LA GOUVERNANCE DES DONNEES : LOCALISATION DES DONNEES, BASE DE DONNEE BIOMETRIQUE ET IDENTITE NUMERIQUE

Par Astou DIOUF

JONCTION

À propos de l'auteur

Astou Diouf est une juriste diplômée de la Faculté des Sciences Juridiques et Politiques (FSJP) de l'Université Cheik Anta DIOP de Dakar. Doctorante en Droit Privé. Elle possède une grande expérience en matière de Contentieux des Affaires, des droits numériques, de cybercriminalité, de cybersécurité et données personnelles.

Elle est auteur de plus articles dont : L'Etude Critique de la Stratégie Nationale de Cybersécurité du Sénégal ; L'Etude de la liberté d'expression sur Internet au Sénégal ; Réactions des Télécoms à la Covid-19 au Sénégal ; Aperçu de la Responsabilité des Intermédiaires au Sénégal ; La liberté d'expression à l'aune de la régularisation des médias sociaux : une équation entre liberté et punité ; Les politiques sénégalaises de lutte contre la pandémie COVID -19 et leur impact sur les droits de l'homme en ligne ; La régulation des plateformes numériques et la liberté d'expression en Afrique de l'Ouest.

Lauréate de la Bourse de recherche 2020 de la Collaboration sur la politique internationale des TIC pour l'Afrique orientale et australe (CIPESA).

Lauréate de la bourse Gaetan Mootoo 2022 pour les défenseures des Droits humains, attribuée chaque année par Amnesty International- Bureau Régional Afrique de l'Ouest et du Centre.

Sommaire

Méthodologie et plan de l'étude

L'étude de la gouvernance des données personnelles intervient dans un contexte où le Sénégal dispose d'un centre national de données pour promouvoir la souveraineté des données conformément à la Stratégie numérique 2025. A cet effet, les agences de l'État sont tenues d'héberger toutes leurs données dans le centre de données de Diamniadio.

La gouvernance des données doit nécessairement promouvoir une politique et des pratiques efficaces en matière de collette et traitement des données des citoyens, de l'administration publique et du secteur privé d'une part et d'autre part, à tenir compte de l'impact de la localisation des données, de la biométrique, du paysage de l'identification numérique et de tous les droits numériques tels que la vie privée et les données personnelles.

À cela s'ajoute une croissance exponentielle d'acteurs non régulés comme les réseaux sociaux ou moins régulés comme les prestataires de service d'information sur les comptes et la prolifération des contenus haineux, racistes, antisémites, des atteintes à la vie privée, des fausses nouvelles, de la désinformation et de la manipulation de l'information. L'ensemble de ces facteurs incitent la société civile du secteur du numérique à s'interroger sur la gouvernance des données personnelles au Sénégal.

La méthodologie qui a été adoptée pour cette étude comprend essentiellement la recherche documentaire et de données disponibles auprès des bibliothèques, des centres de documentation.

Ce travail scientifique est le résultat d'une étude sur : « la gouvernance des données personnelles au Sénégal », afin de permettre un plaidoyer pour une gouvernance des données participative et inclusive au Sénégal.

En outre, une étude sur la gouvernance des données personnelles nécessite une note introductive de l'évolution des TIC et une bonne compréhension des concepts qui ne sont pas souvent familiers aux lecteurs **(I)**. C'est dans cette suite logique que des éléments de réponse mériteraient d'être apportés à la problématique de la gouvernance des données personnelles au Sénégal. L'Etat, acteur principal de la gouvernance des données intervient pour encadrer la collette et le traitement des données dans un cadre normatif **(II)** et institutionnel **(III).** Il est de

coutume que le traitement et la collecte des données personnelles est souvent source d'atteinte aux droits fondamentaux des personnes **(IV).**

Des risques potentiels peuvent résulter des programmes de collecte de données biométriques numériques, de localisation des données ainsi que des politiques d'institution d'identité numérique **(V)**. Pour se faire, on s'efforcera de conclure **(VI)** et de formuler des recommandations à l'endroit des parties prenantes concernées (Administration, secteur privé, société civile) pour une protection efficace des données à caractère personnel **(VII)**.

I. Note introductive des TIC dans la gouvernance des données

Les Technologies de l'Information et de la Communication (TIC) se développent rapidement et sont de plus en plus intégrées dans le quotidien des sénégalais. En effet, le Gouvernement du Sénégal développe activement l'usage généralisé des TIC dans la vie quotidienne au Sénégal, à travers ses différentes initiatives nationales telles que décrites dans sa stratégie « *Sénégal Numérique 2025* »[1], adossée au référentiel de développement du Plan Sénégal Emergent (PSE), adopté en 2012.[2] Ces initiatives entraînent une transformation du Sénégal en une société numérique où le secteur public, les entreprises et le grand public utilisent l'économie numérique comme facteur de croissance et de compétitivité.

C'est pour cela que la Stratégie Nationale de Cybersécurité (SNC 2022) s'avère importante dans le but de guider les actions de l'Etat concernant la cybersécurité tout en proposant une vision aux sénégalais, y compris aux organismes des secteurs privé et public, tout comme aux institutions universitaires, à la société civile et à d'autres parties prenantes.

La stratégie considère la cybersécurité comme la protection des systèmes d'information, des données qui y sont incluses ainsi que des services qu'ils fournissent ou sur lesquels ils s'appuient, contre tout accès, modification, entrave, destruction ou usage illicites.[3]

L'utilisation croissante des TIC au Sénégal repose en grande partie sur la fourniture des biens et services, la collecte et l'exploitation des données, des transactions électroniques et du partage de l'information, impliquant le plus souvent la collecte et l'exploitation des données à caractère personnel. C'est dans ce cadre que Maître Frédéric Forster, Avocat à la Cour d'appel de Paris affirme que : ' *'C'est cette collecte massive de données à caractère personnel qui est souvent présentée comme étant la contrepartie de la gratuité des services sur internet, le*

[1] Le Sénégal a lancé en 2016 sa stratégie « Sénégal numérique 2025 »

[2] PSE vise à stimuler une croissance économique soutenue et inclusive et à faire du Sénégal une économie émergente d'ici 2035.

[3] Sur l'ensemble de la question, voir Etude critique de la Stratégie Nationale de Cybersécurité du Sénégal, disponible sur : http://jonction.e-monsite.com/medias/files/etude-critique-de-la-strategie-nationale-de-cybersecurite-du-senegal-2-.pdf .

« produit » étant la personne qui communique ses données aux différents acteurs de l' internet.''[4]

En effet, la forte informatisation de la société sénégalaise implique pour tous les utilisateurs, la fourniture d'informations sensibles, condition *sine qua none* pour accéder aux technologies, t'elles qu'Internet, la téléphonie mobile[5], cartes bancaires et autres objets connectés. C'est à juste raison que le professeur Abdoulaye SAKHO soutient qu' : *« Il n'y a pas de secteur du numérique, c'est la forme d'expression de l'économie contemporaine. Tout devient numérique dans la société actuelle, il est dans le transport, l'énergie, les banques* ».[6]

Ainsi, compte tenu de l'importance de la donnée, comme l'élément principal exploité à l'ère du numérique, la collecte et le traitement constituent des enjeux majeurs pour l'Etat du Sénégal en raison de la multitude d'intervenants dans la circulation et l'utilisation des informations personnelles sur les réseaux : GAFAM, les grandes entreprises internationales, les opérateurs de télécoms et les sites marchands.

