconnexion ainsi que les autorisations d'interconnexion sont inscrites sur le répertoire des traitements.

CHAPITRE III - DES FORMALITES PREALABLES AU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

Section 1 : Des dispenses de formalités

Article 32

Sont dispensés de toutes les formalités préalables à un traitement des données à caractère personnel quel que soit le support à un tel traitement en conformité avec les textes en vigueur, les traitements :

1. mentionnés à l'article 4 de la présente Loi ;
2. les traitements ayant pour seul objet la tenue d'un registre qui, en vertu de dispositions législatives ou réglementaires, est destiné exclusivement à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime ;
3. les traitements mis en œuvre par une association ou tout organisme à but non lucratif et à caractère religieux, philosophique, politique ou syndical dès lors que ces données correspondent à l'objet de cette association ou de cet organisme, qu'elles ne concernent que leurs membres et qu'elles ne doivent pas être communiquées à des tiers.
4. Réalisés avec le consentement par écrit de la personne concernée.

Section 2 : Du régime de déclaration

Article 33

Tous les traitements de données, en dehors des cas prévus aux articles 32 et 37 de la présente Loi, doivent faire l'objet d'une déclaration auprès de l'Autorité de Protection des Données à caractère personnel.

La déclaration, conforme à un modèle établi par l'Autorité de Protection des Données à caractère personnel, comporte l'engagement que le traitement satisfait aux exigences de la Loi.

L'Autorité de Protection des Données à caractère personnel atteste, par un accusé de réception, que la déclaration requise a bien été faite et délivre immédiatement un récépissé qui permet au demandeur de mettre en œuvre le traitement envisagé.

Seul le récépissé donne droit à la mise en œuvre d'un traitement.

Article 34

Lorsque des traitements de données à caractère personnel relèvent d'un même organisme et ont des finalités identiques ou liées entre elles, ils peuvent faire l'objet d'une déclaration unique.

Dans ce cas, les informations requises en application de l'article 43 de la présente Loi ne sont fournies pour chacun des traitements que dans la mesure où elles lui sont propres.

Article 35

Pour les catégories les plus courantes de traitements de données à caractère personnel dont la mise en œuvre n'est pas susceptible de porter atteinte à la vie privée ou aux libertés des individus, l'Autorité de Protection des Données à caractère personnel établit et publie des normes destinées à simplifier ou à exonérer l'obligation de déclaration.

Les normes relatives à la déclaration simplifiée précisent :

1. les finalités des traitements faisant l'objet d'une déclaration simplifiée ;
2. les données à caractère personnel ou catégories de données à caractère personnel traitées ;
3. la ou les catégories de personnes concernées ;
4. les destinataires ou catégories de destinataires auxquels les données à caractère personnel sont communiquées ;
5. la durée de conservation des données à caractère personnel.

Ces normes peuvent prendre en compte les codes de conduite homologués par l'Autorité de Protection des Données à caractère personnel.

Article 36

L'Autorité de Protection des Données à caractère personnel peut définir, parmi les catégories de traitements visées à l'article 35 de la présente Loi, celles qui sont dispensées de déclaration. Pour ce faire, l'Autorité de Protection des Données à caractère personnel tient compte de leurs finalités, de leurs destinataires ou catégories de destinataires, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées.

Dans les mêmes conditions, l'Autorité de Protection des Données à caractère personnel peut autoriser les responsables de certaines catégories de traitements à procéder à une déclaration unique conformément aux dispositions de l'article 34 de la présente Loi.

Section 3 : Du régime de l'autorisation

Article 37

Ne sont mis en œuvre, qu'après autorisation de l'Autorité de Protection des Données à caractère personnel :

1. les traitements des données à caractère personnel portant sur des données génétiques et sur la recherche dans le domaine de la santé ;
2. les traitements des données à caractère personnel relatives aux infractions, condamnations ou mesures de sûreté ;
3. les traitements des données à caractère personnel ayant pour objet une interconnexion de fichiers ;
4. les traitements portant sur un numéro national d'identification ou tout autre identifiant de portée générale ;
5. les traitements des données à caractère personnel comportant des données biométriques ;
6. les traitements des données à caractère personnel ayant un motif d'intérêt public, notamment à des fins historiques, statistiques ou scientifiques.

Article 38

Les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ayant les mêmes destinataires ou catégories de destinataires, peuvent être autorisés par une décision unique de l'Autorité de Protection des Données

à caractère personnel. Dans ce cas, le responsable de chaque traitement adresse à l'Autorité de Régulation un engagement de conformité de celui-ci à la description figurant dans l'autorisation.

Article 39

L'Autorité de Protection des Données à caractère personnel se prononce dans un délai de deux (2) mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois, sur décision motivée de son président. Lorsque l'Autorité de Protection des Données à caractère personnel ne s'est pas prononcée dans ces délais, la demande d'autorisation est réputée rejetée.

Section 4 : Du régime de l'autorisation sur avis de l'Autorité de Protection des Données à Caractère Personnel

Article 40

Hormis les cas où ils doivent être autorisés par la Loi et par dérogation aux articles précédents, les traitements des données à caractère personnel opérés pour le compte de l'Etat, d'un établissement public ou d'une collectivité locale ou d'une personne morale de droit privé gérant un service public, sont autorisés par acte réglementaire, pris après avis motivé de l'Autorité de Protection des Données à caractère personnel.

Ces traitements portent sur :

1. la sûreté de l'Etat, la défense ou la sécurité publique ;
2. la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ;
3. le recensement de la population ;
4. les données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales, ethniques ou régionales, la filiation, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci ;
5. le traitement de salaires, pensions, impôts, taxes et autres liquidations
6. la mise en œuvre du recouvrement des ressources de l'Etat.

