ProDP AFRICA

www.prodp-africa.com

RENFORCER LA PROTECTION DES DONNEES PERSONNELLES EN AFRIQUE : VERS UN SYSTEME HARMONISE ET EFFICIENT

Rapport Sénégal

Mars 2023

LABORATOIRE D'ANALYSE DES SOCIETES ET POUVOIRS / AFRIQUE - DIASPORAS

LASPAD - Université Gaston Berger
Route de Ngallèle, BP 234 Saint-Louis, Sénégal
Tel. +221 78 469 39 31- www.laspad.org

UNIVERSITE GASTON BERGER

LABORATOIRE D'ANALYSE DES SOCIETES ET POUVOIR – AFRIQUE / DIASPORA

Route de Rosso - BP 234

Saint-Louis du Sénégal

contact@laspad.org

www.laspad.org

Ce document fait partie d'une série de rapports destinés à contribuer aux réflexions et actions en faveur du renforcement des systèmes de protection des données à caractère personnel sur le continent africain.

Le programme ProDP Africa bénéficie du soutien financier et technique de Open Society Foundations (OSF). Que la Fondation soit remerciée pour avoir rendu possible cette recherche.

OPEN SOCIETY FOUNDATIONS

Les auteurs remercient l'ensemble des membres l'équipe, ainsi que tous les experts ayant contribué aux activités du programme : Mame-Penda Ba, Mamoudou Niane, Boubacar Diallo, Ibrahima Kane, Rachid Id Yassine et Roland Goulla.

Nos remerciements vont aussi aux jeunes chercheur·e·s et assistants de ProDP Africa : Guilheim Lein Bassène, Abdoulaye Cissé, Fatimatou Dia, Ghislaine Emma Dioh, Salomon Djidiack Faye, Janvier Owono et Pascal Sagna.

Que soient remerciées enfin toutes les personnes qui ont accepté de répondre à nos questions, de réviser et d'améliorer le rapport : Ibrahima Kane, Yaye Hélène Ndiaye, Papa Assane Touré et l'ensemble des organisations de la société civile.

LASPAD, « Renforcer la protection des données personnelles en Afrique : vers un système harmonisé et efficient. Rapport Sénégal », UGB LASPAD, Saint-Louis, mars 2023.

Le document et son résumé exécutif sont disponibles sur le site www.prodp-africa.com ou sur www.laspad.org.

Pour toute information complémentaire, veuillez contacter :

contact@laspad.org

ProDP AFRICA

Table des matières

SIGLES, ACRONYMES ET ABRÉVIATIONS

ADIE	Agence de l'informatique de l'État
AJS	Association des juristes sénégalaises
ANAIS	Advisory Network for African Information Strategies
ARTP	Autorité de régulation des télécommunications et des postes
ASCOOP	Acte uniforme sur les sociétés coopératives
AUDCG	Acte uniforme portant sur le droit commercial général
AUS	Acte uniforme portant organisation des sûretés
BCEAO	Banque centrale des États de l'Afrique de l'Ouest
BIC	Bureau d'information sur le crédit
CCJA	Cour commune de justice et d'arbitrage
CDP	Commissions de protection des données personnelles
CEDEAO	Communauté économique des États de l'Afrique de l'Ouest
CENTIF	Cellule nationale de traitement de l'information financière
CNC	Commission nationale de cryptologie
CNRA	Conseil national de régulation de l'audiovisuel
CNUCED	Conférence des Nations unies pour le commerce et le développement
COCC	Code des obligations civiles et commerciales
CTMI UEMOA	Centre de traitement monétique interbancaire de l'UEMOA
DGCSSI	Direction générale du chiffre et de la sécurité des systèmes d'information
DP	Données personnelles
FUDPE	Fichier unifié des données du personnel de l'État
GAFAM	Google, Amazon, Facebook, Apple, Microsoft
GIABA	Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest
GIM UEMOA	Groupement Interbancaire monétique de l'UEMOA
GIZ	Gesellschaft für Internationale Zusammenarbeit/ Coopération Allemande
HCR	Haut-Commissariat des Nations unies pour les réfugiés
IA	Intelligence artificielle
LDP	Loi sur la protection des données personnelles

LPSD	Lettre de politique sectorielle de développement du secteur numérique 2019-2023
MVNO	Mobile Virtual Network Operators/Opérateurs de réseau mobile virtuel (ORMV)
OCDE	Organisation de coopération et de développement économiques
ODD	Objectifs de développement durable
OHADA	Organisation pour l'harmonisation en Afrique du droit des affaires
OIM	Organisation internationale pour les migrations
ONG	Organisation non gouvernementale
ONU	Organisation des Nations unies
OPTIC	Organisation des professionnels des TIC
OQSF	Observatoire de la qualité des services financiers
OSC	Organisations de la société civile
OSIRIS	Observatoire sur les systèmes d'information, les réseaux et les inforoutes au Sénégal
OSIWA	Open Society Initiative for West Africa
PME	Petites et moyennes entreprises
RCCM	Registre du commerce et du crédit mobilier
RADDHO	Rencontre africaine pour la défense des droits de l'homme
RAES	Réseau africain pour l'éducation et la santé
SFD	Système financier décentralisé
SIMEN	Système d'information et de management de l'éducation nationale
SONATEL	Société nationale de télécommunications
STAR UEMOA	Système de transfert automatisé et de règlement dans l'UEMOA
SENUM	Sénégal numérique S.A
TDR	Termes de références
TIC	Technologies de l'information et de la communication
TNT	Télévision numérique terrestre
UEMOA	Union économique et monétaire ouest-africaine
UGB	Université Gaston Berger de Saint-Louis
UMOA	Union monétaire ouest-africaine
WURI	West Africa Unique Identification for Regional Integration and Inclusion Program

RÉSUMÉ EXÉCUTIF

Le Sénégal a commencé à légiférer sur la protection des données personnelles en 2008 par, principalement, la loi n° 2008-12 du25 janvier 2008 sur la protection des données à caractère personnel et son décret d'application n° 2008-721 du 30 juin 2008. La législation de 2008 répondait aux problématiques de son époque liées à la naissance et au développement de la société de l'information au Sénégal. Elle prenait en compte les enjeux liés au contexte sénégalais, africain et international de la protection des données personnelles.

Une quinzaine d'années plus tard, le contexte, les enjeux et les problématiques liés, de manière générale, à la société numérique et, de manière spécifique, aux données, ont évolué. Cela est dû au développement, à la diversification et à la généralisation des technologies numériques et de leurs usages. Pour ce qui est de la donnée à caractère personnel, l'attention s'est aujourd'hui portée sur elle en tant que ressource et en tant qu'ensemble global dont fait partie intégrante la donnée personnelle.

La perception de la donnée comme ressource a donné naissance à des usages et des applications technologiques quasi-illimités. C'est l'ère de d'intelligence artificielle, d'objets intelligents et connectés, de données massives, des réseaux sociaux, de la réalité augmentée, de la personne augmentée, etc. Ces civilisations et usages nés du numérique, fondés presque exclusivement sur la donnée, renouvellent, dans une perspective plus complexe, la question de la protection des données personnelles et de la vie privée.

Comment, aujourd'hui, protéger les données personnelles dans un contexte et dans une société où la donnée est perçue comme un objet juridique, une ressource économique, un enjeu politique et stratégique et un levier de développement social et culturel ?

La présente étude, consacrée au Sénégal, part, d'abord, de l'existant. Elle examine toutes les opportunités liées à la donnée personnelle au plan politique, social, culturel et juridique, tout en recensant les risques liés à tous ces usages. L'étude procède ensuite à une analyse du contenu du cadre juridique et institutionnel actuellement en vigueur en matière de protection des données personnelles en vue d'y déceler les risques (identifiés ou non) non pris en charge.

Pour mieux asseoir le diagnostic, l'équipe de projet a mis à contribution les organisations de la société civile en vue de recueillir leurs avis et contributions.

Les insuffisances relevées sont liées, tantôt à la non-maîtrise des usages des données personnelles, tantôt à la qualité de la norme ou à la performance des institutions de mise en œuvre du cadre juridique. Enfin, l'étude s'achève sur des recommandations susceptibles d'aider à la maîtrise des enjeux, à l'amélioration du cadre juridique et à l'anticipation des défis imminents.

INTRODUCTION

A. APERÇU DU CONTEXTE

Le monde actuel est caractérisé par une digitalisation sans cesse croissante des sociétés et des activités humaines. Cela est rendu possible grâce à des technologies nouvelles telles que l'Internet des objets (IdO), la *blockchain* (ou chaîne de blocs), l'intelligence artificielle, l'impression en trois dimensions (3D), l'avènement des plateformes numériques, les données massives.

Cette intensification des usages du numérique modifie profondément les civilisations humaines. En effet, de nos jours, au plan numérique, la personne humaine représente une masse de données : données d'identification sociale, biologique ou morphologique, données économiques ou financières, etc. Rien de la personne humaine n'échappe à une représentation numérique. C'est la raison pour laquelle certains États ont, très tôt, compris la nécessité de réglementer l'usage des données personnelles[1].

Le Sénégal a amorcé la régulation juridique des données personnelles en 2008 en vue de répondre au besoin de protection induite des risques d'atteintes aux droits fondamentaux de la personne humaine. Mais au fur et à mesure que s'accélèrent les progrès technologiques, on assiste à l'émergence de nouveaux usages des données personnelles dans tous les domaines : vote électronique, télétravail, télémédecine, paiements électroniques, plateformes de services en ligne, télé-enseignement, diffusion et consommation de données personnelles sur les réseaux sociaux.

Toutes ces transformations sociales emportent de nouveaux risques en matière de données personnelles et invitent à repenser la protection des données de la personne à l'aune de la digitalisation presque intégrale des activités humaines.

B. ENJEUX ET OBJECTIFS

Les données personnelles mettent en lumière plusieurs enjeux politiques, sociaux, économiques, culturels et juridiques en raison des possibilités infinies que la donnée numérique offre comme perspective d'amélioration de la vie sociale, individuelle et collective.

La présente étude veut contribuer à une meilleure compréhension des enjeux autour des données personnelles en interrogeant, au Sénégal, la cohérence des stratégies mises en œuvre depuis les premières dynamiques nationales de traitement des données personnelles.

[1] Pour l'état des législations en matière de numérique et de données dans le monde, voir, notamment, CNUCED, Rapport 2015 sur l'économie de l'information : Libérer le potentiel du commerce électronique pour les pays en développement, aperçu général, disponible sur : https://unctad.org/fr/system/files/official-document/ier2015overview_fr.pdf (consulté le 21 août 2022) ; CNUCED, Information Economy Report 2015 : Unlocking the Potential of E-commerce for Developing Countries, disponible sur https://unctad.org/system/files/official-document/ier2015_en.pdf (consulté le 21 août 2022).

Cette étude vise ensuite, à saisir les données personnelles au cœur de la multiplicité des usages dont elles sont l'objet. Ainsi, à partir des différentes perceptions et usages, l'étude entend analyser la pertinence des normes et apprécier l'efficacité du cadre juridique et institutionnel de régulation des données personnelles. L'étude entend en outre repérer, le cas échéant, les différentes influences qui ont pu ou qui pourraient impacter les politiques nationales mises en œuvre en matière de gouvernance des données personnelles. Cette étape permettra de relever les mérites à consolider et les insuffisances auxquelles il conviendra de remédier.

Pour mieux organiser la réponse aux risques d'atteintes aux droits, la réflexion a surtout et enfin pour objectif d'évaluer l'efficacité des cadre normatif et institutionnel au regard des multiples usages qui se sont développés autour des données personnelles.

C. DEMARCHE D'INTERVENTION

L'étude a été menée sur la base d'une approche intégrée tenant compte de la dimension systémique du sujet traité. La prise en compte de cette dimension systémique permet de tenir compte de l'ensemble des acteurs intervenant dans l'écosystème des données personnelles ainsi que des relations et interactions directes, indirectes ou complémentaires en cause.

Une telle approche ne peut être réalisée dans le cadre d'une logique monodisciplinaire. Aussi, la démarche retenue est-elle transdisciplinaire afin d'associer des dimensions politique, juridique, technologique, économique, socio-anthropologique ou environnemental des données personnelles.

La démarche est, par ailleurs, à la fois inclusive et endogène afin de n'exclure aucune partie prenante de l'écosystème des données personnelles, quels que soient leur secteur d'intervention : public, privé ou sociétal. Cela a justifié que le régulateur des données personnelles et les OSC aient été associés à l'étude. En outre, la démarche prend en considération les réalités et conditions propres au Sénégal et aux ensembles régionaux et sous-régionaux auxquels il appartient sans nier l'importance de l'influence de la dimension et des acteurs internationaux, singulièrement, en matière de données personnelles.

Plusieurs outils sont utilisés dans le cadre de cette démarche afin de saisir la réalité du phénomène ainsi que les différentes perceptions des parties prenantes, notamment des questionnaires et sondages de perception.

D. RESULTATS ATTENDUS

Au terme de la présente étude, le présent rapport a été élaboré. Il met en lumière :

- les différents acteurs publics et privés, intéressés ou concernés par les données personnelles ;
- les différentes perceptions et les divers usages liés aux données personnelles ;
- le contenu des normes et la pratique des institutions quant à l'application de ces règles ;

- le cas échéant, les stratégies d'influence qui ont jalonné la mise en place, l'application ou les réformes des politiques et du cadre juridique sénégalais des données personnelles.

Le rapport contient également, sous formes de recommandations, les mesures stratégiques et opérationnelles à mettre en œuvre en vue d'assurer une protection idoine des données personnelles au Sénégal.

E. DIFFICULTES RENCONTREES

La principale difficulté rencontrée concerne l'absence de documentation sur des aspects spécifiques ou pointus relatifs aux usages numériques en général et à ceux en rapports avec les données personnelles en particulier. Tels est le cas, spécialement en matière d'utilisation des données à caractère personnel dans les processus électoraux, notamment les pratiques, les finalités, la conformité des traitements au regard de la loi.

F. PLAN DU RAPPORT

Le présent rapport se décline en cinq parties, portant, successivement, sur :

- la connaissance du phénomène (I) des données personnelles ;
- la cartographie des acteurs (II) intervenant dans l'écosystème des données personnelles ;
- la compréhension des perceptions et usages (III) autour de la donnée personnelle ;
- l'encadrement juridique et institutionnel de la donnée personnelle au Sénégal (IV) ;
- Les recommandations pour une meilleure régulation des données personnelles au Sénégal (V).

I. CONNAISSANCE DU PHÉNOMÈNE

La donnée personnelle est définie par la loi. C'est donc un concept juridique nommé[2] dont l'existence est consacrée par la loi (1). Mais au-delà du concept, la donnée personnelle renvoie également à une réalité multidimensionnelle (2) dont les contours comme la substance dépassent le cadre strictement juridique. Toute une chaîne de valeur s'est créée autour de la donnée personnelle grâce aux multiples usages auxquels elle a donné naissance dans la société numérique.

A. LA DONNEE PERSONNELLE COMME CONCEPT JURIDIQUE NOMME

Toute donnée n'est pas nécessairement une donnée personnelle. Au plan juridique, la donnée personnelle désigne 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, etc.[3] A ce titre, la donnée personnelle est d'abord un élément d'identification de la personne au plan physique, biologique, génétique, social et culturel, etc. Les données personnelles ainsi entendues étant des faisceaux d'éléments pertinents à travers lesquels l'individu peut être saisi dans toutes les dimensions de son existence, leur collecte, leur diffusion et leur traitement doivent être encadrés. Au Sénégal, cet encadrement juridique est advenu, notamment à travers la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel et son décret d'application n° 2008-721 du 30 juin 2008 (voir infra, Le contenu du cadre juridique, pp. 33 et ss.).

Toutes les données personnelles n'ont pas la même nature et ne se rapportent pas à la même dimension de l'identité de l'individu. C'est dire qu'il existe plusieurs catégories de données personnelles. En fonction de l'objet auquel elles se rapportent, on distingue les données sociologiques (sexe, race, opinions, etc.), les données physiologiques (dont les données génétiques et biométriques), les données morphologiques (aspects du corps)…

Selon l'importance des enjeux et risques qu'ils cristallisent, la loi sénégalaise opère une distinction entre les données sensibles et les données non sensibles. Sont classées données sensibles, toutes les données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou raciale, à la santé, aux mesures d'ordre so-

[2]Selon le *Vocabulaire juridique* Capitant, une catégorie, une institution, un concept juridique est dit « nommé », lorsqu'il est désigné par un nom ou sous une sous une appellation consacrée par la loi (ou au moins par l'usage), et soumis, en tant que tel, à certaines règles spéciales (G. CORNU, *Vocabulaire juridique*, 12ème édition, 2018, voir « nommé-e »). En revanche, est « innommé », la catégorie, l'institution, le concept juridique « qui n'a reçu de la loi ni dénomination spéciale ni réglementation particulière » (G. CORNU, op. cit., voir « innommé-e »).

[3] Art. 4 de la loi n° 2008-12 du 25 janvier 2008 portant protection des données à caractère personnel au Sénégal.

cial, aux poursuites, aux sanctions pénales ou administratives (pour plus de détails, voir infra, Le contenu du cadre juridique, pp. 33 et ss.).

Quels que soient son objet ou sa nature, la donnée personnelle est partie intégrante d'un ensemble plus vaste : la donnée. Celle-ci constitue désormais une matière première dont les applications possibles sont presque infinies car susceptibles d'intéresser les diverses dimensions de la vie individuelle et collective. Ces diverses applications de la donnée traduisent sa réalité politique, économique, sociale, culturelle, technologique… La donnée en général et la donnée personnelle, en particulier, est devenue une réalité multidimensionnelle qui ne peut être circonscrite dans une discipline.

B. LES DONNEES PERSONNELLES COMME REALITE MULTIDIMENSIONNELLE

La donnée est la matière et l'unité de base de la cybersociété. Il est donc normal que la donnée personnelle soit devenue le fonds de commerce des géants du numérique, autrement appelés GAFAM (Google, Amazon, Facebook, Apple et Microsoft). En effet, plusieurs usages de la donnée personnelle sont envisageables :

- elle est principalement un élément d'identification et permet de saisir l'individu à travers toutes ses composantes et dans toutes ses dimensions ;
- elle se présente comme une ressource pour tous les usages de la société de l'information (usage politique, économique, social et culturel) ;
- elle constitue un critère de définition d'un régime juridique de protection des individus ou d'encadrement des autres usages de la société de l'information.

Autour de la donnée personnelle gravite donc une série d'intérêts individuels et collectifs et des enjeux stratégiques d'ordre politique, technologique, administratif, économique, social et culturel. C'est à l'aune de ces intérêts et enjeux que doit être appréciée la pertinence de la régulation des données personnelles. Grâce à la donnée personnelle, une dynamique de transformations sociales positives a débuté au Sénégal et présente des possibilités quasi-infinies au regard des applications concrètes auxquelles elle peut donner lieu : aménagements numériques des territoires, procédures administratives électroniques, vote électronique, télétravail, télémédecine, enseignements et formations à distance, entreprises ou startup créées exclusivement pour et autour de la donnée (*cloud*, intelligence artificielle et Internet des objets, sécurité de la donnée, etc.), monnaie et paiements électroniques, etc. Toute régulation, pour être pertinente, doit permettre de saisir ces opportunités mais doit également permettre de maitriser les risques induits. A l'opposé des opportunités identifiées se trouvent en effet des risques importants d'atteintes aux personnes, à leurs droits et intérêts à travers leurs données.

II. CARTOGRAPHIE DES ACTEURS

Le champ de la donnée fait intervenir plusieurs acteurs à des échelles différentes et pour des intérêts parfois distincts, quoique complémentaires. Une interaction cohérente et efficace entre ces différents acteurs permet d'aboutir à la création d'une chaîne de valeurs de la donnée en général et de la donnée personnelle en particulier, propice à l'émergence d'un marché pertinent de la donnée.

Ainsi, en procédant à une cartographie basée sur le modèle écosystème, le marché de la donnée personnelle permet de mettre en exergue trois segments intégrés : d'une part, les acteurs de l'écosystème-support composés essentiellement des acteurs normatifs, des acteurs chargés de la mise en place du cadre technique, et le capital humain ; d'autre part, les acteurs de l'écosystème direct comprenant toutes les personnes publiques et privées participant à l'offre de données brutes ou traitées ou directement impliquées dans la chaîne de valeur de la donnée ; enfin, les parties prenantes à l'écosystème indirect ou complémentaire qui permet de mettre en relief les intervenants exploitant les données notamment à de fins de sécurité, d'Internet des objets, d'intelligence artificielle, de services à la demande, etc.

A. L'ECOSYSTEME-SUPPORT

Il est composé essentiellement :

- des acteurs normatifs : il s'agit notamment du parlement, du gouvernement, des experts juridiques, de la société civile et des organisations professionnelles ;
- des régulateurs : il s'agit de la Commissions de protection des données personnelles (CDP), de l'Autorité de régulation des télécommunications et des postes (ARTP), du Conseil national de régulation de l'audiovisuel (CNRA)/Organe de régulation de la chaîne de valeur audiovisuelle ;
- des structures et entreprises chargées du réseau et de sa sécurité : il s'agit notamment de la Direction générale du chiffre et de la sécurité des systèmes d'information (DGCSSI), Sénégal numérique SA, GAINDE 2000, SONATEL, etc. ;
- de la justice, à savoir :
    - le juge constitutionnel, pour le contentieux de la constitutionnalité des Lois sur les données à caractère personnel ;
    - le juge africain et les mécanismes africains et internationaux de protection des droits de l'homme (Cour africaine des droits de l'homme et des peuples (CAfDHP), Commission africaine des droits de l'homme et des peuples (CADHP), Comité des droits de l'homme des Nations Unies (CDH) pour ne citer que ceux-là)
    - le juge communautaire, lorsque le Sénégal intègrera l'Acte additionnel de la CEDEAO sur les données à caractère personnel ;

- le juge administratif pour le contentieux de la légalité des actes règlementaires et pour les recours contre les actes et décisions des autorités administratives indépendantes chargées de la protection des données à caractère personnel, notamment la CDP ;
- le juge civil pour les litiges contractuels ou de droit privé mettant en jeu les données personnelles ;
- le juge pénal en ce qui concerne les actes constitutifs d'infractions en matière de données personnelles ;

- des usagers des services à l'occasion desquels les données sont fournies ou collectées ;
- des responsables des traitements des données à caractère personnel ;
- des fournisseurs d'infrastructures de stockage.

B. L'ECOSYSTEME DIRECT

L'écosystème direct de la chaine de valeurs de la donnée personnelle comprend, entre autres :

- *les acteurs publics et privés chargés de la collecte de l'information administrative* (informations liées à l'état civil, à la situation administrative ou professionnel), de l'information liée à la santé, à l'éducation ou à la vie professionnelle en général, à travers les différents registres tels que les registres d'état civil, de passeports, de sécurité sociale, de gestion administrative des élèves et étudiants, les registres de la justice, de et autres auditeurs des formations initiales ou professionnelles. Au Sénégal, plusieurs plateformes ou registres peuvent être recensés :
- *les parties prenantes chargées par l'autorité publique de la collecte de données économiques et financières* : ce sont les acteurs institutionnels chargés de la collecte des données économiques et financières, opérée par voie d'autorité par l'administration publique. Font partie de cette catégorie d'acteurs, les greffes des juridictions, chargés de la tenue du RCCM, les conservateurs de la propriété foncière, la juridiction en charge du registre national des sûretés ainsi que celle tenant le fichier national du Registre du commerce et du crédit mobilier (RCCM). On peut y ajouter le registre des bénéficiaires effectifs des entreprises minières créé conformément aux principes de l'Initiative pour la transparence dans les industries extractives (ITIE).
- Ce segment comprend également les acteurs du secteur bancaire ainsi que les données collectées notamment à travers le Système de transfert automatisé et de règlement dans l'UEMOA (STAR-UEMOA), le Groupement interbancaire monétique de l'UEMOA (GIM-UEMOA), le Centre de traitement monétique interbancaire de l'UEMOA (CTMI-UMOA), la Centrale des incidents de paiement, etc. ;
- Enfin, font partie de cette chaîne, les acteurs de la police économique et financière : La Cellule nationale de traitement de l'information financière (CENTIF), le Groupe intergouvernemental d'action contre le blanchiment d'argent en Afrique de l'Ouest (GIABA), etc.

- les acteurs privés proposant des produits et services relatifs aux données et, le cas échéant, aux données personnelles : cette catégorie comprend les acteurs privés intervenant dans la collecte de données dans le cadre d'une offre de services ou de la création de valeur ajoutée autour de données collectées. Sont visés, toute entreprise de fourniture de réseaux, de services électroniques, de solutions technologiques liées au paiement électronique ou à la sécurité, tout opérateur de plateformes de services électroniques, tout établissement de crédit, tout bureau d'information sur le crédit, etc. On peut citer Orange, Free, Expresso, Sénégal Numérique SA, GAINDE 2000, SONATEL, ARC informatique, les BIC.
- *Les acteurs de la société civile appelés à collecter et/ou à traiter des données personnelles*. Les acteurs de la société civile sont parfois appelés, en raison de leurs missions, à collecter et/ou à traiter des données personnelles des personnes cibles. Ici, la chaîne de valeur n'est pas forcément à but lucratif quoique cette dimension n'est pas absolument exclue. Au Sénégal, plusieurs organisations de la société civiles sont concernées. En dehors des acteurs de l'éducation formelle et de l'enseignement supérieur et de la recherche (écoles, universités, instituts, etc.), on retrouve d'autres acteurs ayant des statuts divers, les uns ne pouvant échapper au besoin de collecte de données personnelles, les autres, intéressés par la défense des droits dans la société numérique. L'équipe de projet a eu l'opportunité de partager avec elles le pré-rapport afin de recueillir leurs avis et orientations. Il s'agit notamment, de :
  - **3D (Démocratie, Droits humains, Développement)** est une ONG qui intervient dans les domaines de la défense et la promotion des droits humains, la promotion du développement local, de la démocratie et de la bonne gouvernance. Chacun des trois principaux pôles de 3D la met en rapport avec la problématique des données personnelles, soit parce qu'elle en collecte nécessairement, soit parce qu'elle œuvre à une meilleure prise en charge des droits numériques des personnes et des communautés. Elle a été créée en 2000 et son siège est à Dakar.
  - **AfricTivistes** est la ligue africaine des cyber-activistes et blogueurs pour la démocratie qui a été créée en 2013, ayant son siège à Dakar, c'est une association de blogueurs et web-activistes du continent et de sa diaspora dont l'objectif est de promouvoir et défendre les valeurs démocratiques, les droits humains et la bonne gouvernance à travers le numérique. Elle utilise le numérique comme levier de transformation civique, sociale et politique à travers des sessions de formation, des plaidoyers, des réseaux d'influence. Elle procède à des renforcements de capacités dans le domaine de la gestion de projets numériques, de la sécurité informatique, de l'open data, des solutions médias, de la citoyenneté numérique. En outre, elle forme et informe sur le développement et la mise en œuvre de solutions informatiques de contournement des coupures d'internet, de medias audiovisuels, dans le but de renforcer la liberté d'expression et l'accès à l'information (VPN, réseau social privé, radio pirate, Cloud, serveur, etc.). A ce titre, l'association conseille et oriente vers des solutions protectrices des données personnelles.
  - **Amnesty International** est une ONG de défense des droits humains, créée en 1961 et reconnue au Sénégal depuis le 11 octobre 1980. Elle intervient dans

tous les domaines sectoriels en matière de droits humains. Plus spécifiquement, en matière de données personnelles, Amnesty International, à travers un rapport spécial de 2019[4], a alerté sur la menace systémique pour les droits humains que représente la surveillance omniprésente exercée par Facebook et Google sur des milliards de personnes.