Protéger les données à caractère personnel revient à protéger l'intimité, la dignité et les autres droits fondamentaux de la personne comme, le droit à la vie privée, le droit à l'image, le droit à l'honneur, etc.

En sus de ce qui précède, le droit sénégalais a définit les données à caractère personnel au point n°6 de l' article 4 de la loi n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel comme : « *toute information 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* ».

A ce titre, une donnée, même sans être directement identifiable comme le nom ou le prénom, peut néanmoins être indirectement identifiante[7] comme une photo, et relever de ce fait de la loi sur la protection des données à caractère personnel, doit en conséquence être traitée en respectant les principes et obligations issus de cette loi.

Sont également des données à caractère personnel, les données dites sensibles. Au regard de l'article 4 de la loi de 2008 susmentionnée, il s'agit des données relatives aux opinions ou

---

[4] P. F. DRAME et R. SARR, *L'impact du règlement sur la protection des données (RGPD) en Afrique*, L'Harmattan, 2021, P. 15.

[5] M. LO, *La protection des données à caractère personnel en Afrique*, Baol Editions, 2017, P. 19.

[6] SAKHO (A), « article publié Sud Quotidien » : « « Le numérique n'est pas un secteur d'activité, mais une forme d'expression de l'économie », le 7 juin 2017, disponible sur le : https://www.osiris.sn/Abdoulaye-Sakho-Professeur-agrege.html , consule le 17/08 /2022 à 01H 28.

[7] P. F. DRAME et R. SARR, L'impact du règlement sur la protection des données (RGPD) en Afrique, L'Harmattan, 2021, P. 28.

activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre social, aux poursuites, aux sanctions pénales ou administratives.

Du côté de l'Etat et de ses démembrements, l'informatisation de l'administration a entraîné la génération de beaucoup de données personnelles, dont la numérisation du fichier électoral, du permis de conduire, de la carte d'identité nationale et des actes d'état civil.

Déjà, le Sénégal dans sa volonté politique est le premier pays de la CEDEAO a lancé la carte d'identité biométrique. La carte d'identité biométrique CEDEAO a la valeur d'une carte nationale d'identité d'une carte électorale et d'une carte d'identité de la CEDEAO. C'est une carte à puce électronique qui peut servir en même temps à plusieurs applications.[8]

Le succès de l'économie numérique requiert aussi d'authentifier l'identité des populations d'où le lancement du projet d'identité numérique nationale (INN) par le Ministère de l'Économie Numérique et des Télécommunications dans le cadre de la Stratégie « Sénégal Numérique 2025 », un Projet d'Appui à la Gouvernance numérique (PAGNUM) mis en œuvre avec l'appui du PNUD.[9] Ce projet facilitera l'authentification des citoyens, améliorera la capacité des systèmes d'information de l'État et les échanges de données sur les personnes et les entreprises, afin de favoriser l'inclusion de tous les citoyens, réaliser les objectifs de développement durable, ainsi que la création de richesses.

« L'Identité Numérique National s'appuie sur la souveraineté nationale des données numériques et englobera les technologies de pointe comme l'Intelligence artificielle ou les objets connectés »[10] selon Achime Malick Ndiaye, Directeur des TIC au Ministère de l'Économie Numérique et des Télécommunications.

Les programmes de collecte de données biométriques, d'identité numérique et de localisation de donnée sont des techniques informatiques permettant de situer l'emplacement géographique des données, de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, comportementales et de l'enregistrement des faits d'état civil.

Les données biométriques sont des données à caractère personnel car elles permettent d'identifier une personne. Elles ont, pour la plupart, la particularité d'être uniques et permanentes.[11]

---

[8] https://citizenshiprightsafrica.org/senegal-decret-n-2016-1536-du-29-septembre-2016-portant-application-de-la-loi-n-2016-09-du-14-mars-2016-instituant-une-carte-didentite-biometrique-cedeao/?lang=fr .

[9] https://www.socialnetlink.org/2022/06/25/identite-numerique-nationale-le-senegal-vers-une-phase-de-transformation-de-ses-services/ .

[10] https://www.wearetech.africa/fr/fils/actualites/tech/le-senegal-lance-le-projet-d-identite-numerique-nationale .

[11] https://www.cnil.fr/fr/biometrie .

La donnée est désormais au cœur de l'ensemble des activités d'une entreprise, d'où la nécessité de bien gérer ces données, et d'en garantir l'exactitude et l'intégrité. En ce sens, la gouvernance des données consiste à identifier, classifier, gérer et contrôler les données, à travers de multiples processus métiers, acteurs et mécanismes de prise de décision, partagés à travers toute l'entreprise.[12]

De plus, la gouvernance des données regroupe des processus, des rôles, des politiques, des normes et des mesures qui garantissent une utilisation efficace de l'information pour permettre à une entreprise d'atteindre ses objectifs. Elle définit les processus et responsabilités qui garantissent la qualité et la sécurité des données utilisées au sein d'une entreprise.

En d'autre terme, la gouvernance des données est le cadre d'organisation permettant d'établir la stratégie, les objectifs et les politiques dont la résultante est une gestion efficace des données de l'entreprise. Elle comprend les processus, les politiques, l'organisation, les compétences et les technologies nécessaires pour gérer et garantir la disponibilité, la facilité d'utilisation, l'intégrité, la constance, l'auditabilité et la sécurité de vos données.[13]

Une stratégie de gouvernance des données bien conçue est vitale pour toute entreprise manipulant des données.

Un cadre de gouvernance des données planifié avec soin englobe les rôles et les responsabilités stratégiques, tactiques et opérationnels. C'est pour cette raison que la gouvernance de données s'articule autour de cinq éléments essentiels selon ANDSI[14] :

- des processus identifiés pour couvrir les besoins de la gouvernance des données ;
- des rôles clairement définis pour responsabiliser les acteurs et organiser la gouvernance ;
- des responsabilités de chaque rôle sur les activités de la gouvernance formalisées de façon détaillée ;
- des instances établies pour structurer et piloter la gouvernance des données ;
- un socle documentaire et d'outillage facilitant la mise en œuvre opérationnelle.[15]

---

[12] La gouvernance des données : un moteur de création de valeur, https://synotis.ch/data-gouvernance/gouvernance-des-donnees-moteur-de-creation-de-valeur/ .

[13] La gouvernance de la donnée : condition de la réussite de vos projets IA, Proposé par Charles-Eric de La Chapelle, disponible sur : https://myriad-data.com/livre-blanc/myriad-livre-blanc-gouvernance-de-la-donnee.pdf .

[14] Association Nationale des Dirigeants en Sciences de l'Information.

[15] La gouvernance des données, par Association Nationale des Dirigeants en Sciences de l'Information (ANDSI), https://andsi.fr/wp-content/uploads/2021/01/ANDSI_gouvdonne%CC%81es_081220.pdf .

Ainsi donc, il est clair que la gouvernance des données est un processus opérationnel qui renvoie à la définition des données, la qualité des données, la gestion du cycle de vie des données et l'utilisation des données.