Article 41

L'Autorité de Protection des Données à caractère personnel saisie d'une demande d'avis se prononce dans un délai de deux (2) mois à compter de la réception de la demande. Toutefois, ce délai peut être renouvelé une fois, sur décision motivée du président.

Si l'Autorité de Protection des Données à caractère personnel saisie ne se prononce pas jusqu'à l'expiration du délai fixé à l'alinéa précédent, l'avis est réputé favorable.

Article 42

L'acte réglementaire pris sur avis de l'Autorité de Protection des Données à caractère personnel et autorisant les traitements visés à l'article 40 de la présente Loi précise :

1. la dénomination et la finalité du traitement ;
2. le service auprès duquel s'exerce le droit d'accès ;
3. les catégories des données à caractère personnel enregistrées ;
4. les destinataires ou catégories de destinataires habilités à recevoir communication de ces données ;
5. les dérogations à l'obligation d'information prévues par les dispositions de l'article 50 de la présente Loi, s'il y'a lieu.

Section 5 : Des dispositions communes

Article 43

Les demandes d'avis, les déclarations et les demandes d'autorisations doivent préciser :

1. l'identité et l'adresse du responsable du traitement ou, si celui-ci n'est pas établi sur le territoire national, celles de son représentant dûment mandaté ;
2. la ou les finalités du traitement
3. les interconnexions envisagées ou toutes autres formes de mise en relation avec d'autres traitements;
4. les données à caractère personnel traitées, leur origine et les catégories de personnes concernées par le traitement ;
5. la durée de conservation des informations traitées ;
6. le ou les services chargés de mettre en œuvre le traitement, ainsi que les catégories de personnes qui, en raison de leurs fonctions ou pour les besoins du service, ont directement accès aux données enregistrées ;
7. les destinataires habilités - ou non - des données communiquées ;
8. la fonction de la personne ou le service auprès duquel s'exerce le droit d'accès;
9. les dispositions prises pour assurer la sécurité des traitements et des données ;

10. l'indication du recours à un sous-traitant, s'il y a lieu ;
11. les transferts de données à caractère personnel envisagés à destination d'un pays tiers.

Les demandes d'avis portant sur les traitements intéressant la sûreté de l'État, la défense nationale ou la sécurité publique, peuvent ne pas comporter tous les éléments d'information énumérés ci-dessus, sous réserve des informations minimales prévues à l'article 42 de la présente Loi.

Article 44

Le responsable d'un traitement déjà déclaré ou autorisé doit procéder à une nouvelle déclaration ou demande d'autorisation auprès de l'Autorité de Protection des Données à caractère personnel, en cas de changement affectant les informations mentionnées à l'article précédent.

Article 45

L'avis, la déclaration ou la demande d'autorisation peuvent être adressés à l'Autorité de Protection des Données à caractère personnel par voie électronique, par voie de transmission classique sur support papier ou par voie postale.

L'Autorité de Protection des Données à caractère personnel délivre un récépissé ou avis de réception, le cas échéant, par voie électronique.

L'Autorité de Protection des Données à caractère personnel peut être saisie par toute personne agissant par elle-même, par l'entremise de son avocat ou par toute autre personne physique ou morale dûment mandatée.

CHAPITRE IV : DES OBLIGATIONS RELATIVES AUX CONDITIONS DE TRAITEMENTS DES DONNEES PERSONNELLES

Section 1: De l'obligation de confidentialité

Article 46

Le traitement des données à caractère personnel est strictement confidentiel. Il est effectué exclusivement par des personnes qui agissent sous l'autorité du responsable du traitement, et seulement sur ses instructions.

Pour la réalisation du traitement, le responsable doit choisir des personnes présentant, au regard de la préservation de la confidentialité des données, toutes les garanties tant au plan des connaissances techniques et juridiques qu'à celui de l'intégrité personnelle. Sans préjudice de l'application des dispositions de cette Loi, un engagement écrit est

signé des personnes amenées à traiter de telles données, à respecter la confidentialité et la sécurité des données.

Le contrat liant le sous-traitant au responsable du traitement comporte l'indication des obligations en matière de protection de la sécurité et de la confidentialité des données, incombant au sous-traitant ainsi qu'à ses agents intervenant au traitement des données à caractère personnel. Il prévoit que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

Section 2 : De l'obligation de sécurité

Article 47

Le responsable du traitement est tenu de prendre toute précaution utile au regard de la nature des données et, notamment, pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Il prend, en particulier, toute mesure visant à :

1. garantir que les personnes autorisées ne puissent accéder qu'aux données à caractère personnel relevant de leur compétence ;
2. garantir que puisse être vérifiée et constatée, à posteriori, l'identité des personnes ayant eu accès au système d'information et quelles données ont été lues ou introduites dans le système, à quel moment et par quelle personne ;
3. garantir que puisse être vérifiée et constatée l'identité des tiers auxquels des données à caractère personnel peuvent être transmises ;
4. empêcher toute personne non autorisée d'accéder aux locaux et aux équipements utilisés pour le traitement des données ;
5. empêcher que des supports de données puissent, en toute circonstance, être lus, copiés, modifiés, effacés, détruits ou déplacés par une personne non autorisée;
6. empêcher l'introduction non autorisée de toute donnée dans le système d'information, ainsi que toute prise de connaissance, toute modification ou tout effacement non autorisés de données enregistrées ;
7. empêcher que des systèmes de traitements de données puissent être utilisés par des personnes non autorisées à l'aide d'installations de transmission de données;
8. sauvegarder les données par la constitution de copies de sécurité ;
9. rafraîchir, et si nécessaire, convertir les données pour un stockage pérenne.