- **Article 19** est une organisation internationale indépendante de droits humains dont la dénomination est inspirée de l'article 19 de la Déclaration universelle des droits de l'homme (qui garantit la liberté d'expression). Article 19 intervient dans la promotion et la défense de la liberté d'expression. Fondée en 1987 à Londres au Royaume-Uni, l'organisation a, depuis 2007, entrepris de s'implanter dans plusieurs régions du monde. A cet égard, la promotion du droit d'accès à l'information inclut la lutte pour les droits numériques et la protection des données personnelles.
- **Association des juristes sénégalaises (AJS)** fournit des conseils et orientations juridiques et judiciaires et aide les personnes indigentes, vulnérables à avoir accès aux services juridiques et les oriente, le cas échéant, vers les personnes et/ou institutions spécialisées. Elle informe, forme, sensibilise la population cible et œuvre aux transformations sociales, juridiques et institutionnelles jugées nécessaires. L'AJS a été créée en 1974. En raison de son objet social, elle collecte des données personnelles (parfois sensibles : cas de viol, de données de santé, données de condamnations judiciaires) et aide également à la protection de ces mêmes données.
- **Forum civil** est la section sénégalaise de Transparency International.
- **Association sénégalaise des utilisateurs des technologies de l'information et de la communication (ASUTIC)**
- **Internet sans frontières** est une association française (Loi 1901), et un réseau international d'organisations non gouvernementales dont l'objectif est de promouvoir la libre circulation des informations et des connaissances, de défendre les libertés et droits numériques et de lutter contre toutes les formes de censure sur les réseaux connectés. Internet sans frontières a été fondée Paris en 2007 par un groupe de militants de la société civile à la suite de la censure du réseau Internet par un gouvernement militaire en Asie[5]. ISF a, depuis 2019, une représentation au Sénégal. Celle-ci œuvre pour la promotion et la protection des droits numériques, de la santé numérique.
- **Jonction** est une association de droit sénégalais qui a une fonction de commissaire à la CDP. C'est en raison de son expertise dans le domaine des données qu'elle a formulé, le 11 octobre 2013, ses quinze (15) recommandations pour la révision de la Loi sur les données à caractère personnel[6]. Jonction milite pour

[4] Amnesty International : Les géants de la surveillance : le modèle économique de Facebook et Google menace les droits humains (version française résumée), 2019, disponible sur https://www.amnesty.org/en/wp-content/uploads/sites/8/2021/05/POL3014042019FRENCH.pdf (consulté le 13 février 2023).

[5] https://internetwithoutborders.org/organisation

[6] Voir les recommandations de 2013 sur http://jonction.e-monsite.com/medias/files/recommandation-2.pdf (22 février 2023). Il convient de préciser qu'en 2020, à la suite d'un atelier organisé les 27 et 28 février, Jonction a

la paix et la sécurité dans le cyberespace. À cet égard, elle produit plusieurs réflexions et a mené plusieurs activités en rapport avec cette problématique[7] : Quelles responsabilités des parties prenantes ?

- **Polaris Asso** est une association qui agit pour l'autonomisation des jeunes dans l'espace numérique, l'éducation et la sensibilisation à la protection des données personnelles. Elle œuvre à protéger les jeunes des dangers du numérique en renforçant leur capacité et intervient également pour un meilleur accès à l'éducation en mettant à profit les opportunités offertes par le numérique. Enfin, l'association milite en faveur de la paix, de la tolérance et de l'acceptation de l'autre, spécialement dans l'environnement numérique. Dans le cadre de la lutte contre le cyber-harcèlement, Polaris Asso, en collaboration avec Soft Skills Academy de l'Institut supérieur de management (ISM) de Dakar a, notamment, publié un livre blanc intitulé « ce n'est pas de ta faute[8] ».
- **Réseau africain pour l'éducation et la santé (RAES)** est une ONG qui a été créé en 2004 au Sénégal. Elle informe, forme et sensibilise sur des problématiques d'intérêt général telles que le développement, une éducation de qualité, l'égalité entre les sexes, la bonne santé et le bien-être, la durabilité des villes et des communautés, la paix, la justice et l'efficacité des institutions publiques et/ou sociales.
- **Rencontre africaine pour la défense des droits de l'homme (RADDHO)** est une ONG nationale basée à Dakar dont l'objet est la défense et la protection des droits humains. Elle a le statut consultatif spécial auprès du Conseil économique et social (ECOSOC) de l'Organisation des Nations unies (ONU) et bénéficie du statut d'observateur auprès de l'Assemblée générale de l'ONU et de l'Union africaine (UA). Dans le domaine des données personnelles, la RADDHO

---

encore proposé de nouvelles recommandations en vue de l'amélioration de l'avant-projet de loi portant révision de la Loi de 2008 sur les données à caractère personnel. Ces recommandations de 2020 peuvent être consultées sur http://jonction.e-monsite.com/medias/files/recommandations-atelier-fevrier-2020.pdf (22 février 2023).

[7] On peut, notamment, citer :

- Le séminaire international à l'intention des acteurs de la société civile d'Afrique francophone sur le thème : « droit à la vie privée et protection des données personnelles », Dakar, 10 et 11 octobre 2013, dont les recommandations sont disponibles sur http://jonction.e-monsite.com/medias/files/recommandation-2.pdf (consulté le 13 février 2023)
- L'étude de Astou Diouf (département recherche de Jonction) sur « La gouvernance des données : localisation des données, base de donnée biométrique et identité numérique », consultée sur http://jonction.e-monsite.com/medias/files/etude-cipesa-jonction-la-gouvernance-des-donnees-personnelles-1.pdf (consulté le 16 février 2023) ;
- L'atelier de partage de « l'Analyse de la mise en œuvre de la stratégie nationale de cybersécurité de 2018 à 2020 », voir le compte-rendu sur https://www.lactuacho.com/cybersecurite-lactualisation-du-cadre-juridique-un-imperatif-selon-les-acteurs/ (consulté le 13 février 2023) ;
- La déclaration conjointe (avec quatre autres OSC) intitulée « Projet de régulation des réseaux sociaux au Sénégal : Nous alertons », disponible sur http://jonction.e-monsite.com/medias/files/declaration-conjointe.pdf (consulté le 13 février 2023).

[8] Polaris Asso & Soft Skills Academy, Ce n'est pas de ta faute : notre contribution à la lutte contre le cyberharcèlement.

Bien qu'ayant obtenu la version numérique du livre blanc, transmise par le directeur exécutif de Pollaris Asso, l'équipe projet n'a pas eu accès à sa source internet. Néanmoins, il existe une podcast (émission de présentation) du livre blanc « Ce n'est pas de ta faute » sur https://www.youtube.com/watch?v=QOsW_dSGnFI (visionné le 10 février 2023).

œuvre pour une relecture des droits humains sous l'angle du numérique (éducation à la citoyenneté numérique) et, inversement, une approche du numérique sous l'angle des droits humains (humanité numérique et droits humains).

Il convient noter que toutes les sous-composantes de l'écosystème direct interagissent entre elles ou sont susceptibles d'avoir des interactions. Par exemple, les établissements de crédit fournissent des données aux opérateurs de services électroniques ou de plateformes, aux bureaux d'information sur le crédit et aux opérateurs de monnaie électronique. Inversement, les registres de commerce, d'état civil, etc., alimentent les fichiers des établissements de crédit, en raison des pièces exigées pour l'ouverture d'un compte.

La même dynamique interactive est observée avec les acteurs de l'écosystème indirect de la donnée personnelle.

C. L'ECOSYSTEME INDIRECT

L'écosystème indirect désigne, ici, tous les acteurs, produits et services qui créent de la valeur ajoutée à partir de données personnelles de base : par exemple, tous les services de vidéos à la demande, les comparateurs de prix et les notations de solutions, les divers plateformes et services numériques, recourent, en grande partie, à l'amélioration d'informations personnelles, nominatives ou non, qu'ils réutilisent pour leur propre compte ou pour le compte d'autrui. Le système de l'Internet des objets, et, plus généralement, l'intelligence artificielle, proposent des services à très haute valeur ajoutée grâce à la collecte de données personnelles brutes ou peu traitées, qu'ils valorisent en l'enrichissant.

Ecosystème des acteurs

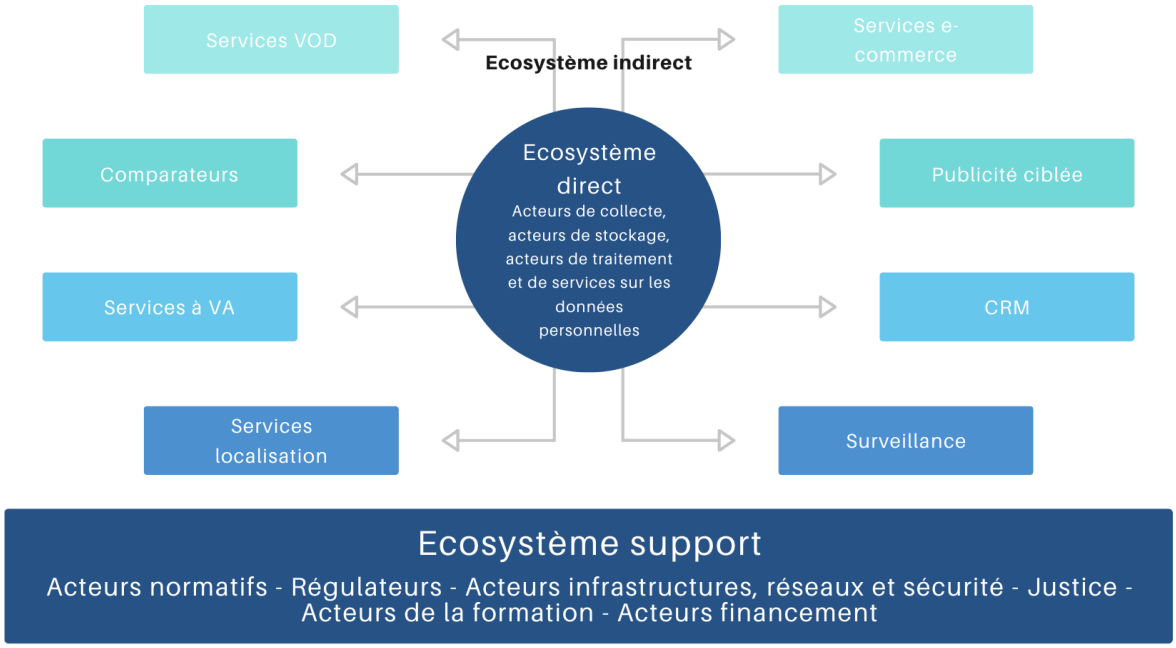

Schéma : Ecosystème des acteurs

III. COMPRÉHENSION DES PERCEPTIONS ET USAGES DES DONNÉES PERSO.

On peut comprendre les perceptions et les usages des données personnelles en commençant par analyser les aspects politique et stratégique, notamment en matière d'élections, de démocratie et de souveraineté numérique (1). L'importance économique et financière de ces données permettra, ensuite, de mettre en lumière les dynamiques de l'économie de la donnée (2). En outre, les transformations socioculturelles induites du phénomène de la monétisation de la donnée révèlent toute la dimension sociale des perceptions et usages liés à sa collecte et à son traitement (3), suggérant, enfin, le modèle de régulation juridique à partir d'une lecture du cadre juridique actuellement en vigueur au Sénégal (4).

A. DIMENSIONS POLITIQUE ET STRATEGIQUE DES DONNEES PERSONNELLES

Les dimensions politique et stratégique des données personnelles sont difficilement dissociables même si, pour mieux les apprécier, il peut être utile de les analyser séparément.

1. La dimension politique de l'usage des données personnelles

Au plan politique, deux niveaux d'analyse peuvent mettre en exergue les usages et perceptions des données personnelles. D'abord, la gestion adéquate de ces données peut aider à atteindre l'objectif de transparence dans la gouvernance publique en général et dans la conduite du processus électoral en particulier. Au chapitre de la gouvernance publique, la mise en œuvre de l'obligation de redevabilité par les acteurs politiques, critère essentiel de mesure de la démocratie, implique la fourniture d'informations aux citoyens, en particulier les informations sur la gouvernance économique, administrative, politique, environnementale, etc. et la protection effective de leurs droits fondamentaux. Par exemple, en matière de gouvernance minière, avec le concours des règles et principes de l'ITIE, et dans le but de maitriser les bénéficiaires effectifs des entreprises minières, les données collectées peuvent aider à instaurer la transparence et la redevabilité. C'est le même postulat de l'instauration d'un niveau de transparence dans la gouvernance économique qui justifie la collecte de l'information économique et financière de toutes les entreprises par le truchement du RCCM et de la CENTIF.

Ensuite, dans le cadre électoral spécifiquement, la contribution des données personnelles à l'efficience du processus est sans conteste.

Primo, les données personnelles constituent la première ressource des opérations et du processus électoraux. Le fichier électoral, les informations électorales de chaque électeur (domicile ou circonscription électorale), l'existence et le poids électoral des partis ou coalitions de partis politiques et les opérations de parrainage depuis l'introduction du parrainage citoyen, se fondent presque exclusivement sur les données à caractère personnel. A ce titre, quatre principaux champs d'utilisation possibles peuvent être recensés :

- l'utilisation des données par les organes du processus électoral en vue de concevoir le fichier des électeurs, la publication des listes des candidats et le traitement du contentieux pré ou post électoral. C'est le code électoral qui consacre ces possibilités ;
- l'utilisation des données personnelles par les candidats individuels et les partis politiques pour leurs adhérents. Car, même si la prospection politique est interdite, les partis politiques peuvent utiliser les données de leurs militants, conformément aux dispositions du code électoral ;
- l'usage, plus problématique, des données personnelles des électeurs par des personnes privées à des fins lucratives ou à des fins politiques ;
- le recours aux données personnelles par des structures publiques ou privées offrant des services de communication politique au profit des États ou des candidats, partis ou organisations politiques.

Ces données personnelles, dûment utilisées, peuvent donc accroître la transparence du processus, améliorer le choix de l'électeur, instaurer ou préserver la paix publique et politique par la prévention ou la réduction du contentieux électoral. En effet, en utilisant correctement les données de faits d'état civil ou celles du fichier électoral, on peut s'assurer de la régularité des opérations électorales et de la sincérité des résultats des joutes électorales. *A contrario*, la manipulation des données à mauvais escient peut constituer le revers de la médaille, en faussant le libre jeu démocratique et remettant en cause l'objectif de transparence électorale.

Secundo, les données personnelles sont aujourd'hui incontournables dans le secteur du marketing et de la communication politiques, dans la mesure où les partis et les organisations politiques, en misant sur la prédictibilité et la prévisibilité de leurs droits et intérêts ont, de plus en plus, recours à toutes sortes de compétences et d'outils d'ingénierie électorale : sondage, prospection politique dissimulée, *scoring* électoral, etc. Cela requiert des données personnelles, fournies à l'entreprise de communication politique par les candidats, partis ou organisations politiques, ou collectées directement auprès des électeurs par celle-ci. Là encore, le risque le plus immédiat réside dans le fait que ces outils de communication ou de prospection politique et électorale soient conçus ou utilisés par des entreprises localisées hors du Sénégal. Mieux, ces entreprises, étrangères pour la plupart, sont capables d'utiliser les données collectées à des fins autres que la seule stratégie de marketing politique. A cet égard, la CDP (Avis trimestriel n°2/2022, p. 26) a rappelé la collecte de données à des fins de marketing politique et (ou) social doit être conforme à la Délibération 2014-20/CDP du 30 mai 2014, portant sur les conditions de la prospection directe[9].

Tertio, il convient de souligner, spécialement, l'impact du parrainage électoral sur le spectre des usages et des risques liés aux données personnelles dans le champ politique et électoral. En effet, l'utilisation des données personnelles à des fins électorales a connu une profonde évolution depuis l'instauration du parrainage citoyen par la loi n° 2018-22 du 04 juillet 2018 portant révision du code électoral. La mise en œuvre de cette loi implique une collecte massive de données personnelles des citoyens, parfois même au-delà du nombre de parrainages né-

[9] Voir la délibération sur : https://www.cdp.sn/content/délibération-n°2014-20cdp-du-30-mai-2014-portant-sur-les-conditions-de-la-prospection (consulté le 20 août 2022).

cessaires à la recevabilité de la candidature parrainée (constitution de réserves de parrains). Cela débouche sur des effets pervers qui constituent autant de risques juridiques que de failles du système de gouvernance des données en matière électorale. Car, il faut préciser qu'il n'existe pas, au niveau des organes électoraux, de mécanismes concrets permettant de vérifier la légalité de la collecte de ces données des électeurs aux fins de parrainage. A titre d'illustration, au cours des dernières opérations électorales (élections législatives de 2022), un nombre important de plaintes devant la CDP a été relevé. Ces plaintes émanent de citoyens dénonçant les pratiques abusives dans la collecte de leurs données. La CDP, dans son Avis trimestriel n° 2 de 2022 avait alors jugé nécessaire de sensibiliser les différents acteurs du processus électoral sur les dangers et risques liés à l'utilisation des données personnelles des électeurs. Ainsi, « suite aux interpellations, plaintes, pétitions et signalements, il est apparu nécessaire pour la CDP, conformément à ses missions de veille, de sensibilisation et de protection, de rappeler le cadre légal de la collecte des données personnelles dans un contexte électoral [10]». L'autorité de protection rappelle « [qu'] aux termes des dispositions de la loi 2008-12, tout traitement, sous quelque forme que ce soit, doit respecter les libertés et droits fondamentaux des personnes physiques. A cet effet, la collecte des données personnelles nécessite au préalable un certain nombre de conditions à remplir par la personne chargée de la collecte[11] ».

Dans le même sillage, il convient de prêter une attention particulière aux risques des dérives liés à la surveillance de masse[12]. En effet, plusieurs nouveaux phénomènes sont devenus courants au Sénégal. Ainsi, on peut constater que :

- plusieurs artères des rues au Sénégal ainsi que des endroits stratégiques sont dotées de caméras surveillance publique alors même que l'on ignore quelles sont les technologies embarquées, les données collectées, leurs lieux de stockages et l'existence ou non d'une régulation des données ainsi collectées et/ou traitées ;
- l'utilisation des drones civils est devenue courante alors que nul ne sait si ces engins et leurs commandants respectent la vie privée des personnes et/ou leurs données personnelles. Autrement dit, on ne saurait dire s'ils sont conformes à la règlementation en vigueur, notamment l'annexe 5 au règlement aéronautique du Sénégal n° 06 et relatif aux systèmes d'aéronefs télépilotés (Chapitre IV, Paragraphe 4.1 à 4.4). En outre, dans un contexte de terrorisme, de lutte contre les trafics de tout genre, il est impératif que les aéronefs télépilotés ou drones à usage civil reçoivent une règlementation spécifique, conséquente, en tenant compte des enjeux et des risques liés à leur utilisation, notamment en matière de données personnelles ;
- les technologies médicales sont légion et rien n'indique qu'elles respectent la règlementation relative aux données personnelles : ce serait le cas de la médecine chinoise par assistance technologique qui est, de plus en plus, prisée dans les pays africains en général et au Sénégal en particulier. La difficulté réside dans l'absence d'informations sur la nature, la quantité et la destination des informations collectées sur les patients à tra-

[10] CDP, Avis Trimestriel n° 2/2022, p. 24 ; disponible sur https://www.cdp.sn/content/avis-trimestriel-n°-02-2022-de-la-commission-de-protection-des-donnees-personnelles-du-0 (consulté le 20 août 2022).

[11] Ib.

[12] L'alerte sur ce risque a été donné par plusieurs participants à l'atelier de partage avec les OSC organisé dans le cadre de la présente étude. Voir en annexe 3, les TDRs de la journée de l'atelier de partage organisée par le LASPAD le jeudi 19 janvier 2023, à l'intention des OSC.

vers ces technologies. Il est nécessaire que cette question soit prise en compte par le futur texte réformé (révision de la Loi sur les données personnelles).

Ces cas de réception et/ou de traitement de certaines plaintes de citoyens dans le cadre des processus électoraux, mentionnés, notamment, dans ces avis trimestriels de la CDP, attestent ainsi de la nécessité de mieux réguler les données utilisées à des fins électorales.

La loi sur la protection des données personnelles en 2008 qui a été renforcée en 2019 avec l'adoption de la loi n°2019-29, énonce les principes fondamentaux de la protection des données personnelles, ainsi que les droits des citoyens sénégalais en matière de protection de leurs données personnelles. Ainsi les juridictions sénégalaises ont un rôle important à jouer dans la protection effective des données personnelles des citoyens face aux menaces extérieures, aux activités malveillantes et à la prédation des données par les entreprises étrangères.

Tout d'abord, les tribunaux sénégalais sont compétents pour traiter les litiges relatifs à la protection des données personnelles. Les citoyens sénégalais peuvent porter plainte devant les tribunaux pour toute violation de leurs droits en matière de protection des données personnelles, que ce soit par des entreprises sénégalaises ou étrangères. Les tribunaux peuvent ordonner la cessation immédiate des pratiques illégales, ainsi que la réparation des préjudices subis.

De plus, la Commission de protection des données personnelles (CDP) est chargée de veiller à l'application de la loi sur la protection des données personnelles. La CDP est une autorité administrative indépendante qui a le pouvoir d'effectuer des contrôles et des enquêtes sur les traitements de données personnelles effectués par les entreprises sénégalaises ou étrangères opérant au Sénégal. Si la CDP constate une violation de la loi sur la protection des données personnelles, elle peut engager des poursuites et demander des sanctions à l'encontre des entreprises concernées.

Enfin, le Sénégal est signataire de plusieurs conventions internationales qui visent à protéger les données personnelles des citoyens, telles que la Convention du Conseil de l'Europe sur la protection des données personnelles et la Convention de l'Union africaine sur la cybersécurité et la protection des données personnelles. Ces conventions fournissent un cadre juridique international qui renforce la protection des données personnelles des citoyens sénégalais et permettent aux juridictions sénégalaises de coopérer avec d'autres juridictions étrangères pour lutter contre les activités malveillantes et la prédation des données par les entreprises étrangères.

En somme, les juridictions sénégalaises ont un rôle crucial à jouer dans la protection effective des données personnelles des citoyens sénégalais. La loi sur la protection des données personnelles et la Commission de protection des données personnelles fournissent un cadre juridique solide pour protéger les données personnelles des citoyens sénégalais, et les conventions internationales renforcent cette protection en permettant une coopération internationale pour lutter contre les menaces extérieures.

2. La dimension stratégique des données personnelles

La donnée est devenue un enjeu de convoitise et un nouveau champ d'expression de la souveraineté des État. Dans le contexte du Sénégal, seule la maîtrise de la donnée en général et de la donnée personnelle en particulier permet d'asseoir un niveau de souveraineté numérique adéquat. Or, sur ce point, force est de relever la maitrise insuffisante de l'écosystème numérique et de la donnée personnelle.

Tout d'abord, au Sénégal, il n'existe pas de texte spécifique qui définisse ce qu'est une donnée de souveraineté, même si le discours politique permet de relever des données considérées comme des données de souveraineté : données d'état-civil, données de la fonction publique, celles relatives à la justice, à la défense et à la sécurité nationales, par exemple. Cette absence d'un régime juridique de la donnée de souveraineté n'est que le corollaire de l'inexistence de Loi d'orientation sur la donnée qui aurait pu permettre, d'une part, de définir de manière claire la notion de donnée de souveraineté et, d'autre part, d'en déterminer le régime et les limites. L'enjeu d'une typologie des données est, *in fine*, d'accroitre la vigilance des différents acteurs, et particulièrement de l'État sur la dimension de souveraineté liée aux données et, conséquemment, de favoriser la mise en place d'un régime spécifique et adapté.

C'est dans ce contexte que l'État du Sénégal ouvre de nombreux chantiers de la donnée numérique dans plusieurs secteurs stratégiques ou met en place des politiques publiques sectorielles visant à avoir un certain niveau de contrôle sur des données jugées stratégiques. On peut citer l'exemple de la plateforme SIMEN du ministère de l'Éducation destinée à collecter et à traiter les données de tous les agents qui relèvent de sa compétence ainsi que des élèves. On peut également citer le projet du ministère de la Justice destiné à la mise en place d'une base de données sur l'ensemble des décisions de justice et des diverses mesures judiciaires (avec un stockage local de données).

Dans cette gouvernance par à-coups de la donnée stratégique, il est important, dans le contexte sénégalais, de noter l'existence d'initiatives provenant du secteur privé. En effet, ce dernier a régulièrement plaidé pour une prise en compte du caractère stratégique des données relatives à certains secteurs d'activités. Car, au-delà de la notion de données de souveraineté, toute faille de sécurité touchant aux données relatives à l'état civil, aux élections, à la santé, etc., peut compromettre la souveraineté de l'État et la vie des citoyens.

En somme, malgré les efforts, le cadre juridique et institutionnel sénégalais souffre d'un handicap de base : l'absence d'un cadre juridique global sur la donnée. Cela est exacerbé par l'absence de statistiques fiables sur le niveau de maitrise ou de contrôle de nos données à caractère personnel, quoique la SENUM S.A et la DGCSSI auraient pu jouer le rôle d'organes de contrôle des données et de collecte des statistiques.

Il faut rajouter à ce tableau, la faiblesse des ressources humaines capables d'assurer une protection souveraine des données produites ou collectées localement.

Sous ce rapport, la communauté scientifique, particulièrement les universités et les institutions de recherche sénégalaises, sont en retard dans la contribution attendue d'elles. L'offre d'enseignements, de programmes et de projets de recherche dédiés à la question de la donnée personnelle est particulièrement faible. En conséquence, le pays ne dispose pas de capital humain suffisant en nombre et en qualité capable de prendre en charge l'ensemble des enjeux

liés à la protection de la donnée. La production scientifique nationale sur le thème des données personnelles reste aussi relativement faible, or l'absence des données probantes des chercheurs entraîne un risque pour la cohérence des politiques publiques, car les liens existants entre les préoccupations des divers acteurs de l'écosystème du numérique ne peuvent ressortir que d'une véritable étude critique et économiquement désintéressée. Cette faible production locale de connaissances entraine par ailleurs une dépendance épistémique qui risque de nous être préjudiciable car les voix et intérêts africains seront inaudibles dans les débats internationaux sur la protection des données personnelles. Il est donc essentiel de poser les jalons d'une production de connaissances à différentes échelles (nationale, régionale, continentale), afin d'éclairer la pratique de la protection des données personnelles.