II. Le cadre légal de la gouvernance des données personnelles

Inspirer par les principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel édictés par l'Assemblée Générale de l'ONU en 1990, les exigences européennes en matière de transfert de données vers des pays tiers et les principes fondamentaux consacrés par la loi d'orientation sur la société de l'information[16], le Sénégal s'est doté de sa première loi relative à la protection des données à caractère personnel en 2008 et de son de son décret d'application.[17]

Cette loi a pour objective de protéger ce qui relève de la vie privée des individus face à la prolifération des technologies de l'information et des communications ; 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. De ce fait, la législation sur les données à caractère personnel s'avère être un instrument de protection générale à l'égard des droits et libertés fondamentaux de la personne.

Le champ d'application de la loi sur les données à caractère personnel est large. Sont soumis à la présente loi[18] :

1) Toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel 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 3 de la présente loi ;

3) Tout traitement mis en œuvre par un responsable tel que défini à l'article 4.14 de la présente loi sur le territoire sénégalais ou en tout lieu où la loi sénégalaise s'applique ;

4) Tout traitement mis en œuvre par un responsable, établi ou non sur le territoire sénégalais, qui recourt à des moyens de traitement situés sur le territoire sénégalais, à l'exclusion des moyens qui ne sont utilisés qu'à des fins de transit sur ce territoire. Dans les cas visés à l'alinéa précédent, le responsable du traitement doit désigner un représentant établi sur le territoire sénégalais, sans préjudice d'actions qui peuvent être introduites à son encontre ;

---

[16] Exposé des motifs de la loi de 2008 portant sur les données à caractère personnel.

[17] DECRET n° 2008-721 du 30 juin 2008 portant application de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel, J.O. N° 6443 du Samedi 20 DECEMBRE 2008.

[18] Article 2 de la loi de 2008 portant sur les données à caractère personnel.

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 économique ou financier important de l'Etat, sous réserve des dérogations que définit la présente loi et des dispositions spécifiques en la matière fixées par d'autres lois.

Cependant, la loi ne s'applique pas :

• 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 systématique à des tiers ou à la diffusion ;

• 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.

Mais depuis l'entrée en vigueur de la loi précitée, l'environnement des réseaux numériques a connu de profondes mutations avec l'essor des mégadonnées et des dispositifs biométriques ainsi que l'avènement des technologies innovantes comme l'internet des objets, l'intelligence artificielle et l'informatique des nuages, etc.

Aussi, dans un contexte marqué par la patrimonialisation des données personnelles, on assiste à la profusion des techniques intrusives (géolocalisation, cybersurveillance, etc.) qui exposent l'intimité de la vie privée des personnes à de nouveaux risques.

A cela, s'ajoute l'utilisation des réseaux sociaux et la numérisation de la médecine, tant pour la recherche scientifique que les dossiers de patients.

C'est fort de constat que l'Etat du Sénégal juge nécessaire de procéder à la refonte du dispositif de protection des données à caractère personnel par une réforme en profondeur de la loi de janvier 2008 sus mentionnée par un projet de loi en processus depuis 2019.

Le projet de loi de 2019 est une étape importante vers la mise en place d'un cadre de protection des données personnelles modernisé au Sénégal, qui respecte les droits fondamentaux et fournit un environnement favorable à l'innovation dans un monde de plus en plus numérisé.

En substance, ce projet de loi a la particularité d'être innovateur en ce sens qu'il prévoie un encadrement sur les nouveaux domaines tels que le cloud, l'intelligence artificielle, la biométrie, les méga données, la géolocalisation et l'aménagement de régimes spécifiques aux traitements des données médicales, des salariés. Il aborde également les insuffisances dans la législation actuelle concernant la composition et l'autonomie de l'autorité de surveillance, les mécanismes pour l'auto-déclaration et de la coopération avec les autres autorités de protection des données à caractère personnel et aux flux transfrontières des données.

En d'autre terme, le projet de loi de 2019 renforce les pouvoirs de la CDP qui dispose désormais d'un pouvoir d'autosaisine ; des droits des personnes (droit à l'oubli) et instaure une minorité numérique. Une réorganisation de sa composition est opérée afin de veiller à la bonne application de la loi.

Pour assurer en bon escient cette nouvelle réglementation dans son ensemble, partant du renforcement dess pouvoirs d'investigation et des garanties d'indépendance des membres et des agents, le projet de loi propose la création d'une l'Autorité de Protection des Données à Caractère Personnel (APDP) pour remplacer la CDP actuelle.

Le projet de loi de 2019 constitue un vrai changement de paradigme en matière de régulation de la protection des données. En effet, pour mieux permette un traitement équitable et garantir les principes d'égale accès à l'autorité, hormis les personnes physiques, les personnes morales légalement constituées ont maintenant la possibilité de déférer leurs requêtes auprès de la nouvelle institution.

Par ailleurs, souhaitant renforcer son dispositif juridique et tenant en compte des standards internationaux en matière de protection des données personnelles, le Sénégal a adhéré[19] à la Convention n°108 du 28 janvier 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Cette convention constitue le premier instrument international juridiquement contraignant à vocation universelle dans le domaine de la protection des données. Ainsi donc, la Convention renforce le cadre juridique sénégalais, et le protocole additionnel[20] créé un espace commun naturel d'échange et de facilitation des flux transfrontières de données.

Le droit à la protection des données à caractère personnel tel qu'établi par ces textes vise à garantir le respect des droits et des libertés fondamentales. La Convention 108 soulignait que « dans certaines conditions, l'exercice d'une complète liberté de traiter les informations risque de nuire à la jouissance d'autres droits fondamentaux (par exemple les droits à la vie privée, à la non-discrimination et à un procès équitable) ou à d'autres intérêts personnels légitimes (par exemple en matière d'emploi ou de crédit à la consommation). C'est pour maintenir un juste

---

[19] CONVENTION 108 DU CONSEIL DE L'EUROPE : Le Sénégal devient le 50ème Etat membre adhérant : « Le Conseil des Ministres qui s'est tenu le 08 juin 2016 a adopté le projet de loi autorisant le Président de la République à ratifier la Convention. Suite à cela, l'Assemblée nationale a voté la loi le 24 juin 2016, (d'où) qui a permis la signature des instruments de ratification, le 03 août 2016. Ainsi, la Convention et son Protocole additionnel entreront en vigueur au Sénégal ce 1er Décembre 2016 », https://www.cdp.sn/content/convention-108-du-conseil-de-l%E2%80%99europe-le-s%C3%A9n%C3%A9gal-devient-le-50%C3%A8me-etat-membre-adh%C3%A9rant

[20] Le Protocole additionnel ouvert à la signature le 8 novembre 2001 impose aux Parties de mettre en place des autorités de contrôle, exerçant leurs fonctions en toute indépendance, qui sont un élément de la protection effective des personnes à l'égard du traitement des données à caractère personnel, https://www.coe.int/en/web/data-protection/convention108-and-protocol.

équilibre entre les différents droits et intérêts des personnes que la Convention impose certaines conditions ou restrictions au traitement d'informations. »[21]

Le Sénégal a aussi ratifié la Convention de l'Union Africaine (UA) sur la Cybersécurité et la protection des données à caractère personnel[22] qui a été adoptée par la 23ème Session Ordinaire de la Conférence de l'Union qui s'est tenue le 27 juin 2014 à Malabo, République de la Guinée Equatoriale.