Section 3 : De l’obligation de conservation

Article 48

Les données à caractère personnel ne peuvent être conservées au-delà de la durée nécessaire qu'en vue d'être traitées à des fins historiques, statistiques ou scientifiques.

Section 4 : De l’obligation de pérennité

Article 49

Le responsable du traitement est tenu de prendre toute mesure utile pour assurer que les données à caractère personnel traitées pourront être exploitées, ultérieurement, quel que soit le support technique utilisé.

Le responsable du traitement est tenu de sauvegarder les données par la constitution de copies de sécurité, et si nécessaire, de convertir les données pour un stockage pérenne.

CHAPITRE V : DES DROITS CONFERES AUX PERSONNES DONT LES DONNEES PERSONNELLES FONT L’OBJET D’UN TRAITEMENT

Section 1 : Du droit à l’information

Article 50

Lorsque des données à caractère personnel sont collectées directement auprès de la personne concernée, le responsable du traitement ou son représentant doit fournir à celle-ci, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes :

1. l’identité du responsable du traitement ou de son représentant ;
2. la ou les finalité(s) du traitement auquel les données sont destinées ;
3. les catégories de données concernées ;
4. le ou les destinataires auxquels les données sont susceptibles d’être communiquées ;
5. le fait de savoir si la réponse aux questions est obligatoire ou facultative, ainsi que les conséquences éventuelles d’un défaut de réponse ;
6. l’existence d’un droit d’accès, de rectification et d’opposition aux données ;
7. la durée de conservation des données ;

8. le cas échéant, les transferts des données envisagés à destination de l'étranger;
9. le fait de pouvoir demander à ne plus figurer sur le fichier, la procédure à suivre et ses conséquences.

Toutefois, les dispositions de cet article ne s'appliquent pas aux données recueillies et utilisées :

- lors d'un traitement mis en œuvre pour le compte de l'Etat et intéressant la sûreté de l'Etat, la défense nationale, la sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté ;
- dans la mesure où une telle limitation est nécessaire au respect des fins poursuivies par le traitement ou à la prévention, la recherche, la constatation et la poursuite de toute infraction ;
- lorsque le traitement est nécessaire à la prise en compte d'un intérêt économique ou financier important de l'Etat, y compris dans les domaines monétaire, budgétaire, douanier et fiscal.

Article 51

Lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, les informations visées à l'article précédent sont transmises à ladite personne, au moment de l'enregistrement des données ou, si leur communication est prévue, au plus tard lors de la première communication.

Article 52

Sauf disposition contraire, toute personne utilisatrice des technologies de l'information et de la communication doit être informée de manière claire et complète par le responsable du traitement ou son représentant :

1. 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 ;
2. des moyens dont elle dispose pour s'y opposer.

Il est formellement interdit de subordonner l'accès à un service disponible sur un réseau de communications électroniques à l'acceptation, par l'abonné ou l'utilisateur concerné, du traitement des informations stockées dans son équipement.

Toutefois, les dispositions de l'alinéa précédent 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 de l'utilisateur t:

3. ont pour finalité exclusive de permettre ou faciliter la communication par voie électronique ;
4. sont strictement nécessaires à la fourniture d'un service de communication en ligne à la demande expresse de l'utilisateur.

Section 2 : Du droit d'accès

Article 53

Toute personne physique justifiant de son identité a le droit de demander, par écrit, quel que soit le support, au responsable d'un traitement des données à caractère personnel, de lui fournir :

1. les informations permettant de connaître et éventuellement de contester le traitement ;
2. la confirmation que des données à caractère personnel la concernant font ou ne font pas l'objet de ce traitement ;
3. la communication, sous une forme accessible et intelligible, des données à caractère personnel qui la concernent ;
4. des informations relatives aux finalités du traitement, aux catégories de données à caractère personnel traitées et aux destinataires auxquels les données sont communiquées ;
5. le cas échéant, des informations relatives aux transferts de données à caractère personnel envisagés à destination d'un pays tiers.

Article 54

Si la personne concernée en fait la demande, le responsable du traitement doit délivrer à la personne concernée une copie, quel que soit le support utilisé, des données à caractère personnel la concernant.

Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme n'excédant pas le coût de la reproduction.

En cas de risque de dissimulation ou de disparition des données à caractère personnel, la personne concernée peut en informer l'Autorité de Protection des Données à caractère personnel, qui prend alors toutes mesures de nature à éviter cette dissimulation ou cette disparition.

Article 55

Toute personne, qui dans l'exercice de son droit d'accès, a des raisons sérieuses de soutenir que les données qui lui ont été communiquées ne sont pas conformes aux données traitées, peut en informer l'Autorité de Protection des Données à caractère personnel qui procède aux vérifications nécessaires.

Article 56

Le droit d'accès d'un patient aux données à caractère personnel le concernant est exercé par le patient lui-même ou par l'intermédiaire d'un médecin qu'il désigne.

En cas de décès du patient, son conjoint vivant avec lui et ses enfants, ou ses parents (père ou mère), s'il s'agit d'un mineur, , peuvent exercer le droit d'accès, par l'intermédiaire d'un médecin qu'ils désignent.

Article 57

Le responsable du traitement des données à caractère personnel peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique.

En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable du traitement auprès duquel elles sont adressées.