B. IMPORTANCE ECONOMIQUE ET FINANCIERE DES DONNEES PERSONNELLES

L'économie numérique est en plein essor au Sénégal et le pays vient d'adhérer au traité établissant une zone de libre-échange économique en Afrique (ZLECAF) dont l'une des ambitions est de développer le e-commerce entre les Etats africains. Elle a justifié l'adoption de la stratégie Sénégal numérique 2016-2025, avec l'ambition d'une contribution du numérique au PIB à hauteur de 10% à l'horizon 2025 et un effet d'entrainement des autres secteurs clés de l'ordre de 300 milliards de F CFA (Stratégie Sénégal numérique 2016-2025, p. 7).

Il ressort de la Lettre de politique sectorielle de développement (LPSD) du secteur numérique 2019-2023 que l'écosystème du numérique est constitué de quatre (4) opérateurs de télécommunications dont un opérateur de service universel, trois (3) Fournisseurs d'accès Internet (FAI), trois (3) Opérateurs de réseau mobile virtuel (ORMV), d'entreprises privées, principalement des Petites et moyennes entreprises (PME) et des Startups (ces derniers évoluant dans le développement d'applications, l'ingénierie et le conseil en général), des organisations professionnelles TIC et des associations de consommateurs (LPSD 2019-2023, p. 10).

Une part importante de cette économie numérique repose sur la donnée. Or, à l'instar de toute économie, l'économie de la donnée présente un double visage à travers deux schémas d'exploitation et d'optimisation économique. D'une part, le modèle de l'exploitation licite, dans le cadre d'une entreprise régulièrement constituée et dont les activités de traitement de données ont fait l'objet des procédures idoines d'habilitation auprès de l'autorité de régulation (CDP). C'est le cas, notamment, des entreprises qui proposent des applications (logiciels) et des solutions technologiques comportant, pour une bonne part, des données personnelles : solutions et applications de gestion de ressources humaines, de télétravail, de monétique ou de monnaie électronique, applications de consultation médicale à distance ou d'enseignement à distance, etc. Or, on retrouve le même modèle de marché de la donnée au Sénégal avec les entreprises telles que la SONATEL, Orange, Free, Expresso (pour les entreprises de télécommunications) ; le groupe ARC avec ses nombreux départements sectoriels (ARC As Services, ARC Solutions, ARC Télécoms, ARCCelerate, etc.) ; GAINDE 2000, notamment avec ORBUS paiement, opérant comme concentrateur de paiement en partenariat avec dix entreprises de paiement électronique ; ainsi que toutes les entreprises privées proposant des services

d'hébergement ou de stockage à travers notamment le cloud. C'est encore le cas avec les BIC ou le schéma économique de Sen'Infogreffe (voir infra) et, d'une manière générale avec toute entreprise intégrant la donnée comme ressource de base ou ressource traitée.

L'achat ou la vente de données est juridiquement admis si la structure déclare son activité à la CDP, et si la cession de fichiers de données à caractère personnel est nécessaire aux opérations sur le fonds de commerce. Il faut préciser néanmoins que, s'agissant des mégadonnées des opérateurs de télécommunication, la jurisprudence de la CDP n'est pas encore stabilisée quant à leur régime juridique.

Nonobstant l'inexistence de statistiques officielles au Sénégal, la monétisation de la donnée existe dans les faits au regard du modèle économique des entreprises susmentionnées, en particulier les BIC et Sen'Infogreffe. En effet, ces entreprises existent principalement ou exclusivement pour la vente ou l'achat de données personnelles de nature économique et financière. Par exemple, les BIC vendent des fiches de solvabilité permettant aux banques d'avoir des éléments de scoring et d'évaluation du client avant de mettre en place un prêt. A la différence du BIC dont l'objet et la mission explicite sont consacrés dans la loi (article 33 de la loi n° 2014-02 du 6 janvier 2014 portant réglementation des bureaux d'information sur le crédit dans les États membres de l'Union monétaire Ouest africaine). Sen'Infogreffe a le même objectif de manière implicite et accessoire.

Cette tendance a vocation à se généraliser, notamment sous l'effet attendu de l'adoption de la loi n° 2020-01 du 6 janvier 2020 relative à la création et à la promotion de la startup au Sénégal. Cette loi vise à promouvoir la startup au Sénégal sur la base de mesures et d'un cadre favorables à la créativité, l'innovation dans des domaines à très forte valeur ajoutée, notamment à travers l'utilisation des TIC (article 1er de la loi). A cet égard, le cadre juridique optimal consisterait à trouver un compromis entre la LDP et la Loi sur les start-up. Car, théoriquement certaines technologies ne peuvent pas fonctionner sans une certaine masse de données, les mégadonnées.

D'autre part, il convient de noter que la commercialisation de la donnée n'est pas toujours régulière. C'est le cas de tous les actes cybercriminels dont font l'objet les systèmes et réseaux d'informations, portant, du même coup, atteinte aux données à caractère personnelles.

C. Dimensions humaine et sociale des données a caractere personnel

La transformation sociale et culturelle induite par la société de l'information est bien perceptible au Sénégal, particulièrement dans le domaine de l'usage des données personnelles.

Au plan social, le numérique a favorisé l'apparition de nouveaux usages dont les figures et les dynamiques sont intimement liées, notamment, à l'universalisation et à la démocratisation de l'accès aux TIC et à l'entrée en jeu des réseaux sociaux et des plateformes d'e-commerce. Cette situation s'explique par la généralisation de la téléphonie mobile qui a atteint un taux de pénétration de 116,71 % et par l'accès à l'Internet dont le niveau de progression s'élève à 60,28 % (statistiques 2016, Stratégie Sénégal numérique, 2016-2025, p. 12). A l'échelle PME, l'effervescence des plateformes comme Expat-Dakar, Ndar Boncoin, Jumia, Dakar-

webstore, etc. traduit les mutations du modèle de consommation des sénégalais. De même, la pandémie de la Covid-19 a révélé les dynamiques d'adaptation des populations aux contraintes sanitaires, grâce à la mise à profit des opportunités offertes par les TIC : webinaires, télétravail, téléspectacles, etc.

Ces contraintes externes créées par la pandémie confortent la prédiction du document de stratégie nationale en matière numérique, notamment en ce qui concerne la promotion de l'industrie culturelle locale. En effet, profitant des effets d'entrainement résultant de la Télévision numérique terrestre (TNT), la Stratégie Sénégal numérique envisage de créer un village artisanal virtuel, de promouvoir la monétisation des contenus locaux déjà entamée par les géants mondiaux du contenu (YouTube, iTunes et Amazon).

Cependant, la création de contenus, la consommation des services et la pratique des réseaux sociaux, aussi bénéfiques qu'elles soient, présentent des risques certains. Ils sont de divers ordres et de différentes échelles de gravité. Au plan social et individuel, le premier danger est la surinformation (infopollution) et la désinformation, premiers facteurs des dérives notées aujourd'hui. En effet, on assiste à une culture de l'influence (buzz) alimentée par la collecte et l'exposition de données personnelles, tout opéré par le biais de la technologie du traçage et du profilage (cookies). Du point de vue de celui qui se dévoile, surtout sur les réseaux sociaux, le risque est souvent mal perçu car, la plupart des « victimes » n'ont pas toujours conscience du danger auquel elles s'exposent. La conséquence est souvent dramatique, surtout lorsqu'un usage malicieux est fait des données exposées, en particulier les données intimes. Il n'est donc pas rare de relever des cas de traumatisme, voire de suicide, dans le cas des scandales de *sextape* ou de révélation, à la suite de chantage, de données en rapport avec l'intimité de la vie privée. Il existe d'autres risques qui s'induisent de telles expositions de données personnelles : risques d'atteintes à l'honneur et à la réputation, risques de violences morales, risques de collecte et de divulgation illégales de données personnelles.

Du côté des auteurs de ces actes illicites, le principal risque est un risque de responsabilité (civile, pénale, administrative) pour atteinte aux données d'autrui et, dans une certaine mesure, un risque de réputation ou de répudiation (sapant l'image de marque d'une personne, d'une entreprise).

Mais l'avènement de la société de l'information n'engendre pas qu'une collecte illicite. Toutes les activités sociales étant saisies par le numérique, les acteurs sociaux sont amenés, le plus souvent, à collecter des données personnelles dans le cadre de leurs activités. Dans le cadre de la présente étude, les échanges avec les organisations de la société civile ont révélé cet état de fait. Les participants à l'atelier de partage conviennent, à l'unanimité, que l'être humain est devenu un faisceau de données numériques avec des conséquences sur le paradigme même de la personnalité juridique telle que traditionnellement conçue. Ils s'interrogent sur les modalités d'une protection des droits de la personne et des droits humains dans cette nouvelle ère des civilisations numériques. Cela suppose une redéfinition de la personnalité juridique en tenant compte de la personnalité et des identités numériques, une relecture du système de protection des droits humains en général et des droits catégoriels en particulier. Ainsi, les acteurs comme Amnesty International, l'AJS, Polaris Asso, etc. précisent que leurs offices les amènent à collecter et à utiliser des données personnelles, voire des données sensibles (données de per-

sonnes réfugiées ou détenues, données d'adolescents ou de jeunes…). La législation actuelle devrait, selon eux, régir notamment, la citoyenneté numérique et l'humanité numérique.

Au plan culturel, le grand risque réside dans la dictature de la pensée culturelle unique, par l'uniformisation et l'universalisation d'un modèle culturel ; ce qui constitue une menace sur la diversité culturelle. En effet, les civilisations numériques épousent les contours du caractère planétaire de la société de l'information et leurs dynamiques sont fonction de la capacité de chaque espace culturel à exister (création de contenus culturels locaux par différenciation) et à s'exporter dans la cybersociété (valeur ajoutée spécifique propice à l'exportation). Sans ces préalables, le risque encouru au Sénégal et en Afrique est une sorte de « cybercolonisation culturelle », susceptible d'aboutir à une acculturation ou à une extraversion culturelle.

Tout ceci impose de repenser le modèle de régulation juridique de la donnée et du marché de la donnée personnelle.

D. MODELE DE REGULATION JURIDIQUE DES DONNEES A CARACTERE PERSONNEL

La donnée personnelle imprègne toutes les dimensions de la vie humaine et est devenue en enjeu stratégique important pour toute communauté sociale, ce qui implique un encadrement juridique adéquat. La donnée personnelle est saisie au plan juridique à un double niveau normatif et institutionnel.

Au plan normatif, la régulation de la donnée personnelle est assurée, en grande partie par l'État du Sénégal, dans une certaine mesure, par les organisations internationales, régionales et sous-régionales. Cela n'obère nullement le modèle conventionnel de la régulation normative.

Du côté de l'État, la première responsabilité des acteurs publics et politiques est de mettre en place un cadre juridique adéquat et d'en assurer l'application. Ce double niveau d'intervention a été assuré avec plus ou moins de succès au Sénégal, en dépit des efforts qui restent à être consentis. En ce qui concerne l'édiction des normes publiques, le Sénégal a été avant-gardiste. Car, dès 2008, une loi et un décret d'application ont été adoptés. Il s'agit de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel et son décret d'application n° 2008-721 du 30 juin 2008 (voir infra, Le contenu du cadre juridique, pp. 33 et ss). Ces deux textes sont le siège de la création et de l'organisation de l'autorité spéciale dédiée à la protection des données à caractère personnel au Sénégal : la Commission des données personnelles (CDP- voir infra, Le contenu du cadre juridique, pp. 34-35).

A côté de ces deux textes, il convient également de citer, principalement :

- la loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal ;
- la loi n° 2008-41 du 20 août 2008 sur la cryptologie ;
- la Délibération n° 2014-001/CDP du 31 janvier 2014 portant règlement intérieur de la Commission de protection des données personnelles (CDP), telle que modifiée par la délibération n° 2016-00230/CDP du 26 août 2016.

En vue d'assurer l'observation des dispositions légales et règlementaires par les administrations, collectivités et établissements publics, le gouvernement a pris des mesures à travers, d'une part, la circulaire primatoriale n° 004/PM/CAB/Info du 12 février 2015 invitant les entités publiques à se conformer à leurs obligations de déclaration auprès de la CDP et, d'autre part, la circulaire primatoriale n° 2557/PM/CAB/Info du 27 juin 2014 portant désignation des points focaux des ministères au sein de la CDP. L'enjeu de ces mesures d'exécution de la loi réside essentiellement dans la promotion d'une conformité des traitements opérés par l'administration publique dans un contexte de digitalisation des procédures administratives, de la communication administrative et de l'aménagement numérique du territoire. Car, même si certains démembrements de l'État ne respectent toujours pas le cadre juridique sur les données personnelles, il ne saurait raisonnablement y avoir un véritable développement de l'e-administration sans ce préalable du respect de la règlementation sur les données à caractère personnel (NB : pour les développements sur l'e-administration publique, voir infra, le point relatif aux changements des cadres juridiques de l'administration publique, p. 47).

Au plan supranational, le Sénégal est partie à des organisations, mécanismes et instruments qui ont mis en place des normes relatives aux données personnelles. Ce sont, notamment :

- la Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel dite Convention de Malabo de 2014 ;
- l'Acte additionnel A/SA.1/01/10 du 16 février 2010, relatif à la protection des données à caractère personnel dans l'espace CEDEAO ;
- la Directive C/DIR/1/08111 du 19 août 2011 portant sur la lutte contre la cybercriminalité dans l'espace de la CEDEAO.
    - Acte additionnel A/SA 1/01/07 du 19 janvier 2007 relatif à l'harmonisation des politiques et du cadre règlementaire du secteur des technologies de l'information et de la communication (TIC)
    - Règlement n°15/2002/CM/UEMOA du 23 mai 2002 relatif aux systèmes de paiement dans les états membres de l'Union Economique et Monétaire Ouest Africaine (UEOMA)
    - Acte additionnel A/SA.2/01/10 du 16 février 2010 sur les transactions électroniques

Mais la régulation normative ne se résume pas à celle effectuée par voie législative ou règlementaire. Dans la pratique, entre les responsables de traitement et le titulaire des données, la gestion des données personnelles est davantage contractuelle. En outre, une personne privée peut détenir des données personnelles en vertu d'obligations contractuelles et assumer la charge d'en assurer la conservation, la sécurité et la confidentialité.

Les outils contractuels de gestion des données varieront alors sensiblement selon qu'on est dans la première ou la seconde hypothèse. En effet, le premier cas recouvre la situation en vigueur dans l'écosystème direct ou indirect de la donnée personnelle. Le modèle illustratif est celui des GAFAM avec leurs « politiques de confidentialité », sortes de contrats d'adhésion dont la souscription est le préalable à l'accès au service proposé. Dans le second cas, il s'agit de toute relation contractuelle portant sur des éléments autres que des données personnelles, mais impliquant une obligation de confidentialité assumée par les parties. Toutefois, les GAFAM étant

difficilement contrôlables par les États africains pris individuellement, la meilleure stratégie de gestion de la question serait qu'elle soit prise en charge par l'Union africaine à travers une vision collective et un cadre juridique à l'échelle du continent.

En tout état de cause, l'efficacité du cadre normatif de la régulation est fortement tributaire de la performance des institutions de mise en œuvre. Or, au Sénégal, le cadre institutionnel de régulation est composé de plusieurs acteurs publics et privés dont la collaboration ressortit peu d'une stratégie d'ensemble. Ces acteurs, publics ou privés, n'évoluent pas sous la bannière d'un cadre spécifique de coordination. Certes, il existe des organes exécutifs (Ministère en charge du numérique), techniques (ARTP, CDP, ADIE) et consultatifs (Conseil national du numérique) en matière de politiques du numérique œuvrant tous avec une relative cohérence dans leurs diverses interventions ; toutefois, il n'en existe pas spécifiquement pour les données personnelles. Cela donne une certaine idée du cadre juridique et institutionnel relatif aux données personnelles (pour plus de détails, voir point IV-B-1 ci-après, pp. 26 et ss.).

IV. ENCADREMENT JURIDIQUE ET INSTITUTIONNEL DES DONNÉS PERSO.

Pour avoir un aperçu global du cadre juridique et institutionnel des données personnelles au Sénégal, il convient d'examiner, d'abord, l'ensemble des politiques et stratégies pertinentes en la matière (A), ensuite, le cadre institutionnel de régulation (B) avant d'analyser, enfin, les règles juridiques applicables aux données personnelles et à leur traitement (C).

A. POLITIQUES ET STRATEGIES DE PROTECTION DES DONNEES PERSONNELLES

Le Sénégal a, très tôt, mesuré les enjeux du numérique. Avec la libéralisation du secteur des télécommunications et la démocratisation progressive de l'accès à l'Internet, le Sénégal a multiplié les initiatives de modernisation des règles juridiques de gouvernance du secteur, notamment l'environnement, les contenus et les usages du numérique. Toutefois, la stratégie a évolué en trois temps : d'abord, la « bataille » pour l'infrastructure ; ensuite, le temps de la régulation juridique ; et aujourd'hui enfin, la promotion de l'économie de la donnée. A chacune de ces étapes, la stratégie nationale présente une figure bien différente.

1. Le temps de l'infrastructure numérique

Au Sénégal, les premiers efforts dans l'instauration d'une société de l'information se sont orientés vers la mise en place de l'infrastructure. Cette dynamique a véritablement été impulsée sous le magistère du président Abdoulaye Wade qui, dès 2002, avait multiplié les plaidoyers pour l'équilibre numérique du monde et avait ardemment conduit la lutte contre la fracture numérique. Remarquant que « *le numérique est en train de créer un homme nouveau dans une civilisation nouvelle, la société de l'information, dans laquelle n'entre pas qui veut comme dans les premiers temps de l'humanité* [et que], *cette fois, il faut payer pour utiliser les équipements coûteux et complexes, ou rester isolé*[13] », il a appelé à la solidarité numérique, se faisant le porte-parole des pays les moins avancés, à la tribune des Nations unies.

En vue de l'opérationnalisation de sa volonté de doter le Sénégal d'une infrastructure numérique adaptée, et en réponse aux conclusions du sommet de Genève de décembre 2003 consacré à la société de l'information, le chef de l'État signa le décret 2001-476 du 18 juin 2001 portant création de la Direction informatique de l'État (DIE). Cela a constitué un tournant décisif de l'e-administration et de la gestion de la sécurité informatique de l'État. Cette dynamique sera renforcée avec le décret n° 2003-298 du 9 mai 2003 portant création, organisation et fonctionnement du projet « Intranet Gouvernemental », puis remplacé par le Décret n° 2004-1038 du 23 Juillet 2004 portant création et fixant les règles d'organisation et de fonctionnement de l'Agence de l'informatique de l'État (ADIE). Plus tard, intervient l'arrêté présidentiel

[13] Discours du président Abdoulaye Wade à la réunion de l'Assemblée générale des Nations unies sur les technologies de l'information et de la communication au service du développement (New-York, 17-1 juin 2002), disponible sur http://www.osiris.sn/Intervention-de-SEM-Abdoulaye-Wade.html (consulté le 11 juin 2022).

n° 4360 en date du 11 juillet 2006 portant création de la Cellule SENECLIC. Aux termes de l'article 2 de ce décret, « *la Cellule SENECLIC a pour mission, dans le cadre de la politique de réduction de la fracture numérique, d'équiper les écoles élémentaires de salles multimédias* ». Ces différents textes mettaient le focus sur la sécurité des infrastructures et des réseaux et le cas échéant, la formation des agents, la gestion des difficultés d'exploitation ou de mise en service. Ils traduisaient également l'option faite par le Sénégal d'investir dans la transformation sociale en prenant comme cible prioritaire, la petite enfance.

Il en résulte donc que, durant cette phase de désenclavement numérique, le focus n'était pas porté sur la protection des données personnelles. Cette dimension était même, pourrait-on dire, occultée. Cependant, grâce à l'investissement en faveur de l'infrastructure, le numérique est devenu une réalité dans tous les domaines, dès la moitié de la première décade du troisième millénaire. Qu'il s'agisse de l'administration électronique, du multimédia, de la dématérialisation des services, les usages nés de la pénétration du numérique dans le quotidien des administrations et des citoyens ont commencé, peu à peu, à transformer le quotidien des administrations, des entreprises et des citoyens. C'est alors que l'État du Sénégal a enclenché les travaux devant conduire à la phase 2 de la société de l'information avec l'adoption d'un cadre juridique relatif aux transactions électroniques, à la promotion de la sécurité technique des réseaux et données numériques et à la lutte contre la cybercriminalité.

2. L'étape de la mise en place du cadre juridique

C'est la phase 2 de la stratégie de développement du numérique et de protection des données personnelles. Elle succède à l'étape de la mise en place de l'infrastructure et vise l'instauration d'une véritable économie numérique à travers le développement d'une infostructure. Cette phase a débuté à la fin des années 2005. Sa justification a résidé dans la nécessité de prévenir les écarts liés aux usages et activités du numérique, d'encadrer l'utilisation du numérique et les activités qui s'y déroulent et le cas échéant, de sanctionner les comportements inappropriés, le tout grâce à un cadre juridique de confiance.

La phase de la régulation juridique de l'économie numérique visait ainsi à accélérer la dynamique de la société de l'information, en prévenant les risques d'exposition des données, spécialement les données à caractère personnel. Au-delà donc de la promotion de l'économie et de la sécurité numérique en général, l'autre problématique spécifique à laquelle l'État du Sénégal a apporté une réponse juridique est la protection des données des usagers du numérique, à travers la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel et son décret d'application n° 2008-721 du 30 juin 2008.

Avant-dernière des cinq lois de 2008 relatives à la société de l'information, la Loi sur les données à caractère personnel constitue donc, ensemble avec la Loi sur la cryptologie[14], le socle normatif support de l'écosystème numérique. Cette loi affichait clairement l'objectif de combler un vide qui a persisté puisqu'à cette époque, « *malgré le démarrage de l'Intranet gouvernemental, le développement du recours à l'informatique dans l'administration, dans les entreprises privées et son utilisation par les personnes, la numérisation du fichier électoral et de la carte*

[14] Voir infra, développements sur l'institution d'un cadre juridique de la cryptologie, pp. 50-51.

d'identité nationale, entraînant ainsi la génération, la collecte et le traitement des données à caractère personnel, le droit positif sénégalais ne fixe pas le cadre et le régime juridique de ces opérations[15] ».

Quoiqu'en 2005 l'économie de l'infostructure était à ses balbutiements, et malgré l'absence d'une stratégie sectorielle spécifique en matière de données personnelles, le gouvernement du Sénégal s'était engagé à « *encourager activement la formation et la sensibilisation sur les problèmes de la confidentialité en ligne, de la protection de la vie privée et plus généralement, de celle des données personnelles des consommateurs*[16] » ; toute chose ayant abouti à l'adoption de la loi n° 2008-12.

Mais quinze années après l'adoption de cette loi, l'économie numérique a beaucoup évolué. Aujourd'hui, la digitalisation croissante des activités humaines, la diversification et la modernisation des applications concrètes de l'intelligence artificielle ont mis la donnée numérique en général et la donnée personnelle en particulier au cœur de l'économie : c'est l'ère de l'économie de la donnée et du marché des données massives, impliquant une vigilance accrue dans la protection des personnes.

3. L'ère de la promotion de l'économie de la donnée

La phase de la promotion de l'économie de la donnée peut être située à partir de 2016, date d'adoption de la Stratégie Sénégal numérique 2016-2025.

Cette stratégie, quoique visant à développer le numérique de manière générale, prend en considération le développement de l'Internet des Objets (IdO) et la communication de machine à machine (M2M) capable d'engendrer une transformation des services offerts aux usagers afin de contribuer à la réalisation des Objectifs de développement durable (ODD). Elle tient également compte de la « *forte capacité de collecte de données en masse [qui] va impliquer des besoins en stockage, traitement et exploitation des méga-données générées, d'où l'intérêt de développer également [un] savoir-faire dans le domaine du Big Data*[17] ».

C'est en raison de la surabondance des données personnelles en circulation et de celles collectées massivement ou dans un ordre de grandeur normal, qu'il est devenu urgent de repenser la protection des données personnelles. Ainsi, tout en proposant la mise en jour de la législation sur la société de l'information, la stratégie met un focus particulier sur la cybersécurité. Ainsi, le gouvernement insiste sur le fait que « *la sécurité numérique doit être portée au rang des priorités de l'action gouvernementale, avec la création d'une agence nationale de cybersécurité destinée à compléter le dispositif constitué de la commission chargée de la protection des données à caractère personnel (CDP), de la Commission Nationale de Cryptologie (CNC) et des structures opérationnelles de défense et de sécurité existantes*[18] ».

---

[15] Exposé des motifs de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel.

[16] Macky Sall (Premier ministre du Sénégal), Discours d'ouverture au Séminaire « *Informatique et libertés, quel cadre juridique pour le Sénégal ?* », Dakar, 29-30 aout 2005, p. 17, disponible sur http://www.adie.sn, (consulté le 15 août 2008).

[17] Stratégie Sénégal numérique 2016-2025, p. 22, n° 84.

[18] Stratégie Sénégal numérique 2016-2025, op. cit., p. 28, n° 109.

C'est sans doute cette dynamique qui a conduit au processus actuel de révision de la Loi sur les données à caractère personnel, dont les travaux, bien qu'avancés, sont toujours en cours. Le projet de loi innove dès son article 1er en déclinant la vision qui a présidé à la réforme envisagée : « *mettre en place un dispositif permettant de réguler les usages du numérique contre les atteintes susceptibles d'être engendrées par le traitement des données à caractère personnel* ». Il ambitionne de renforcer la gouvernance et la régulation des données, plus spécifiquement les données à caractère personnel dont la protection sera confiée à l'Autorité de protection des données à caractère personnel (APDP), dotée de pouvoirs plus étendus et disposant d'un droit d'auto-saisine.

B. GOUVERNANCE ET REGULATION DES DONNEES PERSONNELLES

La gouvernance institutionnelle des données personnelles est le fait de plusieurs organes publics et privés. Elle relève tantôt d'institutions politiques, tantôt de structures techniques ou consultatives. Le synopsis de ces différentes institutions (1) révèle une interaction peu structurée (2).

1. La présentation du cadre institutionnel de la gouvernance des données personnelles

Les organes politiques se composent essentiellement de la primature, du ministère en charge du numérique, du ministère en charge de l'économie et des finances. Ils ont une compétence générale de régulation du numérique.

La Primature était[19], par exemple, l'organe désigné pour assurer la tutelle de la stratégie de gouvernance du numérique en général, conformément au Plan Sénégal numérique. Aux termes de l'article 1er du décret n° 2018-1961 portant création, attributions et modalités d'organisation et de fonctionnement du Conseil national du numérique (CNN) qui est présidé par le Premier ministre.

Le ministère en charge du numérique assure deux rôles institutionnels en rapport avec les données personnelles. D'abord, conformément à sa mission générale et en cohérence avec la Lettre de politique sectorielle 2023, le ministère a pour mission, notamment :

- de mettre en œuvre les politiques visant à réduire la fracture numérique ;
- de promouvoir la production des contenus numériques à travers l'amélioration de la diffusion des contenus cinématographiques, audiovisuels, musicaux ainsi que la sécurisation de la diffusion de l'écrit, et la mise en place d'un statut d'hébergement de données ;
- de promouvoir le développement des logiciels ;
- de diversifier les usages et les services numériques tels que l'e-commerce, l'e-administration, l'e-santé, l'e-éducation, etc. ;
- d'accélérer la compétitivité et la croissance des entreprises par le numérique ;

[19] Le poste de Premier ministre est supprimé par la Loi constitutionnelle 2019-10 du 4 mai 2019, puis rétabli en décembre 2021 (Loi constitutionnelle n° 38/2021 du 10 décembre 2021 portant révision de la Constitution).