L'article 8 de la présente convention prévoit que : « Chaque État partie s'engage à mettre en place un cadre juridique ayant pour objet de renforcer les droits fondamentaux et les libertés publiques, notamment la protection des données physiques et de réprimer toute infraction relative à toute atteinte à la vie privée sans préjudice du principe de la liberté de circulation des données à caractère personnel ; de garantir que tout traitement, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques tout en prenant en compte les prérogatives de l'État, les droits des collectivités locales et les buts pour lesquels les entreprises ont été créées ».

En sus de la Convention de Malabo, s'ajoute l'Acte additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO[23], Abuja 16 février 2010. En plus de l'harmonisation des législations, l'Acte additionnel prévoit un dispositif de protection des données personnelles face aux risques qui peuvent résulter de l'utilisation des TIC.

Cet acte additionnel a été complété par la Directive de la CEDEAO du 19 aout 2011 portant sur la cybercriminalité[24], qui détermine les infractions pénales en matière de protection des données à caractère personnel.

Par ailleurs, le droit à la protection des données à caractère personnel est gouverné par des principes directeurs. A titre d'exemple les principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel issus de la Résolution 45/95 du 14 décembre 1990.[25] Certes non contraignants, ces principes établissement des garanties minimales de licéité, de loyauté de la collecte et du traitement des données à caractère

---

[21] Point 25, du Rapport explicatif à la Convention 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, Strasbourg, 28 janv. 1981.

[22] https://www.afapdp.org/wp-content/uploads/2018/06/CONV-UA-CYBER-PDP-2014.pdf .

[23] https://www.afapdp.org/wp-content/uploads/2018/06/CEDEAO-Acte-2010-01-protection-des-donnees.pdf .

[24] Directive C/DIR/1/08/11 du 19 aout 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO, SOIXANTE SIXIEME SESSION ORDINAIRE DU CONSEIL DES MINISTRES Abuja, 17 – 19 Août 2011, disponible sur : http://www.osiris.sn/IMG/pdf/directive_cybercriminalite_fr_rev2.pdf .

[25] Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, Adoptée le 14 décembre 1990 par l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990, http://hrlibrary.umn.edu/instree/french/Fq2grcpd.html .

personnel, d'exactitude, de finalité, de non-discrimination et sécurité des fichiers.

Dans la même logique, l'article 13 de la Convention de Malabo dégage les six principes suivants relatifs à la protection des données :

• Consentement et légitimité ;

•Traitement loyal et équitable ;

• Objectif, pertinence et conservation des données ;

• Exactitude des données pendant leurs durées de vie ;

• Transparence du traitement ;

• Confidentialité et sécurité des données à caractère personne.

A l'instar de l'Union africaine, du Conseil de l'Europe et de l'ONU, l'Organisation Internationale de la Francophonie (OIF) à travers plusieurs initiatives[26] dont le Sommet de la Francophonie de Dakar (29-30 novembre 2014) a permis aux chefs d'Etat et de gouvernement de réitérer leur appel en vue de « l'adoption et de l'application de normes mondiales et de législations nationales définissant les principes d'une protection effective des données personnelles ».

Par ailleurs, la Loi n° 2016-09 du 14 mars 2016 instituant une carte d'identité biométrique CEDEAO et le Décret n° 2016-1536 du 29 septembre 2016 portant application de la loi n° 2016-09 du 14 mars 2016 instituant une carte d'identité biométrique CEDEAO[27] constituent le cadre législatif de la gouvernance du point de vue de l'identité numérique. La loi de 2016 a abrogé les dispositions contenues dans la loi n° 2005-28 du 06 septembre 2005 instituant la carte nationale d'identité sénégalaise numérisée. L'objectif est d'améliorer l'échange de données, de faire avancer la migration intra-régionale, de limiter le passage illégal aux frontières et de s'attaquer aux problèmes qui en découlent en matière de sécurité.

III. Le cadre institutionnel de la gouvernance des données

Assurer la gouvernance des données à caractère personnel revient à sécuriser les informations et faire respecter les règles de protection des données. Ce respect ne peut se faire que par

[26] Déclaration de Ouagadougou (Burkina Faso), 26-27 novembre 2004 sur la reconnaissance du droit à la protection des données personnelles ; Déclaration de Bucarest (Roumanie), 28-29 septembre 2006 sur l'intensification des travaux nécessaires à l'adoption de législations et de règlementation assurant la protection des personnes, de leurs libertés et de leurs droits fondamentaux dans l'utilisation des fichiers et le traitement de données à caractère personnel.

[27] http://www.jo.gouv.sn › spip › article11135.

l'institution d'un ou de plusieurs organismes chargés de contrôler le respect des dispositions législatives et règlementaires en la matière.

- **L'institution de la Commission de Protection des Données Personnelles (CDP)**

Pour rappel, c'est la loi 2008 qui constitue le cadre légal et institutionnel de protection des données à caractère personnel. Cette loi institue une Commission de Protection des Données à Caractère Personnel dite « Commission des Données Personnelles » en abrégé la « CDP »[28]. La commission des données personnelles 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 présente loi.

Elle est la garante du respect de la vie privée dans le traitement des données personnelles. Elle vient ainsi protéger un droit : « *le droit à la protection des données à caractère personnel* ».

La CDP a Trois (3) principales missions au regard des termes de l'article 16 de la loi de 2008.

Une mission de veille, de sensibilisation, de conseils et de propositions[29]:

- ✓ Veille à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions légales ;
- ✓ Informe les personnes concernées et les responsables de traitement de leurs droits et obligations ;
- ✓ S'assure que les Technologies de l'Information et de la Communication (TIC) ne comportent pas de menace au regard des libertés publiques et de la vie privée des sénégalais ;
- ✓ Homologue les chartes d'utilisation présentées par des responsables de traitement de l'information ou de données ;
- ✓ Tient un répertoire des traitements des données à caractère personnel à la disposition du public ;
- ✓ 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 ;
- ✓ Présente au gouvernement toute suggestion susceptible de simplifier et d'améliorer le cadre législatif et réglementaire à l'égard du traitement des données ;
- ✓ Formule toutes recommandations utiles en vue de veiller à ce que les traitements des données à caractère personnel soient mis en œuvre conformément aux dispositions en

[28] Article 5 de la loi de 2008 sur la protection des données à caractère personnel.
[29] https://www.cdp.sn/content/une-mission-de-veille-de-sensibilisation-de-conseils-et-de-propositions .

vigueur ;

- ✓ Coopère avec les autorités de protection des données à caractère personnel des pays tiers et participe aux négociations internationales en matière de protection des données à caractère personnel.

Une mission d'instruction des dossiers, à ce titre, la CDP :

- ➢ Reçoit les formalités préalables (les déclarations, les demandes d'autorisation) à la création de traitements des données à caractère personnel ;
- ➢ 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 ;
- ➢ Répond à toute demande d'avis ;
- ➢ Autorise les transferts transfrontaliers de données à caractère personnel.

Une mission de contrôle et d'investigation

- Informe sans délai le procureur de la République des infractions dont elle a connaissance ;
- Peut charger un ou plusieurs de ses membres ou des 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 ;
- Peut prononcer une sanction à l'égard d'un responsable de traitement.[30]

En outre, face au développement du recours aux technologies de l'information dans les administrations publiques et privées et qui a comme corollaire, entre autres, la numérisation du fichier électoral et de la carte d'identité nationale, la collecte et le traitement des données à caractère personnel sont devenus monnaie courante.[31] Cette propension à l'utilisation des données dans les secteurs publics, privés et par des tiers incite la CDP à faire beaucoup de sensibilisation auprès des populations.