Article 58

Par dérogation aux articles 53 et suivants de la présente Loi, lorsqu'un traitement intéresse la sûreté de l'Etat, la défense nationale ou la sécurité publique, le droit d'accès s'exerce dans les conditions suivantes. :

1. la demande est adressée à l'Autorité de Protection des Données à caractère personnel, qui désigne l'un de ses membres appartenant ou ayant appartenu à la Cour Suprême pour mener les investigations nécessaires. Celui-ci peut se faire assister d'un agent de l'Autorité de Régulation Multisectorielle. Il est notifié au requérant qu'il a été procédé aux vérifications ;
2. lorsque l'Autorité de Protection des Données à caractère personnel constate, en accord avec le responsable du traitement, que la communication des données qui y sont contenues ne met pas en cause ses finalités, la sûreté de l'Etat, la défense nationale ou la sécurité publique, ces données peuvent être communiquées au requérant ;
3. lorsque le traitement est susceptible de comprendre des informations dont la communication ne mettrait pas en cause les fins qui lui sont assignées, l'acte réglementaire portant création du fichier peut prévoir que ces informations

soient communiquées au requérant par le gestionnaire du fichier directement saisi.

Section 3 : Du droit d'opposition

Article 59

Sauf dans le cas d'un traitement répondant à une obligation légale, toute personne physique a le droit de s'opposer, sans aucun frais, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.

La personne concernée a le droit, d'une part, d'être informée avant que des données la concernant ne soient pour la première fois communiquées à des tiers ou utilisées pour le compte de tiers à des fins de prospection et, d'autre part, de se voir expressément offrir le droit de s'opposer, gratuitement, à ladite communication ou utilisation.

Article 60

Toute personne concernée par un traitement, a le droit de s'opposer, sous réserve des exceptions légales, à ce que les données à caractère personnel la concernant fassent l'objet de la levée du secret professionnel.

Section 4 : Du droit de rectification et de suppression

Article 61

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 supprimées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Article 62

Lorsque l'intéressé en fait la demande par écrit, quel que soit le support, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'article précédent dans un délai d'un (1) mois après l'enregistrement de la demande.

En cas de contestation, la charge de la preuve incombe au responsable du traitement auprès duquel est exercé le droit de rectification.

Si une donnée a été transmise à un tiers, le responsable du traitement est tenu d'accomplir les diligences utiles afin de lui notifier les opérations qu'il a effectuées conformément au premier alinéa.

Article 63

Les héritiers d'une personne décédée justifiant de leur identité peuvent, si des éléments portés à leur connaissance leur laissent présumer que les données à caractère personnel la concernant faisant l'objet d'un traitement n'ont pas été actualisées, exiger du responsable de ce traitement qu'il prenne en considération le décès et procède aux mises à jour qui doivent en être la conséquence.

Lorsque les héritiers en font la demande, le responsable du traitement justifie, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en vertu de l'article précédent.

CHAPITRE VI : DE LA REGULATION EN MATIERE DE PROTECTION DES DONNEES PERSONNELLES

Section 1 : De l'Autorité de Protection de Données à Caractère Personnel

Article 64

Il est créé une Autorité de Protection des Données à caractère personnel, chargée de veiller à ce que les traitements des données à caractère personnel, en Mauritanie, soient mis en œuvre conformément aux dispositions de la présente Loi.

L'Autorité de Protection des Données à caractère personnel est une personne morale de droit public, indépendante, dotée de l'autonomie financière et de gestion. Elle est rattachée au Premier Ministre.

Elle informe les personnes concernées et les responsables de traitement de leurs droits et obligations et s'assure que les Technologies de l'Information et de la Communication ne comportent pas de menace au regard des libertés publiques et de la vie privée.

Article 65

L'Autorité de Protection des Données à caractère personnel est composée de sept (7) membres choisis, en raison de leur compétence juridique et/ou technique, ainsi qu'il suit :

1) trois (3) personnalités qualifiées pour leur connaissances et expériences dans les domaines du droit, de l'informatique et/ou des nouvelles technologies de l'information, désignées par le Président de la République ;
2) deux (2) personnalités désignées sur propositions respectives du président de l'Assemblée Nationale et du président du Sénat ;

3) un (1) magistrat désigné sur proposition du Ministre chargé de la justice ;
4) un (1) représentant des organisations de défense des droits de l'homme, désigné sur proposition des organisations de la Société Civile.

Les modalités et les conditions de nomination des membres de l'autorité de protection des données personnelles sont fixées par décret.

Un Commissaire du Gouvernement, désigné par le Premier Ministre, siège auprès de l'Autorité de Protection des Données à Caractère Personnel. Le Commissaire du Gouvernement est convoqué à toutes les séances de l'Autorité, dans les mêmes conditions que les membres de celle-ci. Il informe l'Autorité sur les orientations du gouvernement et sur les motivations de l'Administration concernant la mise en œuvre des traitements, mais ne prend pas part au vote.

Article 66

Le Président de la République nomme, parmi les membres de l'Autorité de Protection des Données à Caractère Personnel, le président de ladite autorité. Le président est secondé par un vice-président élu en leur sein, par les membres de l'autorité de protection des données à caractère personnel.

L'Autorité de Protection des Données à caractère personnel dispose de services placés sous l'autorité de son Président. Elle dispose, en outre, d'un personnel mis à sa disposition par l'État et peut pourvoir au recrutement d'agents en fonction des besoins de son fonctionnement.

Les agents assermentés, qui peuvent être appelés à participer à la mise en œuvre des missions de vérification mentionnées aux articles 74 et76 de la présente Loi, doivent y être habilités par l'Autorité de protection des données à caractère personnel. Cette habilitation ne dispense pas de l'application des dispositions définissant les procédures autorisant l'accès aux secrets protégés par la Loi.