- de dynamiser la recherche et le développement dans les Technologies de l'information et de la communication (TIC), en favorisant l'adaptation de l'organisation de l'État aux enjeux numériques et en établissant une gouvernance transversale des systèmes d'information de l'État et de s'assurer du respect des résolutions et recommandations internationales sur la gouvernance de l'Internet ;
- de favoriser le développement de l'informatique auprès des jeunes et plus généralement dans les secteurs autres que l'État ;
- d'élaborer et mettre en œuvre une politique nationale de cybersécurité.

En vertu de toutes ces missions, le ministère est membre du CNN.

Ensuite, le ministère en charge du numérique assure la coordination de la stratégie nationale de cybersécurité et participe à l'élaboration et à l'exécution d'une politique nationale de cybersécurité. A cet égard, il assure la présidence du comité de suivi et d'évaluation mis en place à cet effet.

Le ministère en charge de l'économique et des finances intervient dans le cadre de l'économie numérique et de la donnée en participant à la mise en œuvre de la stratégie Sénégal numérique 2025 en tant que partie prenante du CNN.

La particularité des organes politiques de gouvernance réside essentiellement en deux points : d'une part, ils assurent une régulation générale du numérique (ce qui minore l'attention portée à la protection spécifique des données personnelles) et, d'autre part, ils assurent globalement une régulation non technique.

Les structures publiques techniques sont essentiellement composées de la CDP, de l'Agence de l'ADIE (désormais remplacée par Sénégal numérique S.A.) et de la DGCSSI.

La CDP est l'organe technique spécialisé destiné à assurer la conformité des traitements des données à caractère personnel et, le cas échéant, à prendre toute mesure liée aux opérations de collecte, de stockage, de traitement et de transfert de ces données (voir point IV-C-2-a°, pp. 33 et SS).

L'ADIE, récemment disparu du cadre institutionnel, était régie par le décret n° 2004-1038 du 23 Juillet 2004 portant création et fixant les règles d'organisation et de fonctionnement de l'ADIE. Elle avait une mission générale de définition de la stratégie de l'administration électronique. D'une manière spécifique, elle assure des missions opérationnelles d'assistance et d'expertise, d'administration des réseaux et services informatiques de l'État, de sécurisation de l'ensemble des réseaux de l'administration, notamment en ce qui concerne l'accès aux infrastructures, et aux informations, ainsi qu'à l'intégrité et à la conservation des données (article 3-1-b°du décret). En outre, l'ADIE assure la coordination des politiques sectorielles en cohérence avec les différentes administrations publiques, la promotion des TIC et d'une culture de l'administration électronique et des usages, contenus numériques. Enfin, elle a une fonction de veille technologique et de normalisation des méthodes de conception et de réalisation des projets ainsi que les procédures régissant le fonctionnement des systèmes.

Aujourd'hui, l'ADIE est, depuis le 13 décembre 2021, remplacée par Sénégal numérique S.A., société anonyme au capital entièrement détenu par l'État. Reprenant à son compte les prérogatives de l'ADIE, Sénégal numérique S.A. est devrait s'atteler au développement d'une offre

de services numériques innovants, à valeur ajoutée, adaptés aux besoins des administrations et de l'usager. Cette ambition aboutira, à court et à moyen termes, à la mise en place d'un écosystème dense et organisée de l'économie de la donnée.

Depuis un certain temps, Sénégal numérique entame, notamment, un vaste programme de digitalisation des usages administratifs (messagerie administrative) et de la carrière du personnel de l'État à travers le Fichier unifié des données du personnel de l'État (FUDPE). Dans la perspective de la mise en œuvre du FUDPE, Sénégal numérique S.A. envisage le déploiement de plateformes au niveau décentralisé en y intégrant les inspections d'académie (IA) et inspections de l'enseignement et de la formation (IEF) du ministère de l'Éducation nationale, la numérisation des archives de la Direction de la solde du ministère de l'Économie, des Finances et du Plan ; la mise en place d'un système de gestion des imputations budgétaires pour les agents de l'État et leurs ayants droit (https://www.adie.sn/projets/fudpe). La mise en place de ces programmes aura nécessairement un impact sur les données des agents concernés. Lors d'une rencontre tenue le 18 février 2021 autour du programme Smart Sénégal de l'ADIE, la présidente de la CDP et le directeur de l'ADIE ont convenu de veiller à la mise en conformité dudit projet avant son déploiement effectif. Ces rencontres témoignent d'une corégulation des données personnelles par ces deux structures techniques, quoique toutes deux participant d'un modèle d'hétérorégulation (externe), à la différence des structures privées qui expérimentent l'autorégulation.

Quant à la DGCSSI, troisième élément des acteurs publics chargés de la régulation technique, elle remplace le Service technique central des chiffres et de la sécurité des systèmes d'information (STCC-SSI) qui était régi par l'Arrêté n° 02435/PR/SG du 06 février 2014 précisant les attributions et portant organisation du Service technique central des chiffres et de la sécurité des systèmes d'information. La DGCSSI est créée et organisée par le décret 2021-35 du 14 janvier 2021 portant création, et fixant les règles d'organisation et de fonctionnement de la Direction générale du chiffre et de la sécurité des systèmes d'information. Celle-ci est chargée de la mise en œuvre de la politique de sécurisation et de défense des systèmes d'information, définie par le président de la République, en vue de promouvoir au Sénégal un environnement numérique de confiance, sécurisé et résilient.

La DGCSSI est l'autorité nationale de la cybersécurité au Sénégal (article 2 du décret). A ce titre, elle veille, à travers la Direction des systèmes d'information sécurisée, à la protection par le chiffre ou par tout système d'information sécurisé de valeur reconnue, des informations intérieures et extérieures des autorités nationales (article 4 du décret). Dans la même mouvance, la DGCSSI assure, grâce à son centre national opérationnel de cybersécurité, la mise en œuvre de services de veille, de détection, d'alerte, d'analyse et de gestion des risques et des menaces, ainsi que les réactions aux attaques des systèmes d'information du public et du privé. A travers le même centre, elle assure la coordination nationale de la réaction aux évènements, et notamment de la lutte contre la cybercriminalité (article 7 du décret).

Il convient d'ajouter à ces structures techniques, les organes consultatifs tels que le CNN ou l'Observatoire de la qualité des services financiers (OQSF). Le premier est un organe consultatif placé sous l'autorité du premier Ministre ayant pour mission, principalement, la mise en œuvre des choix et orientations des politiques, programmes et projets nationaux dans le do-

maine des communications électroniques et de l'économie numérique (article 2 du décret). L'opérationnalisation du CNN est effective grâce à l'Arrêté primatorial n° 2019-001821 du 30 janvier 2019 portant nomination des membres du Conseil national du numérique.

Quant à l'OQSF, il est institué par le décret n° 2009-95 en date du 2 octobre 2009. Il est placé sous l'autorité du ministre en charge de l'économie et des finances et a pour objet, notamment, de suivre et d'évaluer la qualité des services offerts par les organismes financiers et de fournir au public toute information pertinente à cet effet. Pour la réalisation de sa mission, il collecte les informations nécessaires par le biais d'études, d'enquêtes, de consultations, etc. Il est habilité à traiter ces informations en vue de l'élaboration d'indicateurs pertinents et de l'analyse de l'ensemble des données collectées (article 4 du décret). Ces structures consultatives, comprenant des acteurs institutionnels, des représentants du monde professionnel et des acteurs de la société civile, permettent d'aboutir à une corégulation du marché de la donnée, en intégrant à la démarché publique de régulation une approche propre aux acteurs privés.

Les structures privées renvoient à toutes les personnes privées qui traitent des données personnelles ou à celles qui interviennent sur les politiques de régulation de ces données.

Même si toute personne privée est susceptible de collecter et de traiter des données personnelles, l'analyse se focalisera sur celles qui œuvrent dans les données massives. Elles sont nombreuses. On peut citer les établissements de crédit, les structures de développement de plateformes numériques ou de solutions de sécurité numérique comme GAINDE 2000[20]. Le système de gouvernance ou de régulation des données dont relève ces structures est mixte. D'une manière générale, elles sont soumises à la loi. En outre, elles organisent la gestion de ces données sur la base d'un modèle contractuel. Ainsi, à travers des « politiques de confidentialités » ou *privacy policy*, les acteurs privés gèrent avec leurs relations contractuelles, clients ou partenaires, la collecte et le traitement des données personnelles. Par exemple, le document de politique de confidentialité de GAINDE 2000 énonce que « *Sauf opposition de votre part, vous pourrez recevoir, par courrier postal, SMS, ou par téléphone, des offres de la part de GAINDE 2000 ou de ses partenaires commerciaux, ainsi que des courriers électroniques pour des services analogues proposés. Avec votre accord exprès, GAINDE 2000 pourra vous communiquer par courrier électronique des informations commerciales pour des services non analogues à ceux déjà fournis ou, transmettre à des partenaires commerciaux votre adresse électronique à des fins de prospection directe* ». D'une certaine manière, l'autonomie de la volonté des parties isole la relation contractuelle des pesanteurs légales, sauf clauses abusives ou nulles. Le système légal est alors complété ou suppléé par une approche conventionnelle de gestion des intérêts des parties en présence. Ce modèle de régulation est à la fois distinct de celui des autorités publiques, mais l'est également du mécanisme mis en place par les acteurs de la société civile de promotion du numérique comme l'Observatoire sur les systèmes d'information, les réseaux et les inforoutes au Sénégal (OSIRIS).

OSIRIS a été créé en mars 1998 par un groupe de personnes du monde académique et scientifiques, des agents de l'administration publique centrale et des acteurs du secteur privé, et du

[20] GAINDE 2000 est une entreprise de conception de plateformes numériques de procédures administratives ou privées et plus généralement de la dématérialisation. Elle s'active également dans la sécurité digitale et le paiement électronique. Elle a été créée en 2002.

monde associatif. Il a le statut d'association à but non lucratif reconnue par le ministère de l'Intérieur du Sénégal, sous le récépissé n° 09845 en date du 22 mars 1999. Il devait contribuer, au Sénégal, à la mise en œuvre du Réseau consultatif sur les stratégies d'information en Afrique (Advisory Network for African Information Strategies - ANAIS) dont la vocation était de faciliter l'appropriation des technologies de l'information et de la communication (TIC) par les Africains. OSIRIS sensibilise, informe et produit des analyses sur tous les sujets relatifs à l'utilisation et à l'appropriation des technologies de l'information et de la communication et, d'une manière générale, au développement de la société de l'information au Sénégal et en Afrique. A ce titre, OSIRIS est, par exemple, membre de la Commission nationale de la connectivité (CNC), (article 10 du décret n° 2011-1707 du 07 octobre 2011, portant création et organisation de la Commission nationale de la connectivité).

En définitive, la cadre institutionnel de gouvernance des TIC et des données personnelles est hétérogène, mais surtout, est quelquefois cloisonné, les différents acteurs ayant peu de rapports structurels. Cela pose la problématique de la cohérence de la stratégie de régulation.

2. La cohérence du cadre institutionnel de gouvernance des données personnelles

Au Sénégal, le cadre institutionnel de l'élaboration des politiques et stratégie est très éclaté et, dans une certaine mesure, les différents cadres organiques de mise en œuvre de ces politiques sont également cloisonnés, qu'il s'agisse des rapports entre les organes publics ou entre les structures privées, ou encore entre ces deux catégories.

En ce qui concerne la cohérence de la régulation publique, il convient de rappeler que tous les ministères sont intéressés et concernés par l'économie numérique : le ministère de la Justice, le ministère de la Santé, le ministère en charge des finances, le ministère de l'Économie, le ministère en charge du renouveau du service public, ainsi que les organes opérationnels tels que le parquet, la Police nationale, la Gendarmerie nationale, la DGCSSI ; l'ARTP, le CNRA, etc. En soi, cette diversité des structures ne constitue pas un obstacle à la mise en place d'une stratégie cohérente. Il aurait suffi que des cadres de coordination aient été institués afin d'impulser une même dynamique à toutes les différentes interventions.

Ces interactions existent certes. Par exemple, la présence, au sein de la CDP, d'un commissaire du Gouvernement permet d'atteindre un double objectif : d'abord, informer l'État de l'exécution de ses missions par la CDP ; ensuite, défendre l'État sur les dossiers qui le concerne, même si le commissaire du Gouvernement participe aux sessions sans voix délibérative. En outre, les circulaires primatoriales et l'instruction présidentielle précédemment mentionnées permettent de conformer les différentes politiques sectorielles aux exigences de protection des données personnelles puisque ces circulaires invitent les départements ministériels et les démembrements de l'État à se conformer à la LDP (en déclarant leurs traitements), et désignent un point focal des institutions publiques pour faire office d'interlocuteur avec la CDP. Cela traduit une certaine recherche de cohérence et de coordination de l'action gouvernementale dans le domaine de la protection des données personnelles.

Toutefois, les entretiens menés auprès de la CDP révèlent l'absence de centre de coordination entre la CDP et toutes les autres structures satellites qui interviennent directement ou indirectement sur les données personnelles. Un premier exemple peut être tiré des rapports entre la

CDP et les autres organes techniques : ARTP, CNRA, Sénégal numérique SA, parquet, police judiciaire. Ainsi, même s'il existe entre ces structures des rencontres ponctuelles autour de problématiques d'intérêt commun, il n'existe pas de canevas formels entre ces institutions. Pour preuve, la CDP a plusieurs fois tenu des rencontres avec les institutions spécialisées, notamment l'ARTP (pour les services à valeur-ajoutée), le CNRA (pour régulation des données dans le cadre du secteur audiovisuel), la BCEAO (pour la régulation des données dans le cadre du secteur bancaire et financier) ou encore l'ONQSF (pour la régulation des données dans le cadre des services financiers), etc.

L'absence de centre unique de coordination stratégique des différentes interventions sectorielles ne favorise pas la lisibilité d'ensemble des programmes sectoriels et des différentes actions opérationnelles.

Pourtant, la CDP n'ayant pas d'organe de tutelle (sauf une certaine tutelle financière assurée par le Secrétariat général de la Présidence de la République), le ministère en charge du numérique aurait valablement pu servir d'organe catalyseur et de courroie de transmission entre les différents organes et structures techniques que sont, principalement :

- les autorités de poursuites et de sanction (chaîne pénale : police, gendarmerie, parquet), en étroite collaboration avec le ministère de la Justice et le ministère de l'Intérieur, les organes de tutelle ;
- la Direction générale du chiffre et de la sécurité des systèmes d'information (DGCSSI) ;
- l'Autorité de régulation des télécommunications et des postes (ARTP) ;
- le CNRA, par l'entremise du ministère en charge de la culture ;
- les directions techniques de la BCEAO ;
- etc.

Le même ministère en charge du numérique peut également faire office d'épicentre des relations interinstitutionnelles entre les différents départements ministériels en matière de protection des données personnelles. Pourtant, cette fonction de coordination a déjà été mise en œuvre, de facto, à plusieurs reprises, notamment lors des travaux sur l'identité numérique nationale, lors des discussions sur la gouvernance des données et lors des débats autour de la stratégie sénégalaise sur l'intelligence artificielle. Il est donc possible de l'adopter et de l'étendre aux questions relatives à la protection des données à caractère personnel.

C. ENCADREMENT JURIDIQUE DES DONNEES PERSONNELLES

Au Sénégal, l'encadrement juridique des données personnelles a beaucoup évolué (1). A l'analyse, le cadre juridique prend désormais en charge plusieurs aspects de la protection des données (2).

Dans l'ensemble, le processus d'élaboration du cadre juridique a été endogène (3), même si cela a pu faire intervenir des partenaires extérieurs (4).

Un bilan global nous permet aujourd'hui de mesurer l'efficience de la mise en œuvre du cadre juridique, d'en relever les mérites à consolider et les insuffisances à résorber (5).

1. L'évolution du droit positif des données personnelles au Sénégal

L'évolution du cadre juridique actuel de la protection des données personnelles au Sénégal peut être saisie à travers une date repère : l'année 2008, date à laquelle furent adoptés la Loi sur les données personnelles, son décret d'application ainsi que les autres textes majeurs de la société de l'information au Sénégal.

Depuis 2008 donc, la problématique de la protection des données personnelles a été amplement prise en charge par le Sénégal, malgré les améliorations souhaitables.

a. La période antérieure à 2008

La période d'avant 2008 était marquée par une absence de dispositions nationales spécifiques sur la protection des données personnelles. Cela contrastait avec l'actualité et l'acuité de la problématique. En effet, dès 1980, l'Organisation de coopération et de développement économiques (OCDE) et, plus tard en 1990, l'ONU, avaient indiqué les enjeux et les voies de la protection des données personnelles avec leurs principes directeurs.

A la suite des règles de la *soft law,* dits principes directeurs de l'OCDE, le Conseil de l'Europe adopta en 1981, la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Au Sénégal, les faits ont précédé la régulation juridique des données personnelles. En effet, le traitement des données personnelles a débuté bien avant l'adoption, en 2008, de la Loi sur les données à caractère personnel. Ainsi, dès 2005, le Sénégal instituait la carte nationale d'identité numérisée à travers la loi n° 2005-28 du 6 septembre 2005. Or, le processus de numérisation de la carte nationale d'identité, qui fait inéluctablement intervenir un traitement des données biométrique et d'état civil, aurait dû être précédé d'une prise en charge de la protection des données des citoyens ainsi collectées et traitées. Car, le décret d'application n° 2005-78721 intégrait indiscutablement des données personnelles dans la carte nationale d'identité biométrique. Aux termes de ce décret (article premier), la carte comporte, au verso, deux photographies identiques (mais de grandeur et d'emplacement différents sur la carte) les prénoms, nom, nom du mari le cas échéant, date de naissance, lieu de naissance, sexe, adresse, taille, signature, numéro d'identification national, lequel numéro peut être suivi d'un indice de différenciation. Le verso de la carte contient, en outre, les prénoms et nom du père et de la mère.

L'article 2 du décret prescrit un relevé des empreintes digitales tandis que l'article 3, alinéa 1, exige la signature du titulaire ou, le cas échéant, la mention « ne sait pas signer ».

L'entrée en vigueur de la Loi sur la carte d'identité numérisée ou biométrique[22] a ainsi permis la mise en œuvre d'un vaste programme de collecte et de traitements de données personnelles

[21] Il s'agit du décret n° 2005-787 du 6 septembre 2005 portant fixation du modèle de la carte nationale d'identité numérisée, des libellés de son contenu, des conditions de sa délivrance et de son renouvellement.

[22] Ce n'est qu'en 2016 que certaines failles de la loi n° 2005-787 du 6 septembre 2005 ont été corrigées à travers la loi n° 2016-09 du 14 mars 2016 instituant une carte d'identité biométrique CEDEAO et son décret d'application n° 2016-1536 du 29 septembre 2016.

dont certaines sont sensibles (adresse, statut matrimonial, etc.), sans qu'un régime de protection spécifique ait été défini. Cette absence de protection, ensemble avec les risques qui s'en évincent, n'étaient pas cohérents avec la Constitution qui protège les droits et libertés fondamentaux universellement reconnus.

Le même constat est observable à propos de l'intranet gouvernemental, dont le programme a débuté en 2003 à travers le décret n° 2003-298 du 9 mai 2003 portant création, organisation et fonctionnement du projet Intranet gouvernemental. Ce projet avait pour objectif la modernisation des systèmes d'information de l'administration.

L'adoption, en 2008, des textes exclusivement destinés à la protection des données personnelles venait donc en réponse à un besoin social urgent.

b. La période allant de 2008 à 2022 :

Le cadre juridique spécifique à la protection des données personnes, mis en place à partir de 2008 comprend, d'une part, la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel, son décret d'application n° 2008-721 du 30 juin 2008 et d'autre part, les dispositions pénales spécifiques issues des règles relatives à la cybercriminalité et à la cryptologie.

D'autres chantiers de réformes normatives ayant des incidences sur les données personnelles ont également été achevés. Il s'agit, notamment :

- de la loi n° 2014-02 du 6 janvier 2014 portant réglementation des bureaux d'information sur le crédit dans les États membres de l'Union monétaire ouest africaine (UMOA) ;
- de la loi n° 2018-28 du 12 décembre 2018 portant code des communications électroniques ;
- de la loi n° 2017-27 du 13 juillet 2017 portant code de la presse ;
- de la loi n° 2016-29 du 08 novembre 2016 modifiant la Loi n° 65-60 du 21 juillet 1965 portant Code pénal ;
- des Déclarations de Durban (Afrique du Sud) des 6-7 Septembre 201223 et de Yamoussoukro (Côte d'Ivoire) du 13 février 2015[24] sur les faits d'état civil, qui servent notamment de référence aux programmes de numérisation de l'état civil au Sénégal.

Aujourd'hui, un processus de révision du cadre juridique spécifique des données personnelles est en cours. Il s'agit donc d'une dynamique sectorielle qui concerne les seules données personnelles, mise en œuvre sous l'égide de la CDP.

NB : pour des développements détaillés, voir le point suivant sur le contenu du cadre juridique.

[23] Déclaration de la deuxième Conférence des ministres africains chargés de l'enregistrement des faits d'état civil, Durban, Afrique du Sud des 6-7 Septembre 2012.

[24] Déclaration de la troisième Conférence des ministres africains en charge des faits d'état civil du 13 février 2015, Yamoussoukro, République de Côte d'Ivoire.

2. Le contenu du cadre juridique

Il faut partir du cadre juridique spécial de protection des données personnelles (a), sans occulter les autres textes intéressant les données personnelles (b).

a. Le cadre juridique spécifique aux données personnelles

Il s'agit de la Loi sur les données à caractère personnel et de son décret d'application.

i. La loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel

La loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel a été l'aboutissement d'un long processus de conception, de benchmarking et de consultations techniques destiné à définir le périmètre optimal de celle-ci. Ainsi, dès 2005, sous l'égide de l'ADIE, un séminaire national[25] a regroupé des experts et plusieurs partenaires aux fins de penser la réforme du cadre juridique sénégalais de la société de l'information en général et, plus spécialement dans le domaine de la protection des données personnelles.

La loi définit son objet et son champ d'application. Ainsi, elle s'applique à :

- toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, par l'État, par les collectivités publiques, par toute personne morale de droit public ou de droit privé ;
- tout traitement automatisé ou non de données contenues ou appelées à figurer dans un fichier ;
- tout traitement mis en œuvre par un responsable (tel que défini à l'article 4.14) sur le territoire sénégalais ou en tout lieu où la loi sénégalaise s'applique ;
- 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 ;
- tout traitement des données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'État, même liées à un intérêt économique ou financier important de l'État, sous réserve des dérogations qu'elle définit et des dispositions spécifiques en la matière fixées par d'autres Lois.

Sont exclus du champ d'application de la Loi sur les données à caractère personnel :

- 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 la seule fin de permettre à d'autres destinataires du service le meilleur accès possible aux informations transmises.

[25] ADIE, ministère de la Justice du Sénégal, Coopération française, Rapport général du séminaire « Informatique et libertés, quel cadre juridique pour le Sénégal ? », Dakar, 29 et 30 août 2005.

Le chapitre 2 de la Loi institue la Commission des données personnelles, détermine son statut et fixe son organisation. 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 à la loi. Sa mission est d'informer les personnes concernées et les responsables de traitement de leurs droits et obligations et de s'assurer que les TIC ne comportent pas de menace au regard des libertés publiques et de la vie privée, en accomplissant les missions spécifiques prévues par l'article 16.

La CDP comprend 11 membres choisis en fonction de leurs compétences techniques et/ou juridiques avérées. Le mandat de chaque membre est de quatre ans renouvelable une fois. Leur indépendance est garantie à travers leur inamovibilité. Les fonctions de membre ne cessent qu'en cas de démission ou d'empêchement constaté par la CDP. Avant d'entrer en fonction, chaque membre prête serment devant la cour d'appel de Dakar en formation solennelle et jure « *de bien et fidèlement remplir [sa] fonction de membre de la Commission de Protection des Données à Caractère Personnel, en toute indépendance et impartialité de façon digne et loyale et de garder le secret des délibérations* ». Tout membre est tenu au secret professionnel.

Le chapitre 3 de la Loi a trait aux conditions de traitement des données. En ce sens, le législateur consacre, *de prime abord*, les principes de base en matière de traitement de données. Ce sont :

- Les **principes de légitimité,** de **finalité** et de **proportionnalité** : ces principes posent l'exigence d'un consentement de la personne dont les données sont collectées, sauf lorsque la collecte est requise par la loi, justifiée par la sauvegarde des droits et libertés fondamentaux de l'intéressé ou effectuée dans un cadre contractuel auquel l'intéressé est partie.
  La finalité de la collecte, explicitement déclinée, doit être respectée (article 35 alinéa 1) et la collecte minimisée ou proportionnée à cette finalité (article 35, alinéa 2). La conservation des données doit répondre à ces deux exigences de finalité et de proportionnalité. Lorsqu'il s'agit d'un prestataire de services de certification électronique, il ne peut procéder à la collecte de données personnelles que directement auprès de la personne concernée, et exclusivement pour les besoins de la délivrance et de la conservation des certificats (article 73) ;
- Le **principe de loyauté** et de **transparence** : la loyauté proscrit les manœuvres frauduleuses dans la collecte, tandis que la transparence requiert l'information préalable de la personne concernée quant à la mesure de collecte ainsi que la nature des données collectées ;
- Les **principes de sécurité** et d'**exactitude** des données : le principe de sécurité signifie que les données « doivent être traitées de manière confidentielle et être protégées […] notamment lorsque le traitement comporte des transmissions de données dans un réseau » (article 38). Les obligations spécifiques à la sécurité, incombant au responsable de la collecte ou du traitement, ou à son sous-traitant, ont donc été précisées (article 39).
  Dans le sillage de cette exigence de sécurité, on comprend aisément que les données doivent être exactes au jour de la collecte, mises à jour en cas de changement et ef-

facées lorsqu'elles ne correspondent plus à la réalité ou ne répondent plus aux finalités pour lesquelles elles avaient été collectées (article 36).

Le législateur régule ensuite le traitement des données sensibles en déterminant les conditions de collecte et de traitement des données dans le cadre de certaines professions, et précise les conditions de transfert de données du/vers le Sénégal. De manière concrète, la Loi proscrit :

- la collecte et le 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 ;
- le traitement des données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté ne peut être mis en œuvre que par l'autorité judiciaire, l'autorité administrative agissant conformément à ses attributions légales ou par les auxiliaires de justice pour les besoins de l'exercice de leurs missions ;
- la collecte et le traitement des données personnelles en vue d'une prospection directe, sauf consentement préalable et exprès de la personne concernée (article 47) ;
- l'usage exclusif d'un traitement de données personnelles pour l'analyse ou la prédiction de la personnalité ou du comportement, en vue de l'application d'une décision de justice ou de toute décision produisant des effets juridiques à l'égard de la personne concernée (article 48) ;
- le transfert illégal de données personnelles vers un pays tiers est interdit par l'article 49, sauf :
  - la garantie d'une protection légale au moins égale à celle prescrite par la loi sénégalaise dans cet État tiers, ou d'une protection technique suffisante de la part du responsable de traitement dans ce pays tiers ;
  - et à la condition d'en informer préalablement la CDP et d'en obtenir l'autorisation. La même exigence est appliquée quant au traitement, au Sénégal, de données personnelles provenant de l'étranger.