C'est à ce titre d'ailleurs que, « *le Chef de l'Etat a demandé aux membres du Gouvernement de faire prendre, par les entités sous leurs tutelles, toutes les mesures appropriées, pour faire déclarer les traitements des données personnelles auprès de la Commission des données*

[30] A titre d'exemple, la DELIBERATION N°2017-00307/CDP DU 20 OCTOBRE 2017 METTANT EN DEMEURE EXPRESSO TELECOMS SENEGAL POUR MANQUEMENT AUX DISPOSITIONS DE LA LEGISLATION SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNE, https://www.cdp.sn/content/mise-en-demeure-expresso-t%C3%A9l%C3%A9coms-s%C3%A9n%C3%A9gal des avertissements, **Hello Food Sénégal,** pour manquement à la législation sur les données à caractère personnel 15 mai 2015.

[31] O. THIONGANE, Les promesse du numérique, Editions Sédar, P. 74.

*personnelles (CDP) et de renforcer las allocations budgétaires à la CDP tout en assurant la révision de la loi encadrant son fonctionnemen*t »[32].

La CDP a aussi mis en ligne une plateforme informative.[33] Les particuliers qui souhaitent en savoir plus sur leurs droits sont guidés: « chaque personne dont les données à caractère personnel font l'objet d'un traitement dispose d'un certain de droits c'est-à-dire d'un ensemble des règles qui lui permettent d'exercer un contrôle sur l'usage qui peut être fait de ces données ». C'est-à-dire un ensemble de droits dont le droit à l'information[34], du droit d'accès[35], du droit d'opposition[36] et du droit de rectification et supression.[37]

- **L'apport du Sénégal numérique SA ex ADIE dans la gouvernance des données**

Structure administrative autonome, l'ADIE[38] est le principal levier de la mise en œuvre du projet e-Gouvernement. Elle a pour mission essentielle de mettre en œuvre la politique d'informatisation définie par le Président de la République. A ce titre, elle est chargée de mener et de promouvoir, en coordination avec les différents services de l'Administration, les autres organes de l'Etat et les collectivités locales, tous types d'actions permettant à l'Administration de se doter d'un dispositif cohérent de traitement et de diffusion de l'information, répondant aux normes internationales de qualité, de sécurité, de performance et de disponibilité. Elle s'occupe aussi de la mise en œuvre des systèmes d'information et des infrastructures réseaux de l'Etat[39].

---

[32] Communiqué du Conseil des ministres du 9 octobre 2019, in, O. THIONGANE, Les promesse du numérique, Editions Sédar, P. 74.

[33] https://www.cdp.sn/content/comprendre-vos-droits .

[34] Chacun a un droit de regard sur vos données personnelles. Lorsque des données à caractère personnel sont collectées directement auprès de la personne concernée, le responsable du traitement doit fournir à celle-ci, au plus tard, lors de la collecte et quels que soient les moyens et supports employés, les informations suivantes : son identité et, le cas échéant, celle de son représentant ; la ou les finalités du traitement auquel les données sont destinées ; les catégories de données concernées ; le ou les destinataires ou les catégories de destinataires auxquels les données sont susceptibles d'être communiquées ; le fait de savoir si la réponse aux questions est obligatoire ou facultative ainsi que les conséquences éventuelles d'un défaut de réponse ; le fait de pouvoir demander à ne plus figurer sur le fichier ; l'existence d'un droit d'accès aux données la concernant et de rectification de ces données ; la durée de conservation des données ; le cas échéant, l'éventualité de transferts de données à caractère personnel à destination de l'étranger, https://www.cdp.sn/content/comprendre-vos-droits .

[35] Chacun a le droit de savoir si ses données personnelles font l'objet d'un traitement. 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 les informations permettant de connaître et de contester le traitement, https://www.cdp.sn/content/comprendre-vos-droits .

[36] 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, https://www.cdp.sn/content/comprendre-vos-droits .

[37]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, https://www.cdp.sn/content/comprendre-vos-droits .

[38] Article 1 ; Décret n° 2011-1158 du 17 août 2011 modifiant le Décret n° 2004-1038 du 23 juillet 2004 portant création et fixant les règles d'organisation et de fonctionnement de l'ADIE ; J.O. N° 6639 du samedi 14 janvier 2012.

[39] Article 3 ; Op. cit.

Il est important de noter que l'expertise et le leadership de l'ADIE sont aussi reconnus au niveau international. L'Agence bénéficie d'une reconnaissance de structures étatiques et privées dans les pays de la sous-régions, lesquelles effectuent régulièrement des missions de benchmarketing pour s'inspirer de son fonctionnement, son mode de gouvernance ou encore de son expérience en matière d'exécution des projets comme le projet FUDPE et les projets liés à la Cybersécurité entre autres.[40]

Au plan national, l'ADIE a rendu possible la mise en place d'un point d'échange internet au Sénégal en fin 2016, pour asseoir durablement la souveraineté du Sénégal sur ses données.[41] Elle a fait beaucoup de réalisations en matière de gouvernance numérique, notamment par l'intégration et l'adoption des télé-services dans plusieurs secteurs et la mise en place du FUDPE, le Fichier Unifié des Données du Personnel de l'Etat. Selon Ousmane THIONGANE[42], FUDPE a pour but de contribuer à la transparence et à l'amélioration de la gestion des finances publiques ainsi qu'au renforcement de la bonne gouvernance, par la maîtrise des données qui impactent régulièrement sur un des plus gros postes de dépenses du budget général de l'Etat, à savoir le poste « *dépenses de personnel* ».

La nouvelle société nationale, Sénégal Numérique SA[43] (SENUM SA) pourra contribuer de manière significative à l'amélioration du secteur du numérique au Sénégal en matière de partages et de déploiement d'infrastructures, d'hébergement, d'innovation technologique, de concert avec les différents acteurs du secteur à l'instar des opérateurs, des fournisseurs d'accès Internet, des créateurs de contenu, des universités, etc.[44] La stratégie Sénégal Numérique ambitionne de faire du pays une locomotive de la sous-région en matière de digitalisation et de bonne gouvernance.

- **Le Datacenter de Diamniadio, socle de la souveraineté digitale du Sénégal**

Inauguré le 22 juin, le Data Center de Diamniadio est présenté comme un « *outil de souveraineté numérique* », qui va permettre de stocker les données de l'administration, et celles du secteur privé. Une « *révolution* » selon les autorités, notamment pour faciliter la

[40] https://www.adie.sn/leadership-et-gouvernance .
[41] https://www.adie.sn/leadership-et-gouvernance .
[42] Conseiller Spécial à la Présidence de la République du Sénégal et Coordonnateur de la Cellule Digitale de la Présidence.
[43] https://www.sentresor.org/app/uploads/Loi-n%C2%B02021-39-du-13-12-2021-autorisant-cre%CC%81ation-Socie%CC%81te%CC%81-Se%CC%81ne%CC%81gal-nume%CC%81rique-SA-SENUM-SA.pdf .
[44] https://www.adie.sn/agence/le-mot-du-directeur-g%C3%A9n%C3%A9ral .

dématérialisation des démarches administratives. Un projet qui fait partie du Plan Sénégal Émergent, réalisé avec la coopération chinoise.[45]

Cette infrastructure va permettre de franchir un autre cap qui est la souveraineté des données de l'État. Ce data center va pouvoir héberger l'ensemble des données de l'administration à moindre coût.[46] L'État est très soucieux de la protection des données des sénégalais.