Article 67

Le mandat des membres de l'Autorité de Protection des Données à caractère personnel, est de quatre (4) ans renouvelable, une seule fois.

À l'exception du Président, les membres de la Commission des Données Personnelles n'exercent pas leurs fonctions à titre exclusif, sous réserve des incompatibilités prévues à l'**Erreur ! Source du renvoi introuvable.**.

Les membres de l'autorité de protection des données à caractère personnel sont inamovibles pendant la durée de leur mandat. Sauf faute grave, il ne peut être mis fin à leurs fonctions qu'en cas de démission ou d'empêchement constaté par l'Autorité de Protection des Données à caractère personnel, dans les conditions prévues par le décret qui y est afférent.

Les membres de l'Autorité de Protection des Données à caractère personnel sont soumis au secret professionnel, conformément aux textes en vigueur.

L'Autorité de Protection des Données à caractère personnel établit un règlement intérieur qui précise, notamment, les règles relatives aux délibérations, à l'instruction et à la présentation des dossiers.

Les règles relatives à l'organisation et au fonctionnement de l'Autorité de Protection des Données à caractère personnel sont fixées par décret.

Article 68

La qualité de membre de l'Autorité de Protection des Données à caractère personnel est incompatible avec la qualité de membre du Gouvernement, de l'exercice des fonctions de dirigeants d'entreprise, de la détention de participation dans les entreprises du secteur de l'informatique ou des communications électroniques.

Tout membre de l'Autorité de Protection des Données à caractère personnel doit informer celle-ci des intérêts directs ou indirects qu'il détient ou vient à détenir, des fonctions qu'il exerce ou vient à exercer et de tout mandat qu'il détient ou vient à détenir au sein d'une personne morale.

Le cas échéant, l'Autorité prend toutes les dispositions utiles pour assurer l'indépendance et l'impartialité de ses membres. Un code de conduite est mis en place à cet effet.

Article 69

Si, en cours de mandat, le président ou un membre de l'Autorité de Protection des Données à caractère personnel cesse d'exercer ses fonctions, il est procédé à son remplacement dans les conditions prévues par la présente Loi.

Le mandat du successeur ainsi désigné est limité à la période restant à courir. Ce dernier peut être désigné pour un seul mandat.

Article 70

Les membres de l'Autorité de Protection des Données à caractère personnel, avant leur entrée en fonction, prêtent serment devant la Cour suprême, siégeant en audience solennelle, le serment dont la teneur suit : « **Je jure au nom d'Allah de bien et fidèlement remplir ma fonction de membre de l'Autorité de Protection des Données à caractère personnel, en toute indépendance et impartialité, de façon digne et loyale, et de garder le secret des délibérations** ».

Les autres agents choisis par l'Autorité de Protection des Données à caractère personnel prêtent serment dans les mêmes conditions.

Article 71

Les membres de l'Autorité de Protection des Données à caractère personnel jouissent d'une immunité totale pour les opinions émises dans l'exercice ou à l'occasion de l'exercice de leur fonction.

Dans l'exercice de leur attribution, les membres de l'Autorité de Protection des Données à caractère personnel ne reçoivent d'instruction d'aucune autorité.

Article 72

Les ministres, autorités publiques, dirigeants d'entreprises publiques ou privées, responsables de groupements divers et plus généralement les détenteurs ou utilisateurs de traitements ou de fichiers de données à caractère personnel prennent toutes mesures afin de faciliter la tâche à de l'Autorité de Protection des Données à caractère personnel. Sauf si la Loi en dispose autrement, et sous réserve du droit d'opposition à la visite visé à l'article 74 de la présente loi, ils ne peuvent s'opposer à l'action de l'Autorité de Protection des Données à caractère personnel pour quelque motif que ce soit.

Section 2: Des attributions de l'Autorité de Protection des Données à Caractère Personnel

Article 73

L'Autorité de Protection des Données à caractère personnel exerce les missions suivantes :

1. elle veille à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions de la présente Loi ;
2. elle informe les personnes concernées et les responsables de traitement de leurs droits et obligations. A cet effet :

a. elle reçoit les formalités préalables à la création de traitements des données à caractère personnel;

b. elle reçoit les réclamations, les pétitions et les plaintes relatives à la mise en œuvre des traitements des données à caractère personnel et informe leurs auteurs des suites données à celles-ci ;

c. elle informe sans délai le procureur de la République des infractions dont elle a connaissance et elle peut ester en justice en cas de violation de la présente Loi;

d. elle peut, par décision particulière, charger un ou plusieurs de ses membres ou agents de ses services de procéder à des vérifications portant sur tout traitement et, le cas échéant, d'obtenir des copies de tout document ou support d'information utile à sa mission ;

e. elle peut, dans les conditions définies aux articles 77 et suivants de la présente Loi, prononcer une sanction à l'égard d'un responsable de traitement ;

f. elle répond à toute demande d'avis.