  L'illégalité du transfert à l'étranger n'est pas encourue lorsque ce transfert est ponctuel, non massif et lorsque la personne à laquelle se rapportent les données a consenti expressément à ce transfert ou si le transfert remplit les conditions énoncées à l'article 50 ou, enfin, lorsque le responsable du traitement situé à l'étranger justifie, dûment, sa capacité technique suffisante à protéger les données objet du transfert (article 51).

La Loi détermine les données de santé susceptibles de faire l'objet de traitement tout en fixant les conditions de la collecte (articles 42 et 43) et pose les exigences à respecter pour le traitement de données personnelles à des fins scientifiques, artistiques, littéraires ou de journalisme (articles 44 et 45), sous réserves, pour la presse, que la collecte et le traitement soient nécessaires à l'exercice du droit de réponse.

Enfin, **le chapitre 3 encadre l'interconnexion de fichiers** contenant des données à caractère personnel, en soumettant à l'autorisation préalable de la CDP :

- l'interconnexion de fichiers de données personnelles effectuée par des personnes morales chargées d'une mission de service public ;

- l'interconnexion de fichiers de données personnelles mise en œuvre par l'État dans le cadre de l'administration électronique ;
- l'interconnexion de fichiers de données personnelles réalisée par les personnes privées et dont les finalités principales sont différentes.

Le chapitre 4 porte sur les droits de la personne dont les données à caractère personnel font l'objet d'un traitement. A ce propos, quatre droits sont reconnus à la personne concernée par une collecte ou un traitement de données. Il s'agit :

- du **droit à l'information** (articles 58 à 61) : ce droit postule que la personne dont les données sont collectées doit être informée par le responsable du traitement, au plus tard au jour de la collecte. Celui-ci doit décliner son identité ou celle de son représentant et préciser la nature des données collectées, la finalité de la collecte, l'obligation ou non pour la personne concernée de répondre aux questions posées en vue de la collecte, son droit, à l'avenir, de demander à ne plus voir figurer ses données dans la base de données collectées. Le responsable du traitement lui notifie également les destinataires identifiés ou potentiels des données collectées ainsi que la durée de leur conservation, la probabilité ou non qu'elles fassent l'objet d'un transfert à l'étranger et le droit d'accès à ses données dont elle dispose.
  Lorsque les données sont collectées auprès d'une personne tierce, la personne concernée doit être informée par le responsable du traitement au plus tard à la date d'enregistrement des données.
  Lorsque le stockage et le traitement sont le fait d'un opérateur de communication électronique, il informe de manière claire et complète la personne concernée de la finalité de la collecte et des moyens dont elle dispose pour s'y opposer, à moins que le stockage et le traitement ne soient exclusivement destinés à fournir ou faciliter la communication électronique ou à l'exécution d'un ordre ou de demande de service de communication électronique émanant de la personne dont les données sont collectées ;
- du **droit d'accès** (articles 62 à 67) : il vise d'abord, à permettre à toute personne de saisir par écrit tout responsable de traitement de données à caractère personnel à l'effet de savoir si ses données sont collectées ou stockées, et le cas échéant, de connaître la nature de ces données et les voies par lesquelles elles ont été obtenues.
  Lorsque les données sont effectivement collectées ou stockées, le droit d'accès autorise, ensuite, la personne concernée à obtenir du responsable du traitement, sous une forme accessible, la communication de ses données.
  Si la personne concernée doute de la concordance entre les données à lui communiquées et celles effectivement traitées par le responsable du traitement, ou si elle soupçonne une dissimulation ou une perte de ses données, il peut en saisir la CDP.
  Le responsable du traitement est tenu de transmettre à toute personne qui le demande, une copie de ses données personnelles, sauf si la demande est manifestement abusive. Pour un patient, le droit d'accès est exercé par lui-même ou par son représentant.
  Lorsqu'un traitement intéresse la sûreté de l'État, la défense ou la sécurité publique, le droit d'accès est exercé conformément à l'article 67.

Le droit d'accès permet, enfin, à la personne concernée d'être informée de l'éventualité d'un transfert de ses données à l'étranger ;

- **du droit d'opposition** (article 68) : sauf lorsque le traitement et la communication de données répondent à une obligation légale, le droit d'opposition permet à toute personne concernée : (i) de refuser tout traitement de ses données ; (ii) d'être informée avant toute première communication de ses données à des tiers et, le cas échéant, de s'y opposer gratuitement ;
- du **droit de rectification et de suppression** (article 69) : c'est le droit « [d'] 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 ».

Le chapitre 5 édicte les obligations du responsable du traitement des données. Il s'agit de :

- **l'obligation de confidentialité** (article 70) : elle engage le responsable du traitement à disposer d'un personnel intègre et qualifié au plan technique et juridique. Tout contrat de sous-traitance doit contenir les mêmes exigences à l'égard du sous-traitant ;
- **l'obligation de sécurité** (article 71) : elle met à la charge du responsable du traitement une obligation de précaution en vue d'empêcher que les données soient déformées, endommagées, ou que des tiers non autorisés y aient accès ;
- l'**obligation de non-conservation indue ou illégitime** (article 72) : cette obligation vise à empêcher que les données collectées ou traitées soient conservées au-delà du temps nécessaire à l'atteinte de la finalité de la collecte, à moins que la conservation au-delà de ce délai ne soit dictée par des raisons statistiques, historiques ou scientifiques ;
- l'**obligation de pérennité** (article 74) : elle vise à garantir la non-altération des données collectées et/ou traitées tout au long du temps de conservation et de traitement.

Le chapitre 6 édicte les dispositions pénales par renvoi au code pénal et à la Loi sur la cybercriminalité.

Le **dernier chapitre** porte dispositions transitoires et finales. Les dispositions transitoires ont pour objet de résoudre trois séries de difficultés :

- d'abord, les traitement de données personnelles initiés pour le compte de l'État, d'un établissement public, d'une collectivité locale ou d'une personne morale de droit privé gérant un service public, avant l'adoption de la Loi. A cela, l'article 76 a soumis ces traitements, à titre transitoire, à une obligation de déclaration, conformément à l'article 18. Toutefois, l'article 77-1°) ajoute que, deux ans à compter de l'entrée en vigueur de la Loi, ces situations devraient être régularisées conformément aux dispositions qui s'imposent ;
- ensuite, les traitements opérés par les personnes privées n'agissant pas dans le cadre de l'article 76. A ce propos, l'article 77-2°) énonce que celles-ci disposent

d'un délai d'un an, à compter de l'entrée en vigueur de la Loi, pour respecter ses dispositions ;

- enfin, l'applicabilité de la Loi au programme de numérisation de la carte d'identité nationale. Sur ce point, l'article 78 prévoit que des dispositions règlementaires dérogatoires seront prises pour la mise en œuvre de la loi n° 2005-28 du 6 septembre 2005 instituant la carte nationale d'identité numérisée.

La Loi sur les données personnelles est complétée par le décret 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.

ii. Le décret 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

Le décret organise la Commission des données personnelles : le chapitre 2 du décret, précise l'organisation, la composition et les compétences de la CDP à travers les articles 2 à 19.

Du point de vue de sa composition, la CDP est gérée par un président, un vice-président et des collaborateurs ou experts. Le décret précise d'abord, qu'au titre de la représentation du gouvernement telle que prescrite par l'article 6 alinéa 3 de la Loi, un commissaire du gouvernement siège auprès de la CDP. Celui-ci est désigné pour un mandat de deux ans renouvelable une fois et, en cas d'empêchement, il est remplacé par son suppléant.

Le décret précise les modalités et la procédure de désignation des membres et détermine les conditions de recours aux experts techniques.

Lorsque les opérations de contrôle nécessitent l'accès à des données médicales individuelles, la CDP désigne un médecin inscrit sur une liste fournie chaque année par l'ordre des médecins du Sénégal pour requérir la communication de ces données.

Quant au fonctionnement de la CDP, le décret n° 2008-721 définit les missions du président, traite de l'installation des membres de la CDP et du choix du vice-président, lequel doit être désigné au cours de la première réunion plénière de la CDP. Il appartient au président de la CDP de faire prêter serment aux membres. Il peut déléguer ses compétences au vice-président et à ses collaborateurs.

Les attributions de la CDP sont précisées aux articles 10 à 19 du décret. L'article 10 rappelle les missions stratégiques, de veille et de prospection tandis que les articles 11 à 19 organisent les conditions, modalités d'exécution des tâches opérationnelles. Celles-ci concernent :

- la tenue du répertoire des traitements de données à caractère personnel, dont les modalités d'accès ou de mises à disposition du public sont fixées par l'article 11 ;
- les personnes chargées de procéder aux contrôles, à savoir les membres de la CDP et les agents de service assermentés ;
- les modalités concrètes de tout contrôle qui, qu'il soit sur place ou sur convocation, doit résulter d'une décision de la CDP ;
- les conditions procédurales du contrôle : la décision de contrôler une structure doit indiquer le responsable du traitement concerné, le rapporteur et les autres contrôleurs chargés de l'opération ainsi que la durée de celle-ci. Le procureur de la République

territorialement compétent en est préalablement informé au plus tard vingt-quatre (24) heures avant la date ;

- les conflits d'intérêts : nul ne peut être chargé d'effectuer un contrôle sur une structure au sein de laquelle il y avait eu un intérêt quelconque au cours des cinq années précédant ledit contrôle ;
- les formalités et les formes de constatation du contrôle : l'issu du contrôle est sanctionné par un procès-verbal auquel est annexé l'inventaire des pièces et documents entrant dans le périmètre du contrôle. Le procès-verbal indique, le cas échéant, si la personne contrôlée a opposé un secret professionnel, et mentionne le texte sur le fondement duquel ce secret professionnel a été invoqué ;
- les pouvoirs de réquisition de la CDP.

Le décret règle les différents régimes juridiques applicables au traitement des données à caractère personnel (chapitre 3) : c'est l'objet des articles 20 à 31 du décret. Le décret organise et précise le régime du traitement autour du principe de finalité dégagé à l'article 35, alinéa 1, de la loi. Sur la base ce principe de finalité, l'autorité règlementaire distingue deux régimes de traitement des données à caractère personnel : le régime de la déclaration et celui de l'autorisation.

Le régime de la déclaration concerne, d'abord, les traitements de données à caractère personnel mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels, ensuite ceux mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux, des horaires de travail et de la restauration, et enfin, les traitements effectués dans le cadre de l'utilisation de services de téléphonie fixe et mobile sur les lieux de travail (article 23 du décret). Toutefois, l'article 22 précise que la dispense éventuellement obtenue par le responsable du traitement sur le fondement de l'article 17 de la Loi ne l'exonère pas du respect des obligations légales édictées en vue de garantir les droits des personnes concernées. En tout état de cause, la déclaration doit correspondre à la réalité du traitement envisagé (article 20) et ce traitement ne peut débuter qu'à compter de la réception du récépissé délivré par la CDP (article 24).

Quant au régime de l'autorisation dont les détails sont fixés par l'article 25 du décret, la demande doit, outre les conditions indiquées à l'article 20 de la Loi, comporter, en annexe, l'acte réglementaire autorisant le traitement envisagé[26].

[26] **NB** : Il convient de souligner l'ambiguité de l'article l'article 25 du décret. Cet article consacré au régime de l'autorisation semble indiquer que toute demande d'autorisation de traitement doit comporter nécessairement en annexe l'acte réglementaire autorisant le traitement envisagé. Or, l'autorisation règlementaire du traitement ne concerne que les traitements 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. Les traitements opérés par les personnes privées ne sont donc pas concernés par la production d'un acte règlementaire. Mieux, pour ces traitements envisagés pour le compte de l'État, des personnes publiques ou des personnes morales de droit privé chargées d'une mission de service public, l'acte règlementaire d'autorisation du traitement ne peut être pris qu'après avis motivé de la CDP. Dès lors, faut-il comprendre qu'il faille d'abord requérir l'avis de la CDP pour la prise de l'acte règlementaire d'autorisation administrative du traitement, ensuite, une fois l'avis favorable de la CDP obtenu, prendre l'acte administratif en question et, enfin, introduire la demande d'autorisation de la CDP (laquelle demande comportera en annexe l'acte administratif pré-cité) ?

En vue de l'efficacité de l'exercice des missions de la CDP, et quels que soient la nature et le régime de traitement, les articles 26 à 30 du décret prévoient des procédures que celle-ci peut mettre en œuvre. Ces dispositions prévoient notamment :

- les formulaires à créer (pour les demandes d'avis, de déclarations, de modifications du dossier de déclaration, d'homologation de chartes d'utilisation ou d'autorisation) ;
- les modalités et les formes de saisine de la CDP : les différentes demandes adressées à la CDP sont effectuées soit par lettre recommandée, soit par voie électronique, mais avec accusé de réception qui peut être adressé par la même voie (article 28) ;
- le point de départ du délai accordé à la CDP pour l'instruction des demandes de déclaration ou d'autorisation : le délai de deux mois, fixé à l'article 23 de la Loi pour que la CDP notifie sa réponse, court à compter de la date de l'avis de réception, de la signature de la décharge ou de l'accusé de réception électronique ;
- le délai de notification à la CDP, par le responsable du traitement, des changements intervenus : le responsable du traitement dispose d'un délai d'un mois pour informer la CDP des suppressions de données et d'un délai de quinze jours ouvrables pour l'informer de toute modifications affectant les informations traitées.

Le décret précise les obligations légales relatives aux conditions de traitement des données à caractère personnel en rappelant, tout d'abord, le principe du consentement obligatoire de la personne dont les données sont traitées.

Tout d'abord, le décret indique, plus en détail, les conditions de traitement des données génétiques et ainsi que ceux effectués dans le cadre de la recherche médical. Ainsi, le dossier des demandes d'avis ou d'autorisation de traitement de données à caractère personnel portant sur les données génétiques et sur la recherche dans le domaine médical comprend : (i) l'identité et l'adresse du responsable du traitement et de la personne responsable de la recherche, leurs titres, expériences et fonctions, les catégories de personnes qui seront appelées à mettre en œuvre le traitement ainsi que celles qui auront accès aux données collectées ; (ii) le protocole de recherche ou ses éléments utiles ; (iii) le cas échéant, les avis rendus antérieurement par des instances scientifiques ou éthiques ; (iv) les caractéristiques du traitement envisagé ; (v) le cas échéant, la justification scientifique et technique de toute demande de dérogation à l'obligation d'anonymisation ainsi que la justification de toute demande de dérogation à l'interdiction de conservation desdites données au-delà de la durée nécessaire à la recherche.

Le consentement de la personne est exigé quels que soient le moment, la circonstance et les modalités de collecte des données. Les personnes accueillies dans les établissements ou les centres où s'exercent des activités de prévention, de diagnostic et de soins donnant lieu à la transmission de données à caractère personnel en vue d'un traitement aux fins de recherche médicale, sont informées conformément à l'article 58 de la Loi (article 36, alinéa 1 du décret), sauf si, sur appréciation souveraine du médecin, le malade est laissé dans l'ignorance d'un diagnostic ou d'un pronostic (article 36, alinéa 2 du décret), encore que toute dérogation à l'obligation d'information doit être portée à la connaissance de la CDP (article 36, alinéa 3 du décret). Cette exigence est opportune en raison de l'avènement de la loi n° 2015-22 du 08 décembre 2015 relative au don, prélèvement et à la transplantation d'organes et aux greffes de tissus humains. En effet, les dispositions de l'article 18 de cette Loi, instituant un re-

gistre spécial, ne semblent pas tenir compte des obligations énoncées par les textes relatifs au traitement des données à caractère personnel[27].

Ensuite, le décret précise que des données à caractère personnel initialement collectées pour des finalités déterminées, explicites et légitimes, ne peuvent être communiquées à un tiers en vue d'un traitement ultérieur à des fins historiques, statistiques ou scientifiques qu'à la condition d'être, préalablement à leur communication, rendues anonymes ou codées. En outre, le résultat du traitement à des fins historiques, statistiques ou scientifiques ne doit pas permettre l'identification de la personne concernée, sauf : (i) si celle-ci a consenti à ce que les données ne soient pas codées ou rendues anonymes ou (ii) si la publication des données à caractère personnel non anonymes et non codées est limitée à des données manifestement rendues publiques par la personne concernée.

En outre, les dispositions de l'article 41 clarifient les suites du refus de transmission de données, de rectification ou de suppression de données, opposé sur le fondement de la sûreté de l'État, la défense ou la sécurité publiques. Ainsi, si le responsable du traitement effectué dans l'intérêt de la sûreté de l'État, la défense ou la sécurité publiques refuse de communiquer à un demandeur ses données, ou lui refuse son droit à la suppression ou à la rectification de ses données, la CDP en informe l'intéressé et mentionne ce refus dans son rapport annuel ;

Par ailleurs, **les modalités de traitement des données à caractère personnel susceptibles d'être transférées vers un pays tiers sont précisées** aux articles 42 à 44 : tout premier transfert des données vers un pays tiers doit préalablement être déclaré à la CDP. Les transferts entre entreprises d'un même groupe peuvent faire l'objet d'une déclaration commune.

La CDP établit une liste des pays ayant une législation assurant un niveau de sécurité analogue à celle du Sénégal en matière de protection de données personnelles et la met à la disposition de toute personne souhaitant transférer des données à l'étranger. La mise à disposition d'une telle liste ne dispense pas le responsable du traitement du respect de la règlementation applicable au transfert de données.

Enfin, **le décret reprend et précise les droits conférés à la personne dont les données font l'objet d'un traitement**. Les droits consacrés par la Loi au profit de personne dont les données sont traitées ont été repris et précisés par ces dispositions du décret.

b. Les autres normes juridiques ayant des liens avec les données personnelles

La protection des données personnelles présente également un enjeu dans plusieurs autres domaines. Ce sont, entre autres, les cadres juridiques des données économiques et financières, de

[27] Article 18 de la loi n° 2015-22 du 08 décembre 2015 relative au don, prélèvement et à la transplantation d'organes et aux greffes de tissus humains : « *Tout établissement public de santé agréé effectuant, en vertu des dispositions de la présente loi, des prélèvements ou transplantations d'organes ou des greffes de tissus humains, doit tenir obligatoirement, sous la responsabilité personnelle du directeur, un registre spécial contenant toutes les informations utiles sur les transplantations réalisées tout en préservant le secret professionnel.*
Ce registre, dont le contenu est fixé par arrêté, est coté et paraphé chaque année par le président du tribunal d'instance territorialement compétent ou le magistrat désigné par lui.
Le procureur de la République ou son délégué peut, chaque fois que de besoin, procéder au contrôle du registre.
Le Conseil national du don et de la transplantation peut, à tout moment, demander à consulter le registre.
Le registre spécial est tenu en double. A la fin de l'année, le directeur de l'établissement garde un exemplaire et transmet l'autre au Comité national du don et de la transplantation ».

l'état civil, de l'administration publique et de l'entreprise, des communications électroniques et de la cryptologie, ainsi que des règles d'adaptation des procédures judiciaires.

i. Évolution du cadre juridique du contrôle des données économiques et financières

La collecte, la tenue et la publicité de données économiques et financières est passé, au Sénégal, du support papier au support électronique. Il s'agissait principalement de la collecte des informations économiques, juridiques et financières sur les entreprises, à travers le registre du commerce et, plus tard (avec l'entrée en vigueur des premiers actes uniformes de l'OHADA), le RCCM. Ce dernier avait été institué par l'Acte uniforme portant sur le droit commercial général (AUDCG) de 1997. Trois fichiers ont été conçus : Le fichier local ou fichier de base qui reçoit les différentes informations originelles ; le fichier national qui centralise et agrège les informations du fichier local et, le fichier régional tenu par la Cour commune de justice et d'arbitrage (CCJA) et destiné à recevoir les fichiers centraux nationaux des différents États membres de l'OHADA.

La réforme, en 2010, de cet acte uniforme a permis au Sénégal, à l'instar des autres États membres de l'OHADA, de se doter d'un cadre juridique relatif aux procédures et supports électroniques de déclaration, d'immatriculation et d'inscription d'informations économiques et juridiques, de contrats de crédit-bail et de sûretés au RCCM. Cette réforme, qui visait un double objectif de modernisation et d'informatisation du RCCM, permet ainsi d'interconnecter facilement les différents fichiers locaux, nationaux et régional du RCCM. Le fichier local du RCCM comporte plusieurs données nominatives des personnes physiques et morales assujetties à la publicité légale d'informations économiques et financières. En effet, aux termes de l'article 35 de l'AUDCG, le RCCM est destiné à recevoir les formalités suivantes :

- L'immatriculation des personnes physiques et morales assujetties à l'immatriculation ;
- La déclaration d'activité de l'entreprenant ainsi que ses déclarations modificatives et de cessation d'activité ;
- les dépôts des actes et pièces et mention des informations prévues par les dispositions des actes uniformes ;
- les mentions modificatives, complémentaires et secondaires ;
- la radiation des mentions y effectuées ;
- l'inscription des sûretés et des contrats de crédit-bail ainsi que les modifications, renouvellements et radiations y afférents.

Le RCCM permet également de :

- délivrer, à toute époque, les documents nécessaires pour établir l'exécution par les assujettis des formalités prévues par les actes uniformes et toute autre disposition légale ;
- mettre à la disposition du public les informations figurant dans les formulaires prévus aux articles 39 et 40 de l'AUDCG et 66 de l'AUS ;
- les différentes formalités prévues par l'ASCOOP.

Le programme d'informatisation des formulaires, des fichiers du RCCM et des procédures administratives y afférentes est porté par les dispositions des articles 79 à 100 (relatifs à la consécration et de la normalisation des procédures électroniques, ainsi que de la diffusion électro-

nique des informations) et du Règlement n° 002/2010/CM/OHADA portant création, attribution, organisation et fonctionnement du comité technique de normalisation des procédures électroniques de l'OHADA.

Grâce à cette optimisation du cadre juridique de la donnée, par l'intégration de la dimension numérique, le Sénégal a mis en place un cadre opérationnel du marché de la donnée économique à travers la plateforme numérique Sen'Infogreffe gérée par le ministère en charge de la justice. Sen'Infogreffe se propose d'offrir des services et produits liés à l'exploitation et au traitement des données économiques, suivant un modèle payant et/ou gratuit. Ces produits et services sont fournis selon une segmentation « abonnés » et « grand public ». L'opérationnalisation de ce marché de la donnée économique engendre une intégration de la donnée personnelle dans le marché de la donnée. Cela aura, au moins, deux conséquences majeures au plan des données nominatives des personnes assujetties aux différentes formalités : d'une part, elle place le risque au cœur des données économiques et financières des entreprises et rappelle l'enjeu de la protection des données personnelles ; d'autre part, ce programme met en exergue les précautions préalables à prendre pour une utilisation optimale de l'économie des données dans l'espace OHADA à partir l'interconnexion des fichiers du RCCM.

Les données économiques et financières ont été également règlementées par l'UEMOA à travers deux instruments principaux : la Centrale des incidents de paiement (CIP) et les Bureaux d'information sur le crédit (BIC). La CIP a été créée par le Règlement 15-2022 CM/UEMOA relatif aux systèmes de paiement dans les États membres de l'Union économique et monétaire ouest-africaine (UEMOA) du 19 septembre 2002. Ces dispositions, tout en édictant l'obligation de transmettre à la Banque centrale les incidents de paiement, les interdictions d'émettre des chèques, etc. (pour diffusion auprès du public), n'indiquent pas quelles sont les sanctions auxquelles s'exposent les banques en cas d'inexécution.

Les BIC s'inscrivent dans cette dynamique de collecte de l'information bancaire et financière. Au Sénégal, c'est la loi n° 2014-02 du 6 janvier 2014 portant réglementation des bureaux d'information sur le crédit dans les États membres de l'Union monétaire Ouest africaine (UMOA) qui porte le programme de l'économie des données bancaires et financières.

Aux termes de l'article 33 de la Loi, le BIC est autorisé à exercer les activités suivantes :

- collecter et stocker des informations sur le crédit ;
- traiter des informations sur le crédit ;
- fusionner différentes sources d'informations et mettre à la disposition des utilisateurs des rapports de crédit à titre onéreux ;
- diffuser des informations de crédit et des rapports pour les utilisateurs ;
- offrir des services à valeur ajoutée aux utilisateurs après autorisation de la Banque centrale ;
- toute autre activité connexe autorisée par la Banque centrale.

En vue d'exercer son activité, l'article 38 de la loi accorde au BIC le droit de collecter, conserver, traiter et diffuser dans les rapports de crédit et au titre des services à valeur ajoutée qu'il fournit, des informations publiques[28], notamment :

- l'état civil ;
- les données sur les décisions portant sur des dettes, des dossiers de procédure d'insolvabilité des liquidations d'entreprises figurant dans les registres des greffes des cours et tribunaux ;
- les données figurant dans le Registre du commerce et du crédit mobilier, le livre foncier et dans tout autre registre ou répertoire public existant au Sénégal ;
- les données contenues dans la Centrale des risques bancaires de l'UMOA (CIP-UMOA) ;
- les données figurant dans la Centrale des incidents de paiement de la Banque centrale des États de l'Afrique de l'Ouest (CIP-BCEAO) ;
- les données contenues dans la Centrale des risques des SFD ;
- les informations conservées dans la Centrale des bilans de la Banque centrale des États de l'Afrique de l'Ouest ;
- les données relatives aux accords de classement ou à tout autre système public de notation de la qualité de signature des bénéficiaires de crédit ;
- toute autre information de caractère public.

La mise en œuvre de la collecte et de la diffusion des informations sur le crédit par les BIC est structurée autour du consentement du client. Le contenu du consentement et les modalités d'obtention de ce consentement sont fixés par l'Instruction n° 002-01-2015 du 13 janvier 2015 de la BCEAO, relative aux modalités d'obtention du consentement du client par les fournisseurs de données aux BIC dans le cadre du système de partage d'information sur le crédit dans les États membres de l'UMOA. Selon cette Instruction, le consentement désigne l'autorisation écrite, signée, spécifique et informée par laquelle, le client, personne physique ou morale, donne explicitement son accord au prêteur ou au fournisseur de services de partager les données le concernant, y compris ses données personnelles[29], avec les utilisateurs et le BIC ou pour consulter auprès du BIC des informations sur sa solvabilité. Cependant, même si, en principe, la collecte de données sensibles[30] est exclue[31], l'Instruction semble faire coïnci-

[28] Il convient de souligner l'incohérence de cette disposition qui considère des personnelles parfois sensibles comme des informations publiques. Il en est ainsi de certains éléments de l'état civil (situation matrimoniale par exemple), des informations de solvabilité (ou donc d'insolvabilité), voire même des décisions de condamnation intervenues dans le cadre des procédures d'insolvabilité.