Ce pourquoi, SEM Macky SALL, a instruit le gouvernement et toutes les structures de l'Etat à faire héberger, dorénavant l'ensemble des données et plateformes de l'État dans cette infrastructure aux normes et de procéder à la migration rapide des données hébergées à l'étranger ou ailleurs dans l'Administration dans des locaux non conformes aux standards internationaux.[47]

La mise en service du Centre de données de Diamniadio va consacrer le positionnement du pays comme un hub technologique régional. En effet, selon le Directeur Général de l'Agence de l'informatique de l'État (ADIE) : « *L'Afrique regroupe à peine 1% des Data Center au niveau mondial, ce qui fait qu'aujourd'hui, les données, nous sommes obligés de payer pour y accéder. Donc, aujourd'hui, le Sénégal dispose du plus grand Data Center dernière génération de l'Afrique de l'Ouest, avec presque mille mètres carrés de salles techniques et 1,4 MW de puissance énergétique.* ».[48]

Ce Datacenter est le lieu d'impulsion de la transformation digitale du Sénégal.[49] Il favorise le fonctionnement du guichet unique Sénégal Services présent dans tous les départements et où les citoyens peuvent disposer de l'ensemble des services de l'administration.[50]

La gouvernance des données personnelles est assurée principalement par le Data Center. Cette gouvernance des données permet ainsi de garantir que les données critiques sont disponibles au bon moment, pour la bonne personne, dans une forme standardisée et fiable. Une bonne gouvernance des données induit des pratiques qui optimisent la valeur des données en

---

[45] Sur l'ensemble de la question voir : **https://www.rfi.fr/fr/afrique/20210622-s%C3%A9n%C3%A9gal-inauguration-d-un-data-center-pr%C3%A8s-de-dakar-une-r%C3%A9volution.**

[46] Incursion au Data center de Diamniadio : une infrastructure de 10 milliards de FCfa bâtie sur plus d'1 ha ... plus de 15 000 emplois en perspectives, http://www.osiris.sn/Incursion-au-Data-center-de.html .

[47] **https://www.adie.sn/actualites/le-datacenter-de-diamniadio-lieu-d%E2%80%99impulsion-de-la-transformation-digitale-du-s%C3%A9n%C3%A9gal .**

[48] **https://www.rfi.fr/fr/afrique/20210622-s%C3%A9n%C3%A9gal-inauguration-d-un-data-center-pr%C3%A8s-de-dakar-une-r%C3%A9volution.**

[49] Selon le Directeur Général de l'ADI, le Centre de donnée de Diamniadio est connecté à la fibre optique de l'Etat qui maille le territoire national en 6 000 km mais aussi au câble sous-marin dont l'arrivée est prévue en fin 2021 et qui va renforcer la capacité internet de notre pays avec plus de 100 Gb/s extensible en 16 Tb/s.

[50] **https://www.adie.sn/actualites/le-datacenter-de-diamniadio-lieu-d%E2%80%99impulsion-de-la-transformation-digitale-du-s%C3%A9n%C3%A9gal .**

permettant une propriété et une traçabilité complète de la vie de la donnée ainsi devenue le carburant du système d'information.

Le Data Center de Diamniadio doit s'assurer que les données traitées répondent aux exigences d'efficacité, efficience, confidentialité, intégrité, disponibilité, conformité et fiabilité. Ces données sont un capital dont la volumétrie ne va pas cesser de croître. A cet effet, cette structure technique de l'Etat du Sénégal a pour mission de garantir la souveraineté des données publiques.

La souveraineté est, pour une nation démocratique, l'expression sans entrave sur son territoire de la volonté collective de ses citoyens. Le peuple se détermine et fait ses choix par lui-même, sans subordination ni dépendance envers une autorité étrangère. Les seules limitations du pouvoir populaire proviennent du droit international et des traités. L'État moderne est l'incarnation de cette autonomie et de cette indépendance.[51]

En plus des institutions susmentionnées, la Direction Générale du chiffre et de la sécurité systèmes d'information (DCSSI)[52] joue un rôle très important en matière de gouvernance des données. Il ressort du décret portant création et organisation de la lDirection Générale du chiffre et la sécurité des systèmes d'information, Autorite nationale de la cybersecurité renforce Ia protection du secret des informations interieures et exterieures de l'Etat ; propose aux autorités étatiques des orientations stratégiques en matiere de sécurité des systemes d'information, et de cybersecurité en général, en liaison avec les organismes intéressés, et d'en suivre la mise en œuvre.

La Direction assure également la coordination nationale des activites de detection, d'alerte, et de réponse aux cyberattaques, en collaboration avec tout organisme national ou international intervenant dans ce domaine ; assure le developpement de la sécurité du numerique, la promotion de la culture de la cybersécurité et le renforcement des capacites et des connaissances techniques en la matière dans les secteurs public et privé.[53]

La gouvernance des données ne peut être efface sans la la confiance des utilisateurs.Seule une une maîtrise globale de la sécurité des systèmes d'information et des données est indispensable que ça soit les données biométriques, de l'identité numérique et de la localisation des données hébergées. D'où l'importance de la Commission nationale de Cryptologie.[54] La cryptologie est

[51] Sur l'ensemble de la question, voir, Pierre Bellanger, La souveraineté numérique, Éditions Stock, 2014, P. 15.

[52] Décret n°2021-35 du 14-01-2021 création et organisation Direction Générale du chiffre et sécurité systèmes d'information DCSSI.

[53] Article 2 du Décret n°2021-35 du 14-01-2021 création et organisation Direction Générale du chiffre et sécurité systèmes d'information DCSSI.

[54] Les conditions de fonctionnement sont fixées par la loi n° 2008-41 du 20 aout 2008 sur la Cryptologie ainsi que

la solution technique incontournable pour protéger les échanges et les systèmes d'information sur les nouvelles technologies notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation des données transmises.

IV. Atteintes spécifiques aux droits des personnes au regard du traitement des données à caractère personnel

La gestion des données personnelles est devenue aujourd'hui un enjeu stratégique de dimension mondiale car, interpelle les Etats et devient l'objet de convoitise des GAFAM.

Qualifiée de denrée précieuse, les données personnelles sont utiles au développement de l'économie numérique. Conscient de son importance, l'Etat du Sénégal est dans une dynamique de réguler la collecte et l'utilisation des données à caractère personnel. D'ailleurs, le Président Macky Sall, soucieux de l'enjeu de l'utilisation des données personnelles n'a pas manqué l'occasion de souligner dans son discours à l'audience solennelle de rentrée des cours et tribunaux du 8 juin 2019, que les données sont « *sources de progrès et de création de richesse* ».[55]

Bien important et nécessaire, ce carburant de l'économie numérique est source de problème et d'atteinte à la vie privé par l'usage des techniques comme le traçage, l'analyse comportementale, la géolocalisation, l'identification numérique entre autres.

Le respect de la vie privée peut se résumer à l'idée selon laquelle « *la vie privée est cette partie de la vie qui n'est pas consacrée à une activité publique et où les tiers n'ont en principe pas accès, afin d'assurer à la personne le secret et la tranquillité auxquels elle a le droit* »[56]. Eu égard à cette tentative de définition, la vie privée renvoie à la liberté d'entretenir des relations avec d'autres individus à l'abri de toute ingérence extérieure[57]. Ainsi, « *nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes* »[58].