3. elle homologue les codes de bonne conduite qui lui sont présentés ;

4. elle tient un répertoire des traitements des données à caractère personnel à la disposition du public ;

5. elle conseille les personnes et organismes qui ont recours aux traitements des données à caractère personnel ou qui procèdent à des essais ou expériences de nature à aboutir à de tels traitements ;

6. elle arrête les conditions et les règles de procédure relatives aux transferts transfrontaliers de données à caractère personnel et les autorise, le cas échéant, dans les conditions prévues par la présente Loi;

7. elle présente au gouvernement toute suggestion susceptible de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données à caractère personnel;

8. elle coopère avec les autorités de protection des données à caractère personnel des pays tiers, participe aux négociations internationales en matière de protection des données à caractère personnel ;

9. elle publie les autorisations accordées et les avis émis dans le répertoire des traitements des données à caractère personnel ;

10. elle établit, chaque année, un rapport d'activités remis au Premier Ministre et au Parlement et au Ministre en charge des communications électroniques

Section 3 : Du contrôle et des sanctions administratives et pécuniaires

Article 74

Les agents de L'Autorité de Protection des Données à caractère personnel, ainsi que les agents de service assermentés ont accès, dans les conditions prévues par les dispositions des article 46 et suivants du Code de Procédure Pénale, relatifs à la

répression des infractions flagrantes, pour l'exercice de leurs missions, aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre d'un traitement des données à caractère personnel et qui sont à usage professionnel, à l'exclusion des parties de ceux-ci affectées au domicile privé.

Le Procureur de la République territorialement compétent en est préalablement informé.

Article 75

En cas d'opposition du responsable des lieux, la visite ne peut se dérouler qu'avec l'autorisation de l'autorité judiciaire compétente dans le ressort duquel sont situés les locaux à visiter ou du juge délégué par lui.

Ce magistrat est saisi à la requête du Président de l'Autorité de Protection des Données à caractère personnel. Il statue par une ordonnance motivée, en procédure d'urgence et sans représentation obligatoire.

Article 76

Les agents de l'Autorité de Protection des Données à caractère personnel et les agents mentionnés à l'article 74 de la présente Loi peuvent demander communication de tous documents nécessaires à l'accomplissement de leur mission, quel qu'en soit le support, et en prendre copie.

Ils peuvent recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles. Ils peuvent accéder aux programmes informatiques et aux données, demander la transcription de tout traitement dans des documents appropriés directement utilisables pour les besoins du contrôle.

Ils peuvent être assistés par des experts choisis par le Président de ladite autorité.

Il est dressé contradictoirement procès-verbal des vérifications et visites menées en application des articles précédents.

Article 77

L'Autorité de Protection des Données à caractère personnel peut prononcer les mesures suivantes :

1. un avertissement à l'égard du responsable du traitement ne respectant pas les obligations découlant de la présente Loi et des dispositions réglementaires en vigueur.
2. une mise en demeure de faire cesser les manquements concernés dans le délai qu'elle fixe.

Article 78

Si le responsable du traitement ne se conforme pas à la mise en demeure qui lui a été adressée, l'Autorité de Protection des Données à caractère personnel peut prononcer à son encontre, après procédure contradictoire, les sanctions suivantes :

1. un retrait provisoire de l'autorisation accordée pour une durée maximum de trois mois,
2. un retrait définitif de l'autorisation accordée; le retrait définitif peut faire suite à une période de retrait provisoire à l'issue de laquelle le responsable du traitement ne se serait pas conformé aux exigences de la mise en demeure
3. une amende pécuniaire dans les conditions prévues à l'article 80 de la présente Loi

Article 79

En cas d'urgence, lorsque la mise en œuvre d'un traitement ou l'exploitation de données à caractère personnel entraîne une violation de droits et libertés, l'Autorité de Protection des Données à caractère personnel, après procédure contradictoire, peut décider :

1. l'interruption de la mise en œuvre du traitement pour une durée maximale de trois mois ;
2. le verrouillage de certaines données à caractère personnel traitées pour une durée maximale de trois mois ;
3. l'interdiction temporaire ou définitive d'un traitement contraire aux dispositions de la présente Loi.

Si le traitement a été autorisé par acte réglementaire dans les conditions définies à l'article 42 de la présente Loi, l'Autorité de Protection des Données à caractère personnel informe le Ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée.

Le Ministre fait alors connaître à l'Autorité de Protection des Données à caractère personnel les suites qu'il a données à cette information, au plus tard quinze jours après l'avoir reçue.

Article 80

En cas de manquements aux dispositions légales et réglementaires relatives aux données à caractère personnel, hormis les sanctions ci-dessus, l'Autorité de Protection des Données à caractère personnel peut prendre des sanctions pécuniaires à l'encontre des contrevenants.

Le montant de la sanction pécuniaire est proportionné à la gravité du manquement.

Lors du 1er manquement, il ne peut excéder un million d' ouguiyas (1 000 000 UM).

En cas de manquement réitéré dans les cinq années à compter de la date à laquelle la sanction pécuniaire précédemment prononcée est devenue définitive, il ne peut excéder cinq millions d'Ouguiyas (5 000 000 UM) ou, s'agissant d'une entreprise, 5 % du chiffre d'affaires hors taxes du dernier exercice clos.

Le recouvrement des pénalités se fait conformément à la législation relative au recouvrement des créances de l'Etat, étrangères à l'impôt et au domaine.

Article 81

Les sanctions prononcées par l'Autorité de Protection des Données à caractère personnel sont prises sur la base d'un rapport établi par l'un de ses membres, désigné par le président de ladite Autorité.

Ce rapport est notifié au responsable du traitement, qui peut déposer des observations et se faire représenter ou assister.

Article 82

Les sanctions prononcées par l'Autorité de Protection des Données à caractère personnel peuvent être rendues publiques sur décision de son président. Ce dernier peut également ordonner, aux frais des personnes sanctionnées, l'insertion de ces sanctions dans des publications, journaux ou autres supports qu'il aura désignés.

Article 83

Les sanctions et décisions prises par l'Autorité de Protection des Données à caractère personnel sont susceptibles de recours devant la Cour Suprême.