[29] Voir note ci-avant.

[30] Aux termes de l'article 1er de la Loi sur les BIC, constituent des données sensibles, « les données à caractère personnel relatives aux opinions ou activités religieuse, philosophique, politique, syndicale, à la vie sexuelle ou à la race, à la santé et aux mesures d'ordre social ».

[31] Aux termes de l'article 62 de la Loi sur les BIC, « il est interdit aux fournisseurs et aux utilisateurs de données ainsi qu'au BIC de collecter, conserver, traiter, diffuser, montrer dans un rapport de crédit, ou sous toute autre forme, format ou support, des données sensibles.

La même interdiction s'applique aux données sur les soldes et transactions des comptes d'épargne, des comptes chèques à l'exception des comptes de chèques impayés, des certificats de dépôt de toute nature, des autres dépôts ou autres produits similaires.

der le moment d'obtention du consentement avec la période de la demande de prêt par le client. Ce faisant, en choisissant de recueillir le consentement à la collecte de données lors de l'ouverture du crédit[32], le législateur ne permet pas d'avoir un consentement libre et éclairé, et de préserver les droits du client.

ii. Mutations du cadre juridique de l'état civil

L'état civil ne peut être établi et prouvé que par les actes de l'état civil. Il en résulte une importance primaire de l'état civil comme outil de gouvernance de toute l'existence humaine. Sans état civil, il n'existe pas d'identité civile (personnalité juridique), de citoyenneté (apatridie), de droits citoyens (droits électoraux notamment).

Au-delà de l'enjeu juridique et politique de la maîtrise de l'état civil, se greffe un nouvel enjeu économique lié à la promotion de l'économie numérique. Aucune économie numérique viable ne peut être envisagée sans une sécurité de la chaîne des faits d'état civil. Au regard de cette place cruciale de l'état civil dans la civilisation humaine, l'État du Sénégal a entrepris de renforcer la fiabilité et la sécurité de son système d'état civil en déroulant un important programme d'informatisation de l'état civil. Le cadre juridique est adossé sur les Déclarations de Durban (Afrique du Sud) des 6-7 Septembre 2012[33] et de Yamoussoukro (Côte d'Ivoire) du 13 février 2015[34] sur les faits d'état civil.

Dès la Conférence de Durban, les États membres se sont engagés à : « adopter les technologies appropriées pour accélérer l'enregistrement des faits d'état civil, la gestion des informations d'état civil et assurer leur protection contre les catastrophes naturelles, les guerres civiles, etc. ». Aujourd'hui, tous les efforts sont concentrés sur la mise en place d'un système d'information de l'état civil et à la consolidation d'un fichier national d'identité biométrique au Sénégal. Toutefois, « les dispositifs biométriques, parce qu'ils permettent d'identifier une personne par ses caractéristiques physiques, biologiques, sont particulièrement sensibles et doivent faire l'objet d'une attention particulière, notamment de la part des autorités de protection des

---

Il est expressément interdit au BIC et aux utilisateurs de fournir ou de demander, tout type d'informations et de rapport de crédit à des fins de marketing ou à des fins autres que celles prévues par la présente loi ».

[32] Aux termes de l'article 2, alinéas 4 et 5 de l'Instruction n° 002-01-2015 de la BCEAO du 13 janvier 2015, relative aux modalités d'obtention du consentement du client , « *Le consentement ne peut être obtenu que par le biais du formulaire joint en annexe à la présente instruction en ce qui concerne les demandes de prêt aux guichets des établissements assujettis.*

Pour les demandes de prêts par Internet, le consentement du client peut être obtenu à partir de plate- formes électroniques garantissant :

- l'identification de l'établissement émetteur du formulaire de consentement ;
- la confidentialité de son contenu ;
- la non-répudiation du formulaire de consentement par son auteur ;
- l'intégrité de son contenu ;
- l'authentification du client ;
- la disponibilité de l'archivage du formulaire de consentement ».

[33] Déclaration de la deuxième Conférence des ministres africains chargés de l'enregistrement des faits d'état civil, Durban, Afrique du Sud des 6-7 Septembre 2012.

[34] Déclaration de la troisième Conférence des ministres africains en charge des faits d'état civil du 13 février 2015, Yamoussoukro, République de Côte d'Ivoire.

données personnelles quand elles existent[35] ». L'informatisation des fichiers d'état civil et la mise en place d'un fichier national d'identité biométrique constituent donc un traitement de données à caractère personnel et, de ce fait, entrent dans le champ d'application de la Loi sur les données à caractère personnel, et requièrent une autorisation de la CDP pour leur déploiement. Pourtant, selon les enquêtes et entretiens réalisés auprès de la CDP, le programme a démarré sans que les formalités déclaratives préalables aient été accomplies.

Cette situation interpelle sur l'exigence de conformité de toute la gouvernance publique en matière de protection de données personnelles, en particulier dans le cadre de l'administration électronique.

iii. Changements des cadres juridiques de l'administration publique

La loi n° 2008-10 du25 janvier 2008 portant Loi d'orientation relative à la société de l'information est la base décisive du cadre juridique de l'administration publique électronique sénégalaise. Elle fait également office de texte de base de la digitalisation des activités des entreprises privées.

L'article 9 de cette loi énonce que « l'État et ses démembrements, les organisations de la société civile, les entreprises et les personnes privées concourent, chacun dans le domaine de sa compétence et dans les limites de sa responsabilité, à une politique dont l'objectif est le développement harmonieux de la société de l'information... ». Le législateur engage les différents acteurs dans un vaste chantier de l'e-administration publique ou privée à travers une mission « d'intérêt général [consistant] à promouvoir, produire et utiliser les technologies de l'information et de la communication dans tous les secteurs de la vie économique, sociale, scientifique et culturelle ». Dans le cadre de l'administration publique électronique, les règles de base sont énoncées sous le titre IV de la loi n° 2008-08 sur les transactions électroniques. Ces dispositions posent le principe selon lequel « tous les échanges d'informations, de documents ou des actes administratifs peuvent faire l'objet d'une transmission par voie électronique » et déterminent, spécialement, le régime des procédures électroniques de passation de la commande publique.

Cela postule que les administrations publiques financières doivent se conformer aux dispositions de la loi et du décret sur les données personnelles, dès lors qu'elles sont inéluctablement appelées à effectuer des traitements de données personnelles. L'exigence se pose surtout avec acuité dans notre contexte de généralisation des communications électroniques qui accentue la circulation et l'exposition des données.

iv. Réforme du cadre juridique des communications électroniques

Les communications électroniques renvoient à « toute mise à disposition au public ou d'une catégorie de public, par un procédé de communication électronique ou magnétique, de signes,

[35] Organisation internationale de la Francophonie, Guide pratique pour la consolidation de l'état civil, des listes électorales et la protection des données personnelles : enjeux et principes fondamentaux, p. 12, disponible sur https://www.francophonie.org/sites/default/files/2020-01/oif_guide-pratique_etatcivil-27-11-14.pdf (consulté le 05 juin 2022).

de signaux, d'écrits, d'images, de sons ou de messages de toute nature » (article 2-1°de la loi n° 2008-08 sur les transactions électroniques) :

Les communications électroniques, au sens large, renvoient à plusieurs domaines que sont les télécommunications, l'Internet, le commerce électronique, la poste électronique, l'audiovisuel et la presse électronique, les transactions électroniques, etc. Au sens strict, elles désignent les télé-communications et l'Internet.

Au Sénégal, les communications électroniques *lato sensu* sont régies par la loi n° 2018-28 du 12 décembre 2018 portant code des communications électroniques. L'article 8 de texte renvoie à la Loi sur les données à caractère personnel pour la protection des données collectées, transmises ou stockées par les opérateurs de communications électroniques. Néanmoins le chapitre V du titre I, portant sur la protection de la vie privée des utilisateurs des réseaux et services de communications électroniques, posent les règles spécifiques de régulation des données collectées et circulant sur les réseaux de communications électroniques. Il s'agit des articles 36 à 44. Ces dispositions :

- autorisent les opérateurs de services de communications électroniques, dans le respect de la règlementation sur les données à caractère personnel, à conserver les données des utilisateurs pour les besoins de leurs opérations de facturation, de paiement ou de recouvrement des services, sous réserves que les données conservées ne portent pas sur le contenu des correspondances. Cette possibilité est mise en œuvre conformément aux dispositions d'un décret pris après avis de la CDP ;
- admettent qu'un opérateur puisse réaliser, pour une durée déterminée, un traitement des données du trafic dans l'optique de commercialiser ses propres services de communications électroniques ou de fournir aux utilisateurs des services à valeur ajoutée, à la condition de requérir le consentement préalable de l'utilisateur ;
- obligent les opérateurs de services de communication électroniques à identifier les abonnés ou utilisateurs ;
- astreignent les opérateurs au respect de la règlementation relative à la protection des données à caractère personnel dans le cadre de l'édition et de la diffusion de la liste ou annuaire d'abonnés ;
- imposent à tout opérateur d'effacer ou de rendre anonymes les données de trafic des utilisateurs, sous réserve, pour celui-ci de mettre un place un mécanisme adéquat permettant de déférer correctement aux réquisitions des autorités compétentes. L'éventualité de la transmission de ces données à l'autorité compétente autorise l'opérateur à différer de deux ans au plus son obligation d'effacer ou de rendre anonyme les données relatives au trafic ;
- exigent des opérateurs l'institution d'un mécanisme technique de blocage des communications sur les terminaux déclarés volés, sur demande du propriétaire identifié ou sur réquisition du juge ou des services de police ;
- déterminent les droits des utilisateurs dans le cadre de l'édition et de la diffusion de la liste d'abonnés par les opérateurs, tels que : (i) le droit de s'opposer (dans la limite compatible avec les exigences de la constitution d'annuaire) à l'inscription de certaines données personnelles dans les annuaires ; (ii) le droit d'être informé des fins pour lesquelles l'annuaire est constitué et celles auxquelles son utilisation peut donner lieu.

En tout état de cause, le consentement de l'abonné est requis pour toute inscription de données à caractère personnel dans l'annuaire de tout opérateur de téléphonie mobile.

Cependant, aussi bien dans les textes spécifiques à la protection des données personnelles que dans le code des communications électroniques, le consentement, élément-pivot du système de régulation du traitement des données, est encadré de manière insuffisante. Les modalités du consentement sont définies de manière non-exhaustive, tandis que la charge de la preuve de ce consentement semble être régie par le droit commun. En outre, aucune disposition précise ne résout le problème du consentement du mineur, notamment la forme et les modalités de ce consentement[36]. Enfin, en dépit du contexte lié au niveau d'instruction ou d'alphabétisation des populations, et malgré les principes portés par le service universel (inclusion), aucune disposition dérogatoire n'a été prévue pour les personnes ne sachant ni lire ni écrire (illettrisme) ou ne pouvant ni lire ni écrire correctement (handicap). Il s'ensuit que seules les dispositions du Code des obligations civiles et commerciales (COCC) seront applicables à la charge de la preuve du consentement. Une telle perspective ne protège pas l'utilisateur. Il serait plus indiqué de faire peser sur l'opérateur la charge de la preuve du consentement préalable de l'abonné ou du client. Cette option du renversement de la charge de la preuve a été consacrée par la loi 2008-12 sur les données à caractère personnel pour (i) les contestations portant sur le caractère manifestement abusif des demandes en rapport avec l'exercice du droit d'accès (articles 66 de la loi 2008-12), et (ii) pour les contestations liées à l'instruction effective et correcte, par le responsable du traitement, des demandes de rectification ou de suppression (article 69 de la loi 2008-12). Ainsi, ces dispositions font peser sur le responsable du traitement, la charge de la preuve du caractère abusif des demandes d'accès. C'est également à lui de prouver, dans le cadre des demandes de rectification ou de suppression de données, qu'il a procédé aux rectifications et suppressions réclamées.

La même règle, sous réserves d'aménagements, aurait pu être retenue pour la preuve du consentement à la collecte, à la conservation et au traitement de données personnelles, en raison de l'asymétrie des forces entre le responsable du traitement et l'utilisateur des services de communications écrites.

Cette question de la protection des données se pose d'une manière plus ou moins différente dans le code de la presse qui a, globalement, opté pour une protection pénale.

v. *Révision du cadre juridique de la presse écrite et de la communication audiovisuelle*

La loi n° 2017-27 du 13 juillet 2017 portant code de la presse a réformé le cadre juridique de la presse écrite et de la communication audiovisuelle et doté la presse en ligne d'un cadre légal. Cette réforme s'est imposée compte tenu du « *contexte de bouleversement du secteur, qui se manifeste par une pluralité de vecteurs de l'information et de la communication (développement considérable de la presse écrite, libéralisation de l'audiovisuel, entraînant la création de plusieurs radios et télévisions privées, et utilisation de l'Internet comme moyen de diffusion de l'information*

[36] L'article 4-4°) de la loi 2008-12 énonce, certes, que le consentement de la personne concernée désigne « toute manifestation de volonté expresse, non équivoque, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou conventionnel, accepte que ses données à caractère personnel fassent l'objet d'un traitement manuel ou électronique » ; mais il n'en demeure pas moins que rien n'est précisé quant à la charge de la preuve de ce consentement.

au public) … [contexte marqué] *par une multiplication des dérives dans le secteur de la presse, notamment des atteintes aux droits de certains citoyens et des abus dans des émissions d'animation* ». Cette loi n° 2017-27, intervenant dans un contexte d'accroissement des usages numériques, a voulu instituer une pédagogie de la conscience professionnelle en matière de journalisme en posant, dans les dispositions préliminaires relatives à l'organisation de la profession, les devoirs du journaliste. Ces devoirs engagent le journaliste et le technicien des médias, notamment :

- à une éthique professionnelle à travers la recherche de la vérité, en toute honnêteté et en toute impartialité (article 11), sans déformer les faits, dénaturer les textes, sons, images et opinions d'autrui (article 13), à une investigation loyale (article 14) ;
- au respect de la dignité de la personne et de la dignité humaine, ce qui proscrit l'atteinte à la vie privée, la divulgation de l'intimité de la vie privée d'autrui, la publication de la souffrance humaine ainsi que la publication, par quelque moyen que ce soit, de montage réalisé avec les paroles ou l'image d'une personne, sans son consentement (articles 17 et 18).

Ces règles sont complétées par deux autres obligations générales : celle du respect de la vie privée et des bonnes mœurs (article 57, alinéa 1) et de respect de la règlementation relative à la protection des données à caractère personnel (article 58).

vi. Institution d'un cadre juridique de la cryptologie

Pour prévenir la cybercriminalité qui sape la confiance des divers acteurs de la société de l'information, outre répression pénale des agissements qui violent la structure ou le contenu des systèmes informatiques, la cryptographie a été mise à profit afin de rendre ces systèmes inattaquables, et les informations y contenues inaccessibles.

La cryptographie est régie, au Sénégal, par la loi n° 2008-41 du 20 août 2008 sur la cryptologie. A la lumière de l'article 1er *in fine* de cette loi « *la cryptologie, composée de la cryptographie et de la cryptanalyse, tend à assurer la protection et la sécurité des informations notamment pour la confidentialité, l'authentification, l'intégrité et la non répudiation des données transmises* ». Toute donnée peut être cryptée. De même, l'accès à tout système informatique peut l'être. Le prestataire de services de cryptologie peut alors être appelé à manipuler des données de toute nature, dont des données à caractère personnel. Il peut même, sciemment, manipuler ces données à des fins autres que celles destinées à assurer la gestions des conventions secrètes de cryptage ou de décryptage, à l'insu du cocontractant. C'est pourquoi, l'article 18 de la loi sanctionne, au plan civil, la faute du prestataire technique.

Cette responsabilité civile est complétée par une responsabilité pénale énoncée à l'article 6 du titre III du code pénal consacré aux infractions en matière de cryptologie. Ainsi, « *quiconque aura mis en place un accès dérobé à des données ou à un système informatique sans l'autorisation de l'utilisateur légitime, sera puni d'un emprisonnement de deux (2) ans à cinq (5) ans et d'une amende de 2 000 000 Francs à 30 000 000 Francs ou de l'une de ces deux peines seulement* ».

La répression pénale, réponse ex-post à la violation des droits des personnes concernées par des traitements de données personnelles est, en principe, la dernière option ; celle à envisager lorsque les réponses préventives auront échoué ou se seront révélées insuffisantes. C'est pour-

quoi le titre III du Code pénal issu de la loi n° 2008-41 du 20 août 2008 sur la cryptologie a été renforcé/complété par un nouveau titre IV institué par la loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal.

vii. Modification du code pénal

La loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal a institué un titre IV intitulé « *Des infractions liées aux technologies de l'information et de la communication* », dont le chapitre II est relatif aux atteintes aux données informatiques. Dans ce chapitre, le législateur a consacré la section II aux atteintes spécifiques aux droits de la personne au regard du traitement des données à caractère personnel. Quatre faits ont été érigés en infraction. Il s'agit de :

- le fait, même par négligence, de procéder ou faire procéder à des traitements de 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 (article 431-14), 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 ;
- le fait de procéder ou de faire procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne conformément aux dispositions de l'article 68 de la Loi sur les données à caractère personnel, lorsque ce traitement répond à des fins de prospection, notamment commerciale, ou lorsque cette opposition est fondée sur des motifs légitimes (article 431-20). Cette infraction est punie 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 ;
- le fait, hors les cas prévus par la Loi, de mettre ou de conserver sur support ou mémoire informatique, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales ou qui sont relatives à la santé de celui-ci (article 431-21). Cette violation de la règlementation sur les données personnelles est punie 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.

viii. Mise en cohérence des règles procédurales

La dimension procédurale de la protection des données personnelles se justifie par l'exposition de ces données dans toute procédure, pénale ou extra-pénale. Cette exposition des données résulte du fait qu'elles peuvent, soit être requises à titre de preuve, soit être collectées et conservées comme bases de données judiciaires.

L'utilisation des données personnelles à titre probatoire n'est pas interdite par la Loi sénégalaise sur les données à caractère personnel. Elle est même autorisée, puisque les articles 20-2°) et 21-2°) incluent dans le champ des traitements autorisés ceux en rapport avec la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté. De même, l'article 41-5°) dispose que l'interdiction de collecter et/ou de traiter des données 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, ne s'applique pas lorsqu'une procédure judiciaire ou une enquête pénale est ouverte. Cela sous-entend que la collecte et le traitement de ces données dans la cadre de la procédure sont effectués à toutes fins utiles à la manifestation de la vérité, y compris dans le cadre de l'administration de la preuve. Toutefois, la Loi n'indique pas à quelles conditions et suivant quelles modalités concrètes ces données peuvent être recueillies et traitées à titre probatoire devant l'autorité judiciaire. L'article 48 de la Loi se contente simplement d'interdire le recours aux seules données personnelles ou aux traitements de ces données pour fonder, exclusivement, une décision judiciaire ou administrative ou toute autre décision produisant des effets juridiques.

Quant à la collecte et la conservation des données dans le cadre de la constitution des bases de données judiciaires, elles semblent être autorisées par l'article 42[37] de la loi n° 2008-12. Les juridictions et les auxiliaires de justice sont ainsi habilités à collecter et à traiter les données personnelles aux conditions et suivant les modalités fixées par ledit article.

Le décret 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 aurait pu préciser davantage les conditions du traitement de données personnelles dans le cadre d'une procédure juridique (judiciaire ou extrajudiciaire) et indiquer les conditions et limites de la constitution de bases à partir des données personnelles judiciaires.

Ces quelques insuffisances attestent de l'opportunité d'un processus adéquat d'élaboration de la loi.

3. Le processus d'élaboration du cadre juridique des données personnelles

Au Sénégal, le processus d'élaboration des textes relatifs aux données personnelles n'est pas dissociable du processus global de mise en place du cadre juridique de la société sénégalaise de l'information, même si la dynamique des mutations sociales, notamment politiques, économiques et administratives auraient dû entrainer une réaction plus précoce et alerte quant à la protection spécifique des données personnelles. Cela est souvent imputable à l'absence d'une stratégie cohérente et transversale propre à la problématique de la donnée en général et de la donnée personnelle en particulier.

Le processus d'élaboration du cadre juridique de la société sénégalaise de l'information et des données personnelles a abouti en 2008. Toutefois, il a été précédé d'une première période de prospection. En effet, en 2002, à la tribune des Nations unies, le président Abdoulaye Wade avait judicieusement rappelé que « *le monde ne deviendra véritablement un village planétaire que lorsque toutes ses composantes auront la chance de participer à l'interaction que favorise la*

[37] Article 42 de la loi n° 2008-12 du 25 janvier 2008 sur la protection des données à caractère personnel : « Le traitement des données 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 ».

proximité rendue possible par les nouvelles technologies de l'information et des communications[38] ». Ainsi, en 2004, les réflexions portaient déjà sur l'arbitrage entre les données personnelles, les libertés publiques et la protection des droits de la propriété intellectuelles dans un contexte d'essor des civilisations et de l'économie numériques. Le Sénégal, en partenariat avec l'Agence universitaire de la Francophonie (AUF) et le Service de coopération et d'action culturelle (SCAC) de l'ambassade de France, a réuni des experts à l'effet de réfléchir sur les enjeux et les défis de la société de l'information[39].

Au gré des transformations sociales obtenues grâce au numérique (Intranet gouvernemental, cartes d'identité numérisées et biométriques, etc.), le gouvernement sénégalais a accéléré, en 2005, le processus de mise en place du cadre juridique de la société de l'information. Sous l'égide de l'ADIE, un séminaire de cadrage du futur *corpus juris* a été tenu les 29 et 30 août 2005, en partenariat avec le SCAC de l'ambassade de France et du Centre de formation judiciaire (CFJ) du Sénégal. L'objectif de ce séminaire était de définir les contours du cadre juridique à intervenir, à savoir une loi-cadre contenant les principes de base de la société de l'information et des textes sectoriels portant sur les transactions électroniques, les données à caractère personnel, la cybercriminalité et la sécurité technique des données et des systèmes informatiques. La justification de cette accélération qui a fait du Sénégal le pionner en matière d'encadrement des usages résultant de la société de l'information en Afrique de l'Ouest francophone, résidait dans le fait que « [les TIC] *qui laissent espérer le meilleur en matière de communication, d'éducation et de partage de l'information, font effectivement craindre le pire en matière d'atteintes potentielles aux libertés individuelles, de détournement de fichiers, de criminalité organisée et de terrorisme*[40] ».

Ce Séminaire a donc été organisé pour échanger autour des projets de textes suite au « cyber audit juridique et institutionnel de [l'arsenal] législatif et réglementaire qui a abouti à la proposition de l'élaboration d'une Loi d'orientation sur la société sénégalaise de l'information (LOSI) et la production de trois projets de lois prioritaires portant sur les données personnelles, la cybercriminalité et l'économie numérique[41] ». Au terme des discussions, en tirant également profit de l'expérience de la sous-région à travers l'exemple du Burkina Faso, les experts ont croisé le regard sur le processus en cours au Sénégal et l'ont enrichi des apports de la communauté internationale ; ce qui a permis de prendre la mesure des efforts à déployer pour faire jouer au droit un rôle positif dans la préservation des valeurs de la société de l'information,

---

[38] Discours du président Abdoulaye Wade à la réunion de l'Assemblée générale des Nations unies sur les technologies de l'information et de la communication au service du développement (New-York, 17-18 juin 2002), disponible sur http://www.osiris.sn/Intervention-de-SEM-Abdoulaye-Wade.html (consulté le 11 juin 2022).

[39] Direction de l'informatique de l'État du Sénégal, Service de coopération et d'action culturelle de l'ambassade de France, Agence universitaire de la Francophonie, *Conférences « Société de l'information : Échanges d'expériences entre la France et le Sénégal : " La protection des données personnelles et des libertés publiques, les responsabilités sur l'Internet, la propriété littéraire et artistique et l'Internet, les enjeux industriels de la distribution de contenus"* », Dakar, 28 juin-2 juillet 2004.

[40] M. Sonko (Président du Conseil d'État du Sénégal), « Préface », in Agence de l'informatique de l'État du Sénégal, Service de coopération et d'action culturelle de l'Ambassade de France, *Informatique et libertés, quel cadre juridique pour le Sénégal ?*, Actes du Séminaire « *Informatique et libertés, quel cadre juridique pour le Sénégal ?* », Dakar, 29-30 août 2005, p. 9, disponible sur http://www.adie.sn, (consulté le 15 août 2008).

[41] M. T. Seck (Directeur général de l'Agence de l'informatique de l'État), Discours d'ouverture au séminaire « *Informatique et libertés, quel cadre juridique pour le Sénégal ?* », Dakar, 29-30 août 2005, p. 14, disponible sur http://www.adie.sn, (consulté le 15 août 2008).

veiller au respect des droits fondamentaux dans le traitement des données à caractère personnel et faire confiance au rôle créateur du juge dans un environnement juridique pluraliste en constante évolution[42].

C'est de ce séminaire que sont issus les recommandations sur les avant-projets de textes suivants :

- l'avant-projet de Loi d'orientation relative à la société sénégalaise de l'information ;
- l'avant-projet de Loi sur les transactions électroniques ;
- l'avant-projet de Loi sur les données à caractère personnel ;
- l'avant-projet de Loi sur la cybercriminalité.

Quant à l'avant-projet de Loi sur la cryptologie, élaboré sous l'égide de l'Agence de régulation des télécommunications (ART), il a été versé, plus tard, au panier des quatre premiers projets. Cela explique d'ailleurs qu'il a été adopté en dernier lieu, près de huit mois après l'adoption de ceux-ci.

Il apparait donc que les données personnelles ont été intégrées dans le champ global de la société de l'information ou, à tout le moins, durant la phase de la mise en place des premiers éléments du cadre juridique.

4. Le financement de l'élaboration du cadre juridique des données personnelles

Au moins trois catégories d'acteurs interviennent dans l'élaboration des lois : d'abord, les acteurs du pouvoir normatif (Gouvernement, Parlement, autorités sectorielles, etc.), ensuite, les acteurs de la société civile et, enfin, les ingénieurs du droit, les lobbys, les partenaires techniques et financiers. Cette dernière catégorie d'acteurs constitue la preuve que l'élaboration et la mise en œuvre des textes juridiques nécessitent parfois, des moyens financiers conséquents car, le coût de l'expertise et de l'accompagnement juridiques, nécessaires en amont, peut être élevé.

Mais au-delà de ce coût, l'enjeu véritable est de maîtriser les différentes stratégies d'influence qui peuvent se cacher derrière l'offre extérieure d'expertise juridique ou les mesures d'accompagnement juridique et financier proposées par des partenaires étrangers.

Dans le contexte sénégalais, il convient de souligner, qu'en théorie, l'élaboration du cadre juridique initial a été globalement endogène. L'explication réside, sans doute, dans le fait que la problématique était, en Afrique et au Sénégal, à ses balbutiements. Même si l'on ne peut véritablement avoir une idée de la nature de l'appui extérieur (appui technique et/ou financier), il n'en demeure pas moins que la participation, au moins technique, du Service d'action culturelle de l'ambassade de France a été relevée. Il s'agirait davantage d'un appui technique, au regard de l'objet des activités co-organisées par l'État sénégalais et ce partenaire extérieur (notamment, le séminaire « *Informatique et libertés, quel cadre juridique pour le Sénégal ?* », op. cit.).