---

par Ie décret d'application n" 2010-1209 du 13 septembre 2010 modifié et completé par Ie decret n" 2012-1508 du 31 décembre 2012.

[55] O. THIONGANE, Les promesse du numérique, Editions Sédar, P. 119.

[56] A. ROUX, La protection de la vie privée dans les rapports entre l'État et les particuliers, Presses Universitaires d'Aix-Marseille, 1983, 279 pages.

[57] Déjà en 1236, la Charte de Kurukan Fuga prévoyait à son article 41« n'humiliez pas votre ennemi ». Sur cette question, Voir T. A. NDIOGOU, « Regards croisés sur la charte de Kurukan Fuga et la déclaration universelle des droits de l'homme », in Les sciences sociales au Sénégal : Mise à l'épreuve et nouvelles perspectives, CODESRIA, Vol. 1, 2016, p. 50, in « REFLEXIONS SUR LA NOUVELLE LEGISLATION SENEGALAISE ANTITERRORISTE », par Th. A. NDIOGOU, *op. cit*., p. 39.

[58] Déclaration Universelle des Droits de l'Homme du 10 décembre 1948, Art. 12 ; Convention Européenne des Droits de l'Homme, Art. 8 et ses Protocoles 1, 4, 6 et 7.

En ce sens, il résulte de l'article 35 alinéa 2 de la loi sur les données à caractère personnel que les données personnelles « *doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectés et traitées ultérieurement* »[59].

Même si par principe la loi[60] interdit de procéder à la collecte et à tout traitement qui révèlent l'origine raciale, ethnique 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, on note des cas de violations flagrantes des données à caractère personnel.

Concernant le respect de la confidentialité des correspondances[61], le droit constitutionnel sénégalais a consacré le principe du secret des correspondances. Aux termes de l'article 13 de la constitution du 7 janvier 2001, *« le secret de la correspondance, des communications postales, télégraphiques, téléphoniques et électroniques est inviolable. Il ne peut être ordonné de restriction à cette inviolabilité qu'en application de la loi* ». L'article 431-12 du Code pénal protège la confidentialité des données de contenu en incriminant l'interception fraudeuse de données.

Cependant, l'affirmation du principe de la confidentialité des données électroniques souffre de dérogations tenant essentiellement aux nécessités d'ordre public de l'enquête. Les réseaux modernes disposent de grandes capacités de diffusion d'information sous forme de texte, d'images et de son. Ils offrent par la même occasion de plus vastes possibilités aux cybercriminelles de commettre des infractions impliquant la transmission de contenus illicites[62].

Sur la base des dispositions de la Loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal[63] (Articles 431-14 à 431-28) déterminant les violations de la vie privée et des données personnelles du fait des activités d'information. A titre d'exemple, Celui qui, même par négligence, procédé ou fait procéder à des traitements de

[59] La loi n° 2008 – 12 sur la Protection des données à caractère personnel.
[60] Article 40 de la loi de 2008 sur les données à caractère personnel.
[61] Le respect de la correspondance n'est pas une préoccupation propre aux sociétés modernes. Dès 1742, une déclaration royale punissait de la peine de mort la violation de la correspondance privée. En 1775, un arrêt du Conseil du roi proclamait que : « Tous les principes mettent la correspondance secrète des citoyens au rang des choses sacrées dont les tribunaux comme les particuliers doivent détourner les regards », tandis que le « cabinet noir » du roi permit une information politique qui fut dénoncée dans les cahiers de doléances rédigés lors des états généraux de 1789 (Doc. AN, projet de loi no 2068, p. 2). Le XIXe siècle connaîtra l'utilisation de mesures avoisinantes (Cass. ch. réunies 31 janv. 1888, S. 1889. 1. 241, concernant le fait, pour un juge d'instruction, de se faire passer pour l'inculpé dans une conversation téléphonique avec un présumé complice de celui-ci), in « Les écoutes téléphoniques judiciaires », par P. DOURNEAU-JOSETTE, *op. cit*., p. 2.
[62] P. A. TOURE, *op. cit*., p. 364.
[63] JORS n°6975.

données à caractère personnel sans avoir respecté les formalités préalables à leur mise en œuvre prévues par la loi sur les données à caractère personnel, est puni d'un emprisonnement d'un an à sept ans et d'une amende de 500.000 francs à 10. 000. 000 de francs ou de l'une de ces peines.

V. Les risques potentiels liés à la collecte de données biométriques

Aujourd'hui, la biométrie fait partie intégrante du quotidien des sénégalais. Reconnaissance faciale, empreinte digitale, la vérification d'identité, les techniques de biométrie sont multiples et n'ont pas fini de se développer. L'utilisation de ces données présente des avantages pour la sécurité publique, mais, dans certains cas, des dérives sont pointées du doigt.

Les programmes biométriques sont mis en œuvre alors que la protection des droits numériques est médiocre sans compter les menaces croissantes au droit à la vie privée et aux violations des données personnelles, ce qui jette un doute sur l'intégrité des programmes de bases de données biométriques, de l'identité numérique et de la localisation des données.

Les risques liés à l'utilisation des données biométriques sont majeurs et particulièrement dangereux pour les populations. Ces principaux risques sont le piratage et les violations de données, les cyberattaques, l'usurpation d'identité et la fraude. Ces risques potentiels pourraient être aggravés lorsque les données sont stockées dans des bases de données centralisées et lorsque les politiques de sécurité de l'information sont inadéquates. C'est notamment le cas lorsque les bases de données sont interconnectées avec d'autres agences gouvernementales et reliées pour fournir des services pratiques tels que l'authentification pour les services financiers, les élections, l'enregistrement des cartes SIM ou la fourniture de services sociaux, sans tenir compte des conséquences d'une diffusion généralisée des données.[64]

En général, les risques d'atteinte à la vie privée proviennent de l'État qui cherche à obtenir des renseignements sur des personnes cibles, par l'imprécision de la règlementation ou le recours à la géolocalisation. A titre d'exemple, la législation sénégalaise sur les interceptions des données ne prévoit pas certaines conditions de sauvegarde de la vie privée expressément exigées par le rapport explicatif de la Convention de Budapest sur la cybercriminalité[65].

Sans oublier le traitement des données personnelles par les entreprises privées et le traitement aux fins de journalisme.

---

[64] Sur l'ensemble de la question de la question : État de la liberté de l'Internet en Afrique 2022 : l'essor de la surveillance biométrique (cipesa.org).

[65] En principe, la modification des données de trafic aux fins de faciliter les communications anonymes (comme dans le cas des activités des systèmes de réexpédition anonyme) ou la modification des données aux fins d'assurer la protection des communications (chiffrement, par exemple) sont considérées comme assurant la protection légitime de la vie privée et, de ce fait, sont considérées comme étant réalisées de façon légitime.

En vérité, les insuffisances législatives sont de nature à favoriser des atteintes à la vie des citoyens qui ne disposent pas toujours de garanties suffisantes.