Section 4 : Des dispositions pénales

Article 84

Est puni de trois (3) à cinq (5) ans d'emprisonnement et de cinq cent mille (500.000 UM) à dix millions d'ouguiyas (10.000.000 UM) d'amende, ou de l'une de ces deux peines seulement, le fait d'entraver, intentionnellement et sans droit, l'action de l'Autorité de Protection des Données à caractère personnel soit :

1. en s'opposant à l'exercice des missions confiées à ses membres ou aux agents habilités, lorsque la visite été autorisée par le juge;

2. en refusant de communiquer à ses membres ou aux agents habilités les renseignements et documents utiles à leur mission, en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître;
3. en communiquant des informations qui ne sont pas conformes au contenu des enregistrements, tel qu'il était au moment où la demande a été formulée, ou qui ne présentent pas ce contenu sous une forme directement accessible.

Article 85

Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre, telles qu'elles sont prévues par la présente Loi, est puni de d'un (1) à trois (3) ans d'emprisonnement et de deux cent mille (200.000)à cinq millions d'ouguiyas (5.000.000 UM) d'amende ou de l'une de ces deux peines seulement.

Article 86

Est puni des mêmes peines que celles qui sont prévues à l'article précédent le fait, même par erreur, imprudence ou négligence, de procéder ou de faire procéder à un traitement qui a fait l'objet de l'une des mesures prévues aux articles 77, 78, ou 79 de la présente Loi.

Article 87

Est puni des mêmes peines le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite.

Article 88

Est puni des mêmes peines le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures de sécurité prévues par la présente Loi.

Article 89

Est puni des mêmes peines le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette dernière personne, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes.

Article 90

Le fait, hors les cas prévus par la Loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'identité de celles-ci, est puni de trois (3) à cinq (5) ans d'emprisonnement et de cinq cent mille (500.000) à deux millions d'ouguiyas (2.000.000 UM) d'amende ou de l'une de ces deux peines seulement.

Article 91

Est puni des mêmes peines le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée des données à caractère personnel concernant des infractions, des condamnations ou des mesures de sûreté judiciaires.

Article 92

Le fait de conserver et / ou de traiter des données à caractère personnel au-delà de la durée prévue par la Loi ou le règlement, par la demande d'autorisation ou d'avis, ou par la déclaration préalable adressée à de l'Autorité de Protection des Données à caractère personnel, est puni de trois (3) mois à un (1) an d'emprisonnement et de cent mille (100.000) à cinq cent mille ouguiyas (500.000 UM) d'amende ou de l'une de ces deux peines seulement, sauf si cette conservation est effectuée à des fins historiques, statistiques ou scientifiques dans les conditions prévues par la Loi.

Article 93

Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité, telle que définie par la Loi, le règlement ou la décision de l'Autorité de Protection des Données à caractère personnel autorisant le traitement automatisé, ou par les déclarations préalables à la mise en œuvre de ce traitement, est puni d'un (1) à cinq (5) ans d'emprisonnement et de deux cent mille (200.000) à deux millions d'ouguiyas (2.000.000 UM) d'amende ou de l'une de ces deux peines seulement.

Article 94

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 d'une personne ou à l'intimité de la vie privée de celle-ci, de porter sans autorisation de cette personne, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni d'un (1) à trois (3) ans d'emprisonnement et de deux cent mille (200.000) à un million d'ouguiyas (1.000.000 UM) d'amende ou de l'une de ces deux peines seulement.

La divulgation prévue à l'alinéa précédent est punie de six (6) mois maximum d'emprisonnement et de cinquante mille (50.000) à cent mille ouguiyas (100.000 UM) ouguiyas d'amende ou de l'une de ces deux peines seulement, lorsqu'elle a été commise par imprudence ou négligence.

Dans les cas prévus aux deux alinéas précédents, la poursuite ne peut être exercée que sur plainte de la victime, de son représentant légal ou de ses ayants droit.

Article 95

Dans les cas prévus aux articles ci-dessus de la présente section, l'effacement de tout ou partie des données à caractère personnel faisant l'objet du traitement ayant donné lieu à l'infraction peut être ordonné.

Les membres et les agents de l'autorité de protection des données à caractère personnel sont habilités à constater l'effacement de ces données.

Article 96

Les personnes morales autres que l'Etat, les collectivités locales et les établissements publics sont pénalement responsables des infractions prévues par la présente Loi, commises pour leur compte, par une personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé sur:

a. un pouvoir de représentation de la personne morale;

b. une autorité pour prendre des décisions au nom de la personne morale;

c. une autorité pour exercer un contrôle au sein de la personne morale.

La personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe précédent a rendu possible la commission de l'infraction.

La responsabilité des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits.

Article 97

Les peines encourues par les personnes morales sont :

1. l'amende, dont le taux maximum est égal au quintuple de celui prévu pour les personnes physiques;
2. la dissolution, lorsqu'il s'agit d'une personne morale ou d'une peine d'emprisonnement supérieure à cinq (5) ans, lorsqu'il s'agit d'un crime ou d'un délit commis par une personne physique ;
3. l'interdiction à titre définitif ou pour une durée de cinq ans, au plus, d'exercer directement ou indirectement une ou plusieurs activités professionnelles ou sociales en rapport avec les faits;
4. la fermeture définitive ou pour une durée de cinq ans, au plus, d'un ou de plusieurs des établissements de l'entreprise ayant participé à commettre les faits incriminés ;
5. l'exclusion des marchés publics à titre définitif ou pour une durée de cinq ans au plus ;
6. la saisie et la confiscation de la chose qui a servi ou était destinée à commettre l'infraction ou de la chose qui en est le produit ;
7. l'affichage de la décision de justice prononcée ou la diffusion de celle-ci soit par la presse écrite soit par tout moyen de communication au public notamment par voie électronique.