[42] A. Cissé, « Synthèse », in Agence de l'informatique de l'État du Sénégal, Service de coopération et d'action culturelle de l'Ambassade de France, *Informatique et libertés, quel cadre juridique pour le Sénégal ?*, op. cit., p. 205.

Par suite, dans le cadre de la mise en œuvre du cadre juridique, plusieurs acteurs étrangers ont accompagné le gouvernement ou ont collaboré avec l'État du Sénégal. C'est le cas, notamment de la coopération/collaboration avec World Vision, le Haut-Commissariat des Nations unies pour les réfugiés (HCR), l'Organisation Internationale pour les migrations (OIM), la Croix Rouge, l'Union européenne (UE), la Banque mondiale avec l'implémentation du Programme d'identification unique pour l'intégration régionale et l'inclusion (WURI) pour l'harmonisation des législations sur les faits d'état civil), la délégation de l'UE comme levier d'appui aux programmes sectoriels ou nationaux en matière de données personnelles, la GIZ (coopération allemande), l'Alliance Smart Africa (qui accompagne les projets numériques nationaux et grâce à laquelle le Sénégal a obtenu un accompagnement sur le programme relatif à la protection des données personnelles). Cette collaboration avec Smart Africa a permis d'élaborer des lignes directrices en matière de protection des données personnelles qui sont en voie d'être adoptées par les États membres de l'Organisation à travers le réseau africain des autorités de protection des données à caractère personnel.

L'appui ou l'intervention des acteurs peut être des leviers d'influence extérieure, susceptibles d'affecter l'autonomie de la stratégie nationale, surtout lorsque ces influences émanent d'acteurs étrangers susceptibles d'avoir des intérêts divergents avec ceux de l'État du Sénégal. Toutefois, pour l'heure, il existe peu d'éléments objectifs sur le sens de ces axes de coopération auxquels le Sénégal est partie.

En tout état de cause, cette coopération entre le Sénégal et les partenaires extérieurs est nécessaire à la mise en œuvre adéquate de notre *corpus juris*, à charge pour nos décideurs d'avoir à l'esprit le caractère stratégique de la régulation des données personnelles et les enjeux de souveraineté qui s'y attachent.

5. La mise en œuvre du cadre juridique des données personnelles

La mise en œuvre du cadre juridique relatifs aux données personnelles incombe à plusieurs autorités techniques dont la CDP, le CNRA, l'ARTP ainsi qu'au juge et à tous les acteurs de la chaîne pénale.

La CDP est l'organe spécialisé de protection. Pour l'exercice de ses missions, elle dispose d'une dotation budgétaire annuelle de trois cents (300) millions de francs CFA destinée aux dépenses sociales, salariales et fiscales à hauteur de 90 %, le reste étant consacré aux dépenses de fonctionnement. Au plan du capital humain, la CDP dispose de trente-et-un (31) agents, dont une quinzaine d'agents cadres dont deux cyber-techniciens, cinq juristes dont deux cadres, deux non-cadres et un stagiaire.

Même si ses ressources budgétaires et humaines sont jugées insuffisantes (enquête et entretien auprès de la CDP), textuellement, la CDP, en tant qu'organe spécialisé, a des pouvoirs étendus pour l'exercice de ses attributions en matière contrôle et de sanction, le cas échéant. Elle a une compétence exclusive en matière de sanctions administrative, quoique ses décisions soient susceptibles de recours devant la chambre administrative de la Cour suprême.

La CDP est, d'abord, chargée de veiller à la conformité des traitements et, à ce titre, dispose d'un pouvoir sur tous les responsables de traitements, publics comme privés, sur la base d'un contrôle sur place ou sur pièces. Ensuite, elle a un pouvoir de sanction qu'elle a déjà mis en

œuvre. En outre, elle a une mission de veille, de formation, de sensibilisation, d'éducation. Par ailleurs, elle a un pouvoir consultatif qui permet d'interpréter les textes dans les situations qui pourraient fonder l'usage par elle de ses pouvoirs de sanction. Enfin, l'Autorité a un pouvoir règlementaire pour compléter la Loi et le décret sur des questions nouvelles.

Dans les faits, la mise en œuvre des sanctions se traduit d'abord, par la mise en demeure. Dans le texte actuellement en vigueur, la mise en demeure est une véritable sanction. Une fois prononcée, la mise en demeure est presque systématiquement respectée par le responsable de traitement mis en cause. A ce titre, le taux d'effectivité de cette sanction est maximal.

La CDP est également habilitée à prononcer des sanctions pécuniaires. A cet égard, elle a déjà prononcé une amende. Son recouvrement étant du ressort de l'agent judiciaire de l'État, la CDP est dessaisie une fois la sanction prononcée. Partant, elle dispose de peu de mécanismes pour s'assurer du recouvrement effectif de l'amende, sauf retour d'information de l'agent judiciaire de l'État.

Le CNRA et l'ARTP interviennent, le premier pour la régulation des contenus audiovisuels, la seconde pour la régulation de l'utilisation des ressources rares ou techniques. Par exemple, en 2018, le CNRA a indiqué les enjeux stratégiques de la protection nationale des droits numériques dans un contexte d'universalisation des communications électroniques et des risques qui lui sont inhérentes. Il a alerté l'État du Sénégal dans le Mémorandum du 30 août 2018 portant constatations et observations du CNRA relatives au litige opposant le groupe EXCAF TELECOM à la société STARTIMES sur l'exercice illégal d'activités de distributions de services de communication audiovisuelle et la commercialisation de décodeurs pour la télévision numérique terrestre (TNT) au Sénégal. Le CNRA invite à « *veiller à la stabilité et à la sécurisation du paysage audiovisuel, au moment où les sociétés de télécommunications, les acteurs de moteurs de recherches, les GAFAM (Google, Amazon, Facebook, Apple, Microsoft) ont investi le secteur de l'audiovisuel traditionnel ainsi que les plateformes digitales avec, en appoint, des services à valeur ajoutée. Tout cela vient s'ajouter à l'installation d'opérateurs audiovisuels commercialisant des bouquets satellitaires cryptés, sans jamais honorer quelque redevance auprès des institutions et structures compétents de l'État. Un tel environnement accentue le danger imminent de voir des sociétés étrangères faire main basse sur nos systèmes de communication, de production et de transmissions d'idées, nos modes de cultures voire notre vivre ensemble*[43] ». Ce mémorandum, qui insiste sur l'illégalité des opérations de communication audiovisuelle par satellite, opérées par STARTIMES, repose avec acuité la problématique de la souveraineté de l'État du Sénégal sur ses ressources numérique[44].

---

[43] CNRA, « Mémorandum du 30 août 2018 portant constatations et observations du CNRA relatives au litige opposant le groupe EXCAF TELECOM à la société STARTIMES sur l'exercice illégal d'activités de distributions de services de communication audiovisuelle et la commercialisation de décodeurs TNT au Sénégal », in CNRA, Rapport 2018-2019, pp. 93-99.

[44] Le régulateur de l'audiovisuel, a également, par décision n° 001 du 29 mars 2019, instruit et délibéré sur la plainte déposée par l'ONG JAMRA et le Comité de défense des valeurs morales au Sénégal (CNRA, Rapport 2018-2019, p. 100). La plainte, dirigée contre la 2STV, faisait grief à celle-ci d'avoir diffusé un téléfilm comportant des séquences contraires aux dispositions légales et règlementaires et à ses cahiers des charges. L'instruction du dossier a révélé :

- des propos, comportements et images choquants, indécents, obscènes ou injurieux ;
- des scènes de grande violence ou susceptibles de nuire à la préservation des identités culturelles.

Mais les institutions techniques spécialisées n'ont pas le monopole de la régulation des usages nés des données personnelles, la Loi n'accordant aucune exclusivité ni à la CDP, ni au CNRA ou à l'ARTP. Dès lors, les individus, en fonction de la nature et de l'objet du litige, ont le choix entre saisir l'une quelconque d'entre elles, en particulier la CDP, ou porter l'affaire devant le juge répressif ou civil, ou encore devant les autorités de police judiciaire (police ou gendarmerie).

Il faut souligner que certains citoyens se méprennent sur le champ de compétence de la CDP et pensent que celle-ci est compétente en matière pénale ou en matière de responsabilité civile ; ce qui n'est pas le cas. C'est pourquoi, lorsque la CDP est saisie au pénal ou pour les intérêts civils, elle transmet le dossier au parquet ou invite le requérant à mieux se pourvoir.

Lorsqu'elle est saisie, à tort, au pénal et qu'elle transmet le dossier aux autorités de la chaîne pénale, le seul outil dont dispose la CDP pour s'assurer de l'instruction effective, ce sont généralement les retours d'avis des plaignants, puisque le retour d'information de la part du parquet n'est pas systématique (car il n'existe pas de canaux formels de coordination entre la CDP et la chaîne pénale).

En définitive, la mise en œuvre du cadre juridique des données personnelles incombe à plusieurs institutions. Elle va au-delà du contrôle de conformité et de la sanction et englobe toutes les actions en amont de l'application des textes par ses destinataires (information, formation et sensibilisation) et en aval (évaluation). C'est en cela que les quelques préconisations suivantes permettront aux autorités compétentes ainsi qu'à toutes les parties prenantes, de procéder, le cas échéant, aux réajustements et corrections nécessaires.

Cette décision pose la question de la nature des droits protégés par la LDP, natomment sur l'existence de droits collectifs d'une communauté sociale, professionnelle, religieuse ou raciale.

V. PROPOSITIONS ET RECOMMANDATIONS

Le Sénégal a amorcé sa transformation digitale depuis plus d'une décennie. Aujourd'hui, le Gouvernement ambitionne d'aller plus loin. Par le biais du ministère en charge des télécommunications, il est en train de mettre en place une Stratégie nationale sur l'intelligence artificielle dont l'objectif est de réguler les algorithmes. Au regard de l'intérêt suscité par l'IA, des rencontres et études transdisciplinaires regroupant mathématiciens, politiques, juristes, sociologues, etc., esquissent une cartographie des prérequis pour l'utilisation adéquate et sure de l'intelligence artificielle (IA). D'ores et déjà, la société civile lance l'alerte sur la nécessaire articulation entre le cadre juridique de l'intelligence artificielle et celui relatif aux données personnelles.

Il faut néanmoins souligner que l'opérationnalité des diverses application de l'IA au Sénégal sera tributaire d'un égal accès au marché de la donnée, aujourd'hui dominée par les géants dits GAFAM. Cela pustule la nécessité d'une modération des plateformes en vue de contrecarrer les monopoles, la capacité des petites plateformes nationales étant inhibée par celle des GAFAM. Si on ajoute à cette situation le fait que le potentiel économique des GAFAM leur donne la capacité de désorganiser le marché en leur faveur, il est important que l'État du Sénégal prenne des initiatives propres à porter le débat sur cette problématique au niveau de l'UA. Cela permettra de résoudre deux séries de problèmes : la position dominante des GAFAM et le contrôle de leurs activités de collecte de données personnelles dans le cadre de l'économie de la donnée et de l'intelligence artificielle.

Dans un tel contexte de développement de la culture et des usages numériques, le gouvernement du Sénégal, en étroite concertation avec les différentes parties prenantes devrait adapter le cadre juridique sénégalais en vue de tirer le meilleur parti du secteur de la donnée et de la donnée personnel. A ce titre, six (6) principales préconisations pourraient permettre de remédier aux insuffisances notées. Ces recommandations invitent :

1) Repenser le phénomène :

a. *Concevoir la donnée personnelle en tant que composante de la donnée* : À ce jour, le Sénégal ne dispose pas de cadre juridique de régulation des données en général. Cela constitue, dans une certaine mesure, un facteur d'insécurité juridique pour les entreprises du secteur de l'économie de la donnée, en particulier les start-up désireux d'investir dans ce domaine ;

b. *Procéder à une typologie opératoire des données (données essentielles, données critiques, données de souveraineté)* : Cela constitue la suite logique de l'élargissement du champ de compréhension du phénomène. En saisissant la donnée personnelle comme sous-ensemble de la donnée, il est possible de catégoriser les données suivant leur nature et les enjeux qui s'y rattachent ;

c. *Analyser la donnée comme enjeu de souveraineté* : L'absence de cadre juridique de la donnée réduit le champ de la maîtrise des enjeux liés à l'économie de la donnée. Le Gouvernement, en dehors de la LDP, ne dispose pas d'un cadre clair des données cri-

tiques ou essentielles, ce qui ne permet pas de mettre en place des critères de mesure du niveau de résilience.

d. *Intégrer la cybersécurité dans la régulation de la donnée* : Le futur cadre juridique de la cybersécurité devrait être mis en corrélation avec le droit de la donnée et des données personnelles.

2) Repenser les usages :

a. *Garantir la sécurité individuelle et collective (infrastructures de données, données essentielles)* : il s'agit de mettre en avant la sécurité technique et juridique des données et ainsi permettre de maitriser les risques conformément à la recommandation 1. d°) ;

b. *Passer de l'économie numérique à l'économie de la donnée* : C'est le prolongement de la préconisation 1. a°). Cela permet de mettre en place deux régimes distinct de régulation en fonction de la nature de la donnée ;

c. *Réguler l'économie des métadonnées, de l'intelligence artificielle et de l'Internet des objets* : Il s'agit d'intégrer à la réforme du cadre juridique des données personnelles et/ou de la donnée, les réflexions actuelles en cours au Sénégal ou dans le monde, notamment sur l'IA, les drones civiles et les pratiques médicales comportant le recours aux technologies et à l'IA. Cela implique, incidemment, de réguler le big data et les objets connectés.

3) Élargir et améliorer la protection normative :

a. *Des droits individuels aux droits collectifs ?* : Le modèle actuel de la protection des données personnelles est basé sur des droits individuels. Pour lutter efficacement contre les violations, il serait plus indiqué de consacrer des droits collectifs ou des droits individuels dont l'exercice est collectif ;

b. *Du consentement formel au consentement réel* : il s'agit de créer les conditions d'un consentement libre et éclairé des personnes dont les données personnelles sont collectées. Il en va ainsi des malades, de leurs ayant droits dont l'épreuve ne permet pas toujours de recueillir un consentement intègre ; du demandeur de crédit (pour les données collectées par les établissements de crédits) ; etc.

4) Améliorer le cadre de régulation institutionnelle en prenant en compte l'Agenda 2063 et la vision 2050 de la CEDEAO :

a. *Mettre en place des cadres formels de coopération intragouvernementale*. La faible articulation des organes stratégiques et/ou de contrôle opérationnel doit être corrigée à travers :

- La création/désignation d'un organe unique de coordination des stratégies globale et sectorielle ;
- La création/la désignation d'une structure unique de coordination des actions opérationnelles (autorités d'enquêtes, de poursuites, de contrôle et de sanction). Cette structure, différente de la CDP, peut être un département ministériel dont les actions de coordination intégrera les mesures d'exécution initiées dans le domaine de la

protection des données personnelles par les régulateurs sectoriels (ARTP, CNRA), la CDP et les autorités de la chaîne pénale ;

b. *Promouvoir la coopération intersectorielle* : Dans la suite de la recommandation 4. a°) ci-dessus, il s'agit de faciliter le partage d'informations et d'expériences, ainsi que les actions concertées entre tous les acteurs intervenant en matière de protection des données à caractère personnel ;

5) Mettre en place un index de sécurité technique et de protection juridique des données personnelles :

a. *Indicateur de sécurité des infrastructures essentielles* : Cet indicateur mesure le niveau de sécurité des installations physiques ou électroniques de communication ou de stockage et des données. Les normes de l'Union internationale des télécommunications (UIT) en matière de cybersécurité peut servir de modèle à l'élaboration de cet indicateur ;

b. *Indicateur de sécurité des données critiques* : Il s'appliquera aux données essentielles et/ou de souveraineté et permettra de mettre en œuvre des actions correctives lorsqu'une menace est détectée. Là encore, le guide de l'UIT sur la cybersécurité peut utilement être mis à profit pour la définition des indicateurs et de seuils de résilience ;

c. Index de sécurité juridique des droits individuels et collectifs. Cet index vise à mesurer :
   - le niveau de prise en charge, au plan juridique des risques individuels et collectifs liées aux données personnelles ;
   - l'exhaustivité des droits reconnus au regard des risques encourus ;
   - le taux d'effectivité des droits consacrés ;

d. Indicateur de performance des organes de contrôle et de sanction : Il permet d'apprécier les outils d'intervention des acteurs institutionnels (manuel de procédure, stratégie d'information et de communication, instruments, moyens et capacités d'investigation, etc.).

NB : Les différents indicateurs doivent être mesurables afin de pouvoir servir d'outils de comparaison entre systèmes nationaux ou sectoriels de protection des données personnelles.

6) Allouer des moyens suffisants :

a. *Renforcer les capacités des ressources humaines* : Cette exigence est le premier gage de performance du cadre institutionnel de gouvernance et de régulation des données personnelles. Avec les développements techniques en cours et les applications en perspectives, le capital humain devient l'écosystème-support complémentaire. L'allocation optimale de ressources humaines permet de réussir la prévention des menaces sur les infrastructures et données critiques, de renforcer la résilience et assurer la mise en œuvre optimale du cadre juridique ;

b. *Développer des curricula et former aux problématiques de la donnée et des données personnelles* : il s'agit de concevoir deux schémas de formation. Les formations initiales et les formations professionnelles (académiques ou à la carte). Cela permet d'atteindre l'objectif visé par la recommandation 6.a°) ci-dessus.

VI. ANNEXES

ProDP Africa

Renforcer la protection des données personnelles en Afrique : vers un système harmonisé et efficient

- - -

Rapport Sénégal

Questionnaire d'état des lieux

Cher contributeur,

Le Laboratoire d'analyse des sociétés et pouvoirs – Afrique/Diaspora (LASPAD) de l'Université Gaston Berger (UGB) de Saint-Louis, Sénégal, dans le cadre du projet de recherches sur la protection des données personnelles en Afrique (ProDP Africa), entend contribuer au renforcement de la connaissance et des compétences sur les données personnelles en Afrique.

A cette fin, il est prévu de procéder à un état des lieux à travers l'administration du présent questionnaire aux différentes parties prenantes de l'écosystème des données personnelles au Sénégal. L'objectif poursuivi est de permettre de :

- dresser une cartographie des acteurs de l'écosystème des données personnelles ;
- connaitre l'état actuel de l'économie autour des données personnelles ;
- comprendre les perceptions des parties prenantes sur les problématiques liées aux données personnelles ;
- analyser les cadres juridique et institutionnel des données personnelles.

La mission se propose, dans le contexte de l'émergence de technologies nouvelles telles que l'Internet des objets (IdO), la blockchain ou chaînes de blocs, l'intelligence artificielle, l'impression en 3D, l'avènement des plateformes, les données massives… de contribuer à une meilleure compréhension des enjeux autour des données personnelles. Le présent questionnaire aidera ainsi à définir des recommandations pour une meilleure prise en charge des problématiques liées aux données personnelles.

Le questionnaire est administré par les experts du LASPAD aux différentes parties prenantes identifiées par le coordonnateur de la mission.

Informations sur l'entretien

Date de l'entretien

Cliquez ou appuyez ici pour entrer du texte.

Lieu de l'entretien

Cliquez ou appuyez ici pour entrer du texte.

Nom de la personne interrogée

Cliquez ou appuyez ici pour entrer du texte.

Fonction

Cliquez ou appuyez ici pour entrer du texte.

Structure / organisation

Cliquez ou appuyez ici pour entrer du texte.

Secteur / Domaine d'activité

Cliquez ou appuyez ici pour entrer du texte.

Adresse postale

Cliquez ou appuyez ici pour entrer du texte.

Adresse électronique

Cliquez ou appuyez ici pour entrer du texte.

Numéro de téléphone

Cliquez ou appuyez ici pour entrer du texte.

Informations supplémentaires (i.e. site internet)

1. Le phénomène

1. Qu'est-ce qu'une donnée personnelle ?

Cliquez ou appuyez ici pour entrer du texte.

2. Comment avez-vous entendu parler de la notion de données personnelles pour la première fois ?

Cliquez ou appuyez ici pour entrer du texte.

3. Quelles sont les différentes catégories de données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

4. Qu'est-ce qu'une donnée sensible ?

Cliquez ou appuyez ici pour entrer du texte.

5. A quoi sert une donnée personnelle ?

Cliquez ou appuyez ici pour entrer du texte.

6. Les données personnelles sont-elles protégées au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

7. La protection des données personnelles est-elle suffisamment assurée au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

8. Où sont stockées les données personnelles des usagers sénégalais ou résidant au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

9. Jusqu'où s'étend la liberté pour une personne de disposer de ses propres données personnelles au Sénégal ? (Exclusion de tous traitements obligatoires)

Cliquez ou appuyez ici pour entrer du texte.

10. Quels sont les registres de l'État existant au Sénégal qui contiennent des données personnelles ? (Exemples : état civil, CNI, Passeport, Permis de conduire, casier judiciaire, carte grise, RCCM, CMU, liste électorale, etc.)

Cliquez ou appuyez ici pour entrer du texte.

11. Selon vous, les registres de l'État existant au Sénégal sont-ils conformes à la réglementation sur les données personnelles ? (exemples : état civil, CNI, passeport, permis de conduire, casier judiciaire, carte grise, RCCM, CMU, etc.)

Cliquez ou appuyez ici pour entrer du texte.

12. Quels registres existant au niveau régional comprennent des données personnelles ? (Exemples : CEDEAO – CNI, passeports - ; UEMOA – BIC, CIP - ; OHADA – FRCCM, etc.)

Cliquez ou appuyez ici pour entrer du texte.

13. Les registres existant au niveau régional sont-ils en conformité avec la réglementation sur les données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

2. Les acteurs

1. Qui collecte les données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

2. Qui stocke les données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

3. Qui traite les données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

4. Qui définit les politiques et stratégies sur la protection des données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

5. A votre avis, quelles sont les possibles atteintes aux données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

6. A qui doit-on s'adresser lorsqu'on subit une atteinte aux droits protégeant les données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

7. Qui intervient dans l'élaboration des lois protégeant les données personnelles au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

8. Qui finance les études, missions, activités destinées à l'élaboration des textes protégeant les données personnelles au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

9. Qui traite des cas de violation des données personnelles au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

3. Perceptions et usages des données personnelles

a. Politique et démocratie

1. En quoi les données personnelles pourraient-elles influencer la démocratie au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

2. Quel impact les données personnelles peuvent-elles avoir sur les élections au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

3. Comment les données personnelles sont utilisées dans le processus électoral au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

4. Les partis politiques peuvent-ils utiliser les données personnelles des militants / des électeurs pour les contacter dans le cadre de leurs campagnes électorales (sms, mailing, téléphone…) ?

Cliquez ou appuyez ici pour entrer du texte.

5. Comment les données personnelles peuvent-elles affecter la souveraineté du Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

b. Économie et finances

6. Comment peut-on gagner de l'argent avec des données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

7. Avez-vous connaissance, au Sénégal, de structures ou organisations qui achètent des données personnelles ? Selon vous, ont-elles le droit ? A quelle (s) fin (s) le font-elles ?

Cliquez ou appuyez ici pour entrer du texte.

8. Connaissez-vous, au Sénégal, des structures ou organisations qui vendent des données personnelles ? A votre avis, pourquoi font-elles cela ? En ont-elles le droit ?

Cliquez ou appuyez ici pour entrer du texte.

9. A votre avis, quels cadres juridique et institutionnel mettre en place pour permettre une exploitation économique optimale des données personnelles au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

c. Social et culturel

1. Selon vous, quels sont les dangers/risques aux plans social et culturel liés aux usages de vos données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

2. Selon vous, quels sont les risques encourus dans l'utilisation des données personnelles d'autrui ?

Cliquez ou appuyez ici pour entrer du texte.

3. A votre avis, quelles données sont les plus sensibles (d'une manière générale ou en ce qui concerne ses propres données ?) ?

Cliquez ou appuyez ici pour entrer du texte.

4. A l'occasion de quel (s) usage (s) pensez-vous que vos (les) données sont les plus exposées ?

Cliquez ou appuyez ici pour entrer du texte.

d. Technologie

1. Quelles sont les technologies utilisées pour la collecte, le traitement, le stockage, etc. des données personnelles (IA, IdO, Big Data etc…) ?

Cliquez ou appuyez ici pour entrer du texte.

1. Quelles sont les infrastructures de stockage (Data Center ou autres) qui existent au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

2. L'utilisation des données personnelles dans le cadre des réseaux sociaux vous semble-t-elle conforme à la loi ? Justifiez votre réponse

Cliquez ou appuyez ici pour entrer du texte.

3. Si non, l'utilisation des données personnelles dans le cadre des réseaux sociaux doit-elle faire l'objet d'un encadrement juridique spécifique ? Justifiez votre réponse

Cliquez ou appuyez ici pour entrer du texte.

4. Sur quoi devrait porter un encadrement juridique de l'utilisation des données personnelles dans le cadre des réseaux sociaux ?

Cliquez ou appuyez ici pour entrer du texte.

4. Cadre de gouvernance des données personnelles

1. Quel est le rôle du gouvernement du Sénégal en matière de données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

2. Quels sont les pouvoirs du gouvernement du Sénégal en matière de protection des données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

3. Quelle structure/autorité au sein du gouvernement du Sénégal élabore les politiques/stratégies de protection des données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

4. Quelle structure/autorité au sein du gouvernement du Sénégal assure la tutelle/le contrôle des organes en charge de la protection des données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

5. Quelle est la place des institutions régionales et sous régionales en matière de protection des données personnelles au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

6. Avez-vous une idée des relations entre le gouvernement et les autres institutions publiques en matière de protection de données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

7. Connaissez-vous d'autres organismes régionaux et internationaux intervenant dans la gouvernance en matière de protection des données personnelles ? Comment leur action est-elle articulée avec celle des institutions nationales de gouvernance, le cas échéant ?

Cliquez ou appuyez ici pour entrer du texte.

5. Cadre de régulation des données personnelles

a. Textes de base

1. Quels textes (loi, décret, arrêté, circulaire, convention, etc.) nationaux organisent la protection des données personnelles au Sénégal ?

Cliquez ou appuyez ici pour entrer du texte.

2. Quels textes (Acte additionnel, Règlement, Directive, Acte uniforme, Décision, Convention etc.) organisent, au niveau régional (échelles UA, CEDEAO, OHADA, UEMOA…) la protection des données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

3. Quelle (s) est (sont) (les) l'autorité(s) spécialement chargée(s) de protéger les données personnelles à l'échelle nationale/régionale ?

Cliquez ou appuyez ici pour entrer du texte.

4. De quels moyens matériels, financiers, technologiques et humains dispose cette (ces) autorité(s) pour la protection des données personnelles ? Est-ce suffisant ?

Cliquez ou appuyez ici pour entrer du texte.

5. Quels sont les pouvoirs de cette autorité pour la protection des données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

6. Quelles autres instituions peuvent être impliquées dans la régulation des données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

7. Quelles relations ces autres institutions ont-elles avec l'autorité chargée de la régulation de la protection des données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

b. Objets de la régulation

Cliquez ou appuyez ici pour entrer du texte.

1. Les algorithmes sont-ils encadrés/régulés ?

Cliquez ou appuyez ici pour entrer du texte.

2. Quelles données/usages/personnes sont concerné(e)s par la régulation/protection des données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

c. Effectivité des droits

3. Avez-vous une idée des droits individuels reconnus aux individus quant à l'utilisation et au traitement de leurs données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

4. Connaissez-vous les voies de droit ou les moyens d'action dont disposent les individus pour agir et protéger leurs données personnelles ?

Cliquez ou appuyez ici pour entrer du texte.

5. Avez-vous une idée du nombre de plaintes que l'autorité de protection des données personnelles reçoit chaque année ?

Cliquez ou appuyez ici pour entrer du texte.

6. Selon sous, quelles sanctions peuvent être prononcées par l'autorité de protection des données personnelles en cas de violation des droits des usagers ?

Cliquez ou appuyez ici pour entrer du texte.

7. Les sanctions prononcées par l'autorité de protection des données personnelles en cas de violation des droits des usagers sont-elles appliquées effectivement ?

Cliquez ou appuyez ici pour entrer du texte.

8. Quels sont les mécanismes juridiques qui permettent de s'assurer de cette effectivité ?

Cliquez ou appuyez ici pour entrer du texte.

6. Considérations diverses

Quels sont les autres besoins en matière de protection des données ?

Cliquez ou appuyez ici pour entrer du texte.

ANNEXE 2 : LISTE DES PERSONNES INTERROGEES

Organisation	**Centres d'intérêts et actions de l'organisation**	**Adresse de l'organisation**
CDP : Autorité Administrative Indépendante	Régulation et protection des données personnelles	PG6G+7R3, 70 Rue MZ 72, Dakar
Enseignant-chercheur, Expert CDP	Régulation et protection des données personnelles	
Consultant au consortium CARAPACES Stratégies & Conformité	Ingénierie des réformes normatives et institutionnelles, cyberstratégie, légistique, prospective juridique.	carapaces@carapaces.net - www.carapaces.net
ONG 3D	Droits humains, développement local, démocratie, gouvernance	Comico Mermoz, Dakar, Sénégal. 33 825 69 69/ https://ong3d.org
Association Africtivistes	Blog, web-journalisme, web-activisme, démocratie, droits humains, bonne gouvernance. Projets numériques, sécurité informatique, open data, solution médias, citoyenneté numérique	BP 19968 Dakar , Cité Sofraco , VDN 3 prolongée. (+221) 33 837 51 24 https://www.africtivistes.com
ONG Amnesty International	Droits humains	Secrétariat national Amnesty International Sénégal, 8412, Sacré-Cœur 1 ; BP 35269, Dakar Colobane. https://www.amnesty.sn
Association Article 19	Promotion et défense de la liberté d'expression, droits numériques et protection des données personnelles.	P O Box 5175 Dakar, Fann; senegal@article19.org; westafrica@article19.org; https://article19ao.org;
Association des juristes sénégalaises (AJS)	Droit, conseils et orientations juridiques et judiciaires	Cité Sonatel, en face de SAMU Municipale de Grand-Yoff, BP 2080 Dakar RP. https://femmesjuristes.org/?page_id=438
ONG Forum civil (Section Sénégalaise de Transparency International)	Lutte contre la corruption et promotion de la bonne gouvernance	40, avenue El Hadj Malick Sy, Immeuble "LA LINGUERE", au 1er Étage, Dakar.
Association Internet sans frontières	Promotion et protection des droits numériques	

Association Jonction	Droits humains, promotion de la cybersécurité, protection des données personnelles, lutte contre la cybercriminalité	Grand-Médine Villa n° 512 BP 4126 Dakar - Sénégal http://jonctionsenegal.free.fr http://jonction.e-monsite.com
ONG OSIWA	▪ Réforme de la justice et de l'état de droit ; ▪ Égalité et lutte contre la discrimination ; ▪ Pratique démocratique ; ▪ Gouvernance et avancement économique.	Stèle Mermoz, Rue El Hadj Ibrahima Niass, BP 008 Dakar-Fann ; www.osiwa.org
Association Polaris Asso	Autonomisation des jeunes dans l'espace numérique, éducation aux données personnelles, *policy brief*	Boulangerie Jaune, Sacré Cœur 3 Sénégal Dakar, https://polaris-asso.org
ONG Réseau africain pour l'éducation et la santé (RAES)	Développement, éducation de qualité, égalité entre les sexes, bonne santé et bien-être, durabilité des villes et des communautés, paix, justice	
ONG RADDHO	Défense et protection des droits humains.	Sicap Dieupeul 2, Villa 2500, Dakar, Sénégal BP 15246 -Fann Sénégal www.raddho-africa.org
Acteur de l'enseignement supérieur	Nouvelles méthodes cognitives, e-learning, Formations ouvertes et à distance (FOAD)	Route de Ngallèle, Saint-Louis. www.ugb.sn

ANNEXE 3 : TDRS DE L'ATELIER D'ECHANGES AVEC LES ORGANISATIONS DE LA SOCIETE CIVILE INTERVENANT DANS LE DOMAINE DE L'ECONOMIE DE LA DONNEE ET DE LA DONNEE PERSONNELLE

LABORATOIRE D'ANALYSE DES SOCIETES ET POUVOIRS / AFRIQUE - DIASPORAS

ProDP Africa

Renforcer la protection des données personnelles en Afrique : vers un système harmonisé et efficient

Rapport Sénégal

Atelier d'échanges avec les organisations de la société civile intervenant dans le domaine de l'économie de la donnée et de la donnée personnelle

Termes de références

I. CONTEXTE ET JUSTIFICATIONS

Internet des objets, objets connectés, impression 3D, intelligence artificielle, État-plateforme, télé-enseignement, télémédecine, télétravail, vidéo à la demande, *mobile-banking*, paiement électronique, etc. La sémiotique des temps modernes est caractérisée par le spectre envahissant des technologies de l'information et de communication dont le fonctionnement repose essentiellement ou exclusivement sur une infrastructure de données (données informatiques) et/ou une infostructure de données (données sociales, génétiques, biologiques, raciales, politiques, économiques et financières, etc.).

Cette digitalisation sans cesse croissante des sociétés modernes et des activités humaines pose, avec acuité, la problématique de la régulation de l'usage des données en général et des données personnelles en particulier. Une telle nécessité se justifie surtout depuis l'avènement des données massives et de leurs usages variés dans toutes les dimensions de la vie des personnes et des organisations.

Toutes ces transformations sociales qui modifient la civilisation en améliorant la condition humaine, invitent néanmoins à repenser la protection de la personne à l'ère du « Tout numérique » et cela, en raison de plusieurs dangers : atteinte à la vie privée et à la réputation des individus, manipulation, suppression, transfert et traitement illégaux des données, etc.

Même si toutes les données ne sont pas exposées aux mêmes risques et de la même façon, il est évident que les données personnelles présentent une plus grande vulnérabilité. C'est pourquoi, très tôt, les États et les organisations ont entrepris de traiter ces risques en adoptant une série de réponses, parmi lesquels la régulation du traitement des données personnelles.

Au Sénégal, l'amorce de la régulation juridique des données personnelles a commencé, de manière

décisive, en 2008, avec un cadre juridique spécialement dédié à leur protection, à travers l'institution d'un régime clair du traitement de ces données.

Quinze années après l'avènement de ce premier jalon, il apparait opportun d'en faire le bilan afin d'en recenser les mérites à consolider et d'en relever les lacunes à combler.

Pour établir ce bilan, il est important, d'abord, de s'interroger sur le niveau d'appropriation par le citoyen du cadre juridique de protection de la donnée personnelle, ensuite, de mesurer le niveau de dissémination d'une culture de la protection de la donnée personnelle à travers l'examen des curricula scolaires et académiques, avant enfin, d'évaluer le cadre normatif et institutionnel de protection.

Le présent atelier est organisé après l'établissement du projet de Rapport Sénégal. Ce projet de rapport comprend, d'ores et déjà, l'étude des usages et l'analyse du cadre normatif et institutionnel. L'atelier vise donc à partager ces premiers éléments avec les organisations de la société civile intervenant dans le domaine de la donnée en général et de la donnée personnelle en particulier, afin de recueillir leurs avis et suggestions pour la rédaction du rapport final.

II. OBJECTIFS

L'objectif de l'atelier est, d'une part, d'identifier de manière claire et précise les acteurs de la société civile qui s'intéressent à la problématique des données en général et/ou des données personnelles en particulier.

L'atelier vise surtout à recueillir les avis des organisations de la société civile, en vue de leur prise en charge dans le rapport.

III. RÉSULTATS ATTENDUS

Au terme de cet atelier :

- Les organisations intéressées à la problématique de la donnée en général et de la donnée personnelle en particulier sont connues ;
- Une cartographie des organisations de la société civile actives dans le domaine de la donnée en général et/ou de la protection des données personnelles est établie ;
- Les avis et suggestions des organisations de la société civile sur le projet de rapport sont recueillis ;
- Le rapport intègre, le cas échéant, les suggestions et recommandations faites par les organisations de la société civile.

IV. THÉMATIQUE DE L'ATELIER

L'atelier se déroulera autour de quatre thématiques transversales et transdisciplinaires et d'une thématique conclusive, à savoir :

Thématique 1 : La connaissance des données à caractère personnel : il s'agit de s'interroger sur ce qu'est une donnée personnelle suivant la perspective à partir de laquelle on l'envisage.

Thématique 2 : La perception des usages liés aux données à caractère personnel

Cette thématique vise à répertorier les diverses possibilités offertes par les données personnelles en fonction de la dimension/du secteur envisagé (e).

Thématique 3 : La Cartographie des acteurs

C'est le lieu de recenser les différentes catégories d'acteurs impliqués dans le champ de la donnée personnelle.

Thématique 4 : L'encadrement juridique des données à caractère personnel

Cette section fait, d'abord, le bilan des normes règlementant les usages liées aux données personnelles. Elle aborde ensuite le cadre institutionnel de régulation des données personnelles.

Thématique 5 : Les recommandations pour une régulation efficiente des données à caractère personnel

Cette étape fait le point sur les recommandations fortes établies à partir des insuffisances relevées. Elle propose, le cas échéant, des mesures de remédiation ou d'accompagnement.

V. MÉTHODOLOGIE

L'atelier se déroule comme suit :

- Présentation de chaque thématique, suivie d'échanges ;
- Synthèse des débats par le modérateur thématique ;
- Rédaction et présentation de la synthèse générale de l'atelier.

ANNEXE 4 : CARTOGRAPHIE DES ACTEURS DE LA SOCIETE CIVILE INTERVENANT, SPECIALEMENT OU INCIDEMMENT DANS LE DOMAINE DES DONNEES PERSONNELLES ET AYANT PRIS PART A L'ATELIER DE PARTAGE DES RESULTATS PROVISOIRES DE L'ETUDE

Catégories	Acteurs	Centres d'intérêts	Liens pertinents avec les données personnelles
Droits humains	Amnesty International	Droits humains	▪ Collecte et traitement de données personnelles ; ▪ Lutte contre la collecte et le traitement illicites ou non conformes des données personnelles.
	Jonction	Droits humains, cybersécurité, cybercriminalité, données personnelles	▪ Collecte et traitement de données personnelles en rapport avec le champ d'intervention (droit humains) ▪ Lutte contre la collecte et le traitement illicites ou non conformes des données personnelles, lutte contre la cybercriminalité et promotion de la cybersécurité.
	RADDHO	Droits humains	▪ Promotion d'une perception des droits humains dans l'environnement numérique ; ▪ Collecte et traitement de données personnelles ; ▪ Lutte contre la collecte et le traitement illicites ou non conformes des données personnelles.
Justice, égalité, gouvernance	3D	Droits humains, développement local, démocratie, gouvernance	▪ Collecte et traitement de données personnelles et **sensibles** ; ▪ Lutte contre la collecte et le traitement illicites ou non conformes des données personnelles.
	AJS	Droit, conseils et orientations juridiques et judiciaires	▪ Collecte et traitement de données personnelles et **sensibles.**
	Amnesty International	Droits humains, justice	▪ Collecte et traitement de données personnelles **sensibles** ; ▪ Lutte contre la collecte et le traitement illicites ou non conformes des données personnelles.
	Forum civil	Lutte contre la corruption et promotion de la bonne gouvernance	▪ Collecte et traitement de données personnelles ;
	OSIWA	▪ Réforme de la justice et de l'état de droit ; ▪ Égalité et lutte contre la discrimination ; ▪ Pratique démocratique ; ▪ Gouvernance et	▪ Financement de la recherche sur les données personnelles ; ▪ Plaidoyer pour une meilleure compréhension et protection des données personnelles.

		avancement économique.	
Liberté d'expression, presse et communication	Article 19	Liberté d'expression et de presse	▪ Lutte contre le cyberharcèlement des professionnels de la presse.
Sensibilisation/ éducation	Africtivistes	Formation et sensibilisation aux usages, aux risques et aux droits numériques	▪ Lutte contre la collecte et le traitement illicites de données personnelles ; ▪ Capacitation en mesures de prévention du traçage informatique.
	Internet sans frontières	Formation et sensibilisation aux usages, aux risques et aux droits numériques	▪ Protection des droits numériques ; ▪ Sécurité des communications.
	Polaris	Formation et sensibilisation aux usages, aux risques et aux droits numériques	▪ Protection des droits numériques ; ▪ Sécurité des communications ; ▪ Sensibilisation à la prévention des risques dans l'environnement numérique.
	Réseau africain pour l'éducation et la santé (RAES)	Formation et sensibilisation aux usages et aux droits numériques	▪ Formation et sensibilisation aux usages et aux droits numériques
	Université Gaston Berger de Saint-Louis	Nouvelles méthodes cognitives, e-learning, formations ouvertes et à distance (FOAD)	▪ Les mesures de prévention des atteintes aux droits numériques dans les méthodes didactiques en ligne

ANNEXE 5 : BILAN DES ACTIVITES DE LA CDP DE JANVIER 2014 A SEPTEMBRE 2022.

Autorisations et récépissés de déclarations délivrés

Année	Premier trimestre		Deuxième trimestre		Troisième trimestre		Quatrième tri-mestre		Total
2022	Autorisations	12	Autorisations	16	Autorisations	17	Autorisations	-	45
	Déclarations	64	Déclarations	34	Déclarations	38	Déclarations	-	136
2021	Autorisations	12	Autorisations	18	Autorisations	13[45]	Autorisations	19[46]	62
	Déclarations	33	Déclarations	55	Déclarations	30	Déclarations	116	234
2020	Autorisations	17[47]	Autorisations	09[48]	Autorisations	12[49]	Autorisations	16	54
	Déclarations	27[50]	Déclarations	18	Déclarations	54	Déclarations	89[51]	188
2019	Autorisations	13	Autorisations	18[52]	Autorisations	14	Autorisations	10	55
	Déclarations	15[53]	Déclarations	45	Déclarations	22	Déclarations	20[54]	102
2018	Autorisations	17[55]	Autorisations	13	Autorisations	16	Autorisations	10	56

[45] Refus d'autorisation opposé à SENAS – AUCHAN RETAIL SENEGAL pour :
- consentement recueilli de façon non libre, avec des cases pré-cochées sur le formulaire d'adhésion au programme ;
- durée exacte de conservation des données non définie dans les conditions générales d'utilisation ;
- mise en œuvre du traitement avant autorisation de la CDP.

[46] En plus de ces 19 autorisations accordées, il faut signaler que la CDP a décidé de sursoir à l'examen de neuf (09) dossiers.

[47] Trois demandes d'autorisations ont été rejetées.

[48] Deux refus d'autorisations opposés à :
- un particulier pour l'insatallation de sa caméra de vidéosurveillance (la caméra filme la voie publique) ;
- au Centre de formation aux métiers portuaires et à la logistiqu e (CFMPL) pour l'insatallation de sa caméra de vidéosurveillance car, les caméras installées dans les salles des formateurs sont susceptibles de filmer les enseignants sur leurs positions de travail de manière permanente. En outre, le sous-traitant n'est pas conforme à la Loi sur la protection des données à caractère personnel.

[49] Au cours de ce troisième trimestre 2020, la CDP a accueilli onze (11) structures venues s'imprégner de la législation sur les données à caractère personnel.

[50] Onze structures ont été appelées à la déclaration de leurs bases de données, à savoir : (1) INTERAKTIVE, (2) PCO PARTNERS, (3) TANASOYA.COM, (4) AFRICA TRANSACTION PROCESSING AND SERVICE SA (ATPS), (5) BANQUE ISLAMIQUE DU SENEGAL (BIS), (6) GLOBALE SÉCURITÉ, (7) IDEAL TRANSIT TRANSPORT, (8) INTELCIA SENEGAL, (9) MEDITERRANEAN SHIPPING COMPANY (MSC), (10) PRESTIGE DECO SAU, (11) UNIVERSAL TECH-NOLOGIE.

[51] la CDP a décidé de sursoir à l'examen de deux (02) dossiers.

[52] 02 refus d'autorisations ont été émis.

[53] Refus d'autorisation opposé à PHILIP MORRIS MANUFACTURING SENEGAL (PMMSN) – MITSHIBUSHI CORPORATION BUREAU DE LIAISON DE DAKAR pour :
- absence d'un professionnel de santé dans le processus de traitement des données de santé des employés de PMMSN.
- absence d'informations sur les destinataires des données à l'étranger.
- non existence d'un engagement de confidentialité

[54] 02 refus d'autorisations ont été émis : AFRICAN PAYMENT GATEWAY (APG) , LA BANQUE OUTARDE S.A pour les motifs suivants :
- collecte disproportionnée de données à caractère personnel ;
- collecte excessive et disproportionnée de données au regard de la finalité du traitement.

	Déclarations	35	Déclarations	23	Déclarations	19[56]	Déclarations	41	118
2017	Autorisations	19	Autorisations	25	Autorisations	06	Autorisations	20	70
	Déclarations	83[57]	Déclarations	39	Déclarations	23	Déclarations	46	191
2016	Autorisations	23	Autorisations	08	Autorisations	12	Autorisations	18	61
	Déclarations	28[58]	Déclarations	28	Déclarations	22[59]	Déclarations	42	120
2015	Autorisations	23	Autorisations	45	Autorisations	39	Autorisations	33	140
	Déclarations	66[60]	Déclarations	89	Déclarations	53	Déclarations	41	249
2014	Autorisations	16	Autorisations	19	Autorisations	20[61]	Autorisations	10	65
	Déclarations	41	Déclarations	55[62]	Déclarations	46	Déclarations	77	219
Totaux									2165

[55] Refus d'autorisation de traitement : 01

[56] Rejet de déclaration de traitement : TERROU –BI

[57] Refus d'autorisation de traitement : SBO CONCEPT

- La numérisation ou de dématérialisation de registres et d'actes d'état civil sont du ressort du Centre national d'état civil (CNEC), à travers le Programme d'appui à la modernisation de l'état civil (PAMEC) ;
- l'existence de risque potentiel pour la sécurité et la confidentialité des registres et actes d'état civil manipulés

[58] 1 refus de délivrance de récépissé de déclaration à ABDXMEDIA pour les motifs suivants :

- la collecte déloyale des données personnelles à partir de recherches d'adresses sur des pages web et réseaux sociaux ;
- l'absence d'information préalable des personnes concernées par la collecte de leurs données personnelles et de la finalité de ladite collecte ;
- l'envoi de courriers électroniques de prospection commerciale en violation des exigences légales en matière de prospection directe.

[59] Refus d'autorisation de traitement :

- GIE Yobalema, transport et commerce en ligne
- BEULEUP ENTREPRISE, société de gardiennage de surveillance et d'escorte

[60] Le premier trimestre de l'année 2015 a été aussi marqué par une nouvelle forme de traitement de données personnelles consistant en la collecte de documents d'identité perdus par des particuliers.

[61] Les 20 autorisations concernent les traitements de données de santé, les systèmes de pointage, de gestion des accès et du temps de présence par biométrie, le transfert des données personnelles vers des pays tiers et la collecte des photographies de rues et de places publiques pour un service de géolocalisation.

[62] Durant ce trimestre, il a été relevé que maints opérations et traitements de données personnelles l'avaient été en violation de la législation. On recense, entre autres, des transferts des données personnelles vers des pays tiers (USA, Suisse, France), des collectes et traitements des données biométriques (voyageurs aux frontières, personnels d'un cabinet d'avocat et d'un établissement d'enseignement), des bases de données d'opérateurs de télécommunications, des formulaires de collecte de données personnelles sur des sites , une mise en œuvre de systèmes de vidéosurveillance, des systèmes de contrôle d'accès à des locaux sécurisés, l'exploitation d'un système de gestion d'un fichier clients et des opérations de prospection directe (SMS indésirables ou SPAM).

Plaintes et signalements

Année	Premier trimestre		Deuxième trimestre		Troisième trimestre		Quatrième tri-mestre		Total
2022	Plaintes	8[63]	Plaintes	5	Plaintes	9	Plaintes	-	22
	Signalements	4	Signalements	4	Signalements	5	Signalements	-	13
2021	Plaintes	7	Plaintes	13	Plaintes	16	Plaintes	11	47
	Signalements	5	Signalements	5	Signalements	4	Signalements	5	19
2020	Plaintes	11	Plaintes	5	Plaintes	24	Plaintes	4	44
	Signalements	3	Signalements	3	Signalements	24[64]	Signalements	4	34
2019	Plaintes	12	Plaintes	5	Plaintes	07	Plaintes	12	36
	Signalements	03	Signalements	5[65]	Signalements	03	Signalements	12	23
2018	Plaintes	05	Plaintes	06	Plaintes	07	Plaintes	10	28
	Signalements	-	Signalements	-	Signalements	-	Signalements	04	04
2017	Plaintes	03	Plaintes	08	Plaintes	06	Plaintes	03	20
	Signalements	-	Signalements	-	Signalements	-	Signalements	-	
2016	Plaintes	01[66]	Plaintes	02	Plaintes	04	Plaintes	06	13
	Signalements	03	Signalements	-	Signalements	-	Signalements	-	03
2015	Plaintes	09	Plaintes	-	Plaintes	-	Plaintes	-	09
	Signalements	-	Signalements	-	Signalements	-	Signalements	-	
2014	Plaintes	-	Plaintes	21	Plaintes	-	Plaintes	06	27
	Signalements	-	Signalements	-	Signalements	-	Signalements	10	10
Totaux									352

Sanctions

[63] A ces 12 plaintes et signalements, il convient d'ajouter la petition introduite auprès de la CDP par M. Emmanuel Diokh, Monsieur Mouhamed Bocoum et cinquante-deux (52) autres signataires, en vue de contester la licéité des prospections politiques dans le cadre des élections locales du 23 janvier 2022. La CDP a pris acte de la pétition mais a toutefois informé les initaiateurs que les canaux légaux prévus par la loi sont la plainte et le signalement.

[64] Les plaintes sont relatives aux collectes frauduleuses de données personnelles, aux publications ou menaces de publication de photos ou de vidéos intimes de citoyens, à des fins de cyberchantage et d'extorsion de fonds.

[65] Les mis en cause dans ces plaintes étaient :

- Fédération des Crédit mutuel du Sénégal (CMS) ;
- M. J.M.M.R.

[66] Le mise en cause avait publié une photo sur facebook sans le consentement du requérant.

Année	Premier trimestre	Deuxième trimestre	Troisième trimestre	Quatrième trimestre	Total
2022	-	-	(1) Deux mises en demeure adressées à : ▪ SONATEL pour manquements liés à la prospection commerciale, effectuée par automate d'appel ; ▪ Société d'exploitation du train express régional de Dakar (SETER), pour mise en œuvre irrégulière d'un système de géolocalisation sur les véhicules de fonctions du personnel et pour défaut de consentement préalable des personnes dont les données sont collectées. (2) Un avertissement servi à Monsieur Lat Diop, homme politique, pour prospection directe à caractère politique non sollicitée.	-	**03**
2021	-	-	-	Mise en demeure **de la société Groupe Fauzie Layousse** d'avoir à se conformer à la règlementation quant à l'installation d'un système de vidéosurveillance et d'un système de pointage biométrique dans les locaux de l'entreprise. **Injonction de la CDP à la société MHI Equipement Services Africa (MESA)** d'avoir à se conformer aux procédures légales en matière de vidéosurveillance et de pointage biométrique dans les locaux de l'entreprise.	**02**

2020	-				
2019				Mise en demeure du **Groupe SENTEL GSM** pour non-respect du droit d'opposition et du créneau horaire d'envoi des SMS de prospection directe ; - affiches d'information de la présence des caméras de surveillance non-conformes à la délibération n°2016-00238/CDP du 11 novembre 2016, portant sur les règles d'installation et d'exploitation d'un système de vidéosurveillance dans les lieux de travail - traitement de données de santé des travailleurs non autorisé ; - absence d'une politique de protection des données personnelles.	**02**
2018					
2017				Mise en demeure de : 1) **Expresso Sénégal (opérateur de télécommunications)** pour : ▪ absence de conformité des termes et conditions d'utilisation du site Web www.expressotelecom.sn ; ▪ inobservation de certaines règles liées à la prospection directe ; ▪ absence d'une durée claire de conservation des données des demandeurs d'emploi. 2) **CBAO Groupe Attijariwafa Bank** avec les conclusions suivantes : ▪ la durée de conservation de certaines données n'est pas explicite ; ▪ il existe des accès non autorisé à des données ; ▪ il y a usage de quatre PC sous XP.	**02**

2016					
2015		La CDP a servi un avertissement à l'endroit d'une structure pour envoi répété de courriels et de SMS non sollicités sans mise à disposition d'une possibilité de désabonnement fonctionnel.	La CDP a prononcé deux avertissements pour pratique illégale et répétée de la prospection commerciale directe.	Mise en demeure d'une société pour atteinte à la vie privée des salariés à la suite de l'installation irrégulière d'un logiciel d'espionnage sur les ordinateurs de travail.	**03**
2014		Deux (02) délibérations portant mise en demeure pour manquement à la législation sur les données personnelles ;			**01**
Totaux					**13**

Missions de contrôle sur sites

Année	Premier trimestre	Deuxième trimestre	Troisième trimestre	Quatrième trimestre	Total
2022	-	(1) Mission de contrôle sur site (à blanc) de l'entreprise Endeavour Mining (Sabadola) en vue de juger de la conformité de l'installation des caméras de surveillance de l'entreprise. L'entreprise Endeavour Mining souhaitait être évaluée et accompagnée, avant le dépôt de son dossier auprès de la CDP ; (2) Soutien à la conformité aux structures suivantes : ▪ Fly Air Sénégal ; ▪ MCA Senegal (Mille-	6 contrôles sur sites effectués chez un particulier et auprès des entreprises suivantes : ▪ Brioche Dorée ; ▪ Total Énergies ; ▪ Pullman Dakar Téranga ; ▪ SONATEL ; ▪ SETER.		**14**

		nium Challenge Account) ; ▪ ANSD ; ▪ Ministère de l'Urbanisme, du Logement et de l'Hygiène publique (MULHP) ; ▪ Lengo ; ▪ AZA Finances ; ▪ Haut-Commissariat des Nations unis pour les réfugiés (UNHCR