Plusieurs entités privées et publiques collectent des données personnelles au Sénégal. Par exemple, il existe un enregistrement obligatoire de la carte SIM[66] lié à la base de données nationale d'identité. Cependant, de nombreux cas de non-respect de la loi sur la protection des données et des règlements de la Commission des données personnelles (CDP) ont été signalés. Voir, par exemple, l'avis trimestriel du CDP.[67]

Le plus gros problème avec les données biométriques n'est pas la technologie de stockage ou d'authentification utilisée, mais la nature statique des données biométriques elles-mêmes.[68] C'est à juste raison que William Culbert, directeur Europe du Sud de BeyondTrust a donné l'exemple suivant : « Si un mot de passe est compromis, vous pouvez le changer et empêcher ainsi les attaques visant à réutiliser un mot de passe compromis. Mais si des données biométriques sont compromises, vous ne pouvez pas les changer. Vos yeux, votre visage ou vos empreintes digitales sont reliés en permanence à votre identité ».[69]

VI. Conclusion

La gouvernance des données personnelles reste et demeure toujours sujette de débats voire même d'inquiétude malgré les efforts de l'Etat.

L'étude a révélé que la protection des données personnelles est un droit pour tout citoyen et une responsabilité de l'Etat. Il est donc nécessaire de renforcer le cadre légal et réglementaire de la gouvernance des données personnelles en mettant l'accent sur la coopération interétatique. La coopération internationale est une nécessité absolue car, en matière de cybercriminalité, on ne peut pas faire cavalier seul. Quand les attaques viennent d'intrus étrangers, une approche multilatérale est indispensable à l'efficacité de la cyber-répression et de la cyberdéfense.

La bonne gouvernance est possible. Elle passe par la prise de conscience par les pouvoirs publics de l'enjeu national de la souveraineté numérique et, par conséquent, de l'établissement d'une politique industrielle des réseaux informatiques et de l'Internet.

Il est temps de reconquérir notre souveraineté sur les réseaux, y retrouver la maîtrise de nos données. Telle est la souveraineté numérique. L'accomplissement de cet objectif ne dépend pas seulement notre souveraineté sur internet, mais notre souveraineté globale.

---

[66] enregistrement obligatoire de la carte SIM

[67] l'avis trimestriel du CDP.

[68] https://www.lesechos.fr/idees-debats/cercle/opinion-les-donnees-biometriques-un-risque-inedit-pour-la-securite-992773 .

[69] Les données biométriques, un risque inédit pour la sécurité, https://www.lesechos.fr/idees-debats/cercle/opinion-les-donnees-biometriques-un-risque-inedit-pour-la-securite-992773 .

VII. Recommandations

1. En vue de la réalisation des objectifs de la bonne gouvernance, l'État du Sénégal doit convoquer des forums multipartites, avec les autorités de protection des données, les contrôleurs de données et d'autres parties prenantes, pour compléter les bases juridiques par des codes de conduite volontaires mettant en œuvre les meilleures pratiques en matière de protection des données personnelles.
2. L'Etat du Sénégal devrait accélérer le processus d'adoption du projet de loi 2019 afin de renforcer la protection des droits des personnes dans l'environnement numérique.
3. Les autorités chargées de la protection des données doivent disposer des pouvoirs et des ressources nécessaires pour faire respecter le principe de la vie privée sur les fins de la collecte. Elles devraient donner des orientations aux fournisseurs et aux prestataires de services sur la nécessité de la transparence et de la responsabilité en ce qui concerne le principe de l'objet de la collecte, en tant que fondement de la confiance des consommateurs.
4. Les gouvernements doivent veiller à ce que les autorités de la protection des données disposent des ressources nécessaires pour surveiller et faire appliquer le principe de « l'objectif de collecte ».. Si nécessaire, une législation de protection des consommateurs doit être adoptée pour renforcer les droits de la personne concernée dans l'environnement numérique.
5. L'Etat du Sénégal devrait mettre en œuvre les lois et les politiques sur les systèmes d'identité et de localisation des données tout en accordant une attention particulière au respect des principes internationaux reconnus en matière de protection des données et de respect de la vie privée pour la collecte des données biométriques.
6. Nous encouragions l'Etat du Sénégal à considérer les organisations de la société civile comme des partenaires dans la sensibilisation de la population pour former des « citoyens numériques », informée, capable et à l'abri du danger.
7. L'Etat devrait améliorer la gouvernance des données personnelles par la transparence des traitements, le contrôle que les personnes peuvent exercer sur leurs données, renforcer les compétences et pouvoirs des autorités de protection des données, préciser et étendre les obligations des responsables de traitement, revoir et étendre les sanctions pénales.
8. L'efficacité et l'efficience de la gouvernance des données personnelles passent par une stabilité du cadre institutionnel et la suppression de la multiplicité des pôles de décision.

Pour une plus grande cohérence, regroupons au sein d'une même autorité des moyens humains et financiers consacrés au numérique et la création d'un conseil national du numérique, instance consultative de haut niveau regroupant l'ensemble des parties prenantes.

9. La société civile devrait continuer à jouer un rôle clé en matière de défense et de protection des droits et libertés fondamentaux en garantissant les individus contre les atteintes cybernétiques.
10. La société civile doit travailler main dans la main avec d'autres parties prenantes, y compris le gouvernement, le secteur privé, les médias afin de promouvoir la compréhension de la biométrie, notamment par la sensibilisation et le renforcement des capacités des acteurs clés en matière de protection des données et de la vie privée.

VIII. Liste des déférences

DRAME (P.F) et SARR (R), L'impact du règlement sur la protection des données (RGPD) en Afrique, L'Harmattan, 2021, 251 p.

KAMTO (M), Droit international de la gouvernance, Editions A. PEDONE, 2013, 338 p.

LO (M), *La protection des données à caractère personnel en Afrique, Réglementation et régulation,* Baol Editions, 2017, 267 p.

THIONGANE (O), Les promesse du numérique, Editions Sédar, 134 p.

TOURE (P.A.), *Le traitement de la cybercriminalité devant le juge : L'exemple du Sénégal,* L'Harmattan 2014, 616 p.

Acte additionnel 1/01/ 10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO.

Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel signée à Malabo en Guinée équatoriale le 27 juin 2014.

Loi n° 2008-12 du 25 janvier 2008, sur la protection les données à caractère personnel (JORS, n°6406, du 3 mai 2008, p.434).

Décret n° 2008-721 du 30 juin 2008, portant application de la loi 2008-12 du 25 janvier 2008 sur la protection les données à caractère personnel (JORS, n° 6443 du 20 décembre 2008).

Loi n° 2008-41 du 20 aout 2008 sur la Cryptologie ainsi que par Ie décret d'application n" 2010-1209 du 13 septembre 2010 modifié et completé par Ie decret n" 2012-1508 du 31 décembre 2012.

Loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal (JORS n°6975).

Décret n°2021-35 du 14-01-2021 création et organisation Direction Générale du chiffre et sécurité systèmes d'information DCSSI.

TOURE (P.A.), « Adoption des Conventions de Budapest et de Malabo : un pas important pour cybersécurité et de cybercriminalité » sur *www.osiris.sn* ou sur *www.pressafrik.com*

TOURE (P.A.), « La lutte contre la diffusion de contenus illicites en ligne : de nouveaux remèdes pour exorciser le cybermal », disponible sur https://www.pressafrik.com/La-lutte-contre-la-diffusion-de-contenus-illicites-en-ligne-de-nouveaux-remedes-pour-exorciser-le-cybermal-_a1