Article 98

Le procureur de la République avise le président de l'Autorité de Protection des Données de toutes les poursuites relatives aux infractions pénales prévues par la présente Loi, et le cas échéant, des suites qui leur sont données.

Il l'informe de la date et de l'objet de l'audience de jugement au moins dix jours avant cette date.

La juridiction d'instruction ou de jugement peut appeler le président de l'Autorité de Protection des Données à caractère personnel ou son représentant à déposer ses observations ou à les développer oralement à l'audience.

CHAPITRE VII : DES DISPOSITIONS TRANSITOIRES ET FINALES

Article 99

A compter de la date d'entrée en vigueur de la présente Loi et de la mise en place effective de l'Autorité de Protection des Données à caractère personnel, tous les traitements de données à caractère personnel doivent répondre aux prescriptions de celle-ci, dans les délais ci-après :

1. trois ans, pour les traitements de données opérés pour le compte de l'Etat, d'un établissement public, d'une collectivité locale ou d'une personne morale de droit privé gérant un service public
2. deux ans, pour les traitements de données à caractère personnel effectués pour le compte de personnes autres que celles soumises aux dispositions du point précédent.

Article 100

A défaut de la régularisation dans les délais fixés à l'article précédent, les traitements sont réputés avoir été exercés sans déclaration ou sans autorisation au mépris des dispositions de la présente loi.

BIBLIOGRAPHIE ET WEBOGRAPHIE

LOIS & DECRETS

- **Burkina Faso** :

LOI N° 010-2004/AN PORTANT PROTECTION DES DONNEES A CARACTERE PERSONNEL

- **Côte d'Ivoire** :

Loi N ° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel

Décret N ° 2012-934 du 19 septembre 2012 portant organisation et fonctionnement de l'autorité de régulation des Télécommunications/TIC de Côte d'Ivoire

ARRETE N" 511 MPTICICAB DU 11 NOVEMBRE 2014 PORTANT DEFINITION OU PROFIL ET FIXANT LES CONDITIONS D'EMPLOI DU CORRESPONDANT A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Sénégal :

Loi n° 2008 – 12 sur la Protection des données à caractère personnel

Décret N ° 2011-929 du 29 juin 2011 MODIFIANT LE DECRET ~ 2009 -392 DU 20 AVRIL 2009 PORTANT NOMINATION DES MEMBRES DE LA COMMISSION DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

France :

Loi n° 7817 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Version consolidée au 23 avril 2016)

Mauritanie :

Loi N ° 2013-025 du 15 juillet 2013 portant sur les communications électroniques

Loi N ° 2011-003 du 12 janvier 2011 abrogeant et remplaçant la Loi N ° 96-019 du 19 juin 1996 portant Code de l'Etat Civil

Décret N ° 2010-150 du 06 juillet 2010 portant création, organisation et fonctionnement de l'Agence Nationale du Registre des Populations et des Titres Sécurisés (ANRPTS)

OUVRAGES & ARTICLES

ABITEBOULE Serge, « Leçon inaugurale Collège de France »

CASILLI Antonio, « Vie privée dans un monde dense », dans « La dynamique d'internet Prospective 2030 »

COMET François, « Dynamique européenne de la régulation et de l'industrie des télécommunications : Le cadre »

CNIL, « Open Data, quels enjeux pour la protection des données personnelles ? »

DELCROIX Geoffrey, « Labo CNIL »

DOUNES GILLES, « iPod Backstage, les coulisses d'un succès mondial », 2005, Editions Dunod

FORSTER Frédéric, « La Protection de la Vie Numérique »

GILLE Laurent, « La donnée au cœur du numérique : questions »

GILLE Laurent et MARCHANDISE Jacques-François, « La dynamique d'internet Prospective 2030 »

GUILLAUD Hubert, « Vers un nouveau monde de données », InternetActu.net

KAPLAN Daniel, « Informatique, libertés, identités », « La valeur de la vie privée, c'est de nous permettre d'avoir une vie publique ! », avril 2010, Fyp Editions

LECLERCQ Floriane, « Eléments de présentation de l'AFAPDP »

NEPOTE Charles, GROUPE "INFORMATIQUE & LIBERTES 2.0 ?", « LE NOUVEAU PAYSAGE DES DONNEES PERSONNELLES : QUELLES CONSEQUENCES SUR LES DROITS DES INDIVIDUS ? », Note de travail, Janvier 2009, IDENTITES ACTIVES.NET, FING

RAULIN-SERRIER Pascale, « Rôle et missions de la CNIL »

SCOTTEZ Clémence, « Enjeux de la protection des données personnelles dans le secteur économique »

TOUBIANA Vincent, GROUPE "INFORMATIQUE & LIBERTES 2.0 ?", « LE NOUVEAU PAYSAGE DES DONNEES PERSONNELLES : QUELLES CONSEQUENCES SUR LES DROITS DES INDIVIDUS ? », Note de travail, Janvier 2009, IDENTITES ACTIVES.NET, FING

WAELBROECK, Patrick, « Protection de la vie privée », dans « La dynamique d'internet Prospective 2030 »

WAELBROECK, Patrick, « Protection de la vie privée et pathologies du Web », Document de travail CVPIP-13-01, Chaire Valeurs et Politiques des informations personnelles

SITES CONSULTES

Site web de l'AFAPDP, http://www.afapdp.org/pays

Site web du Journal LIBERATION
http://www.liberation.fr/sciences/2015/02/09/votreteleviseurvousenregistretilavotreinsu_1198872

Site web de la FING http://fing.org/?InformatiqueLibertesIdentites

Table des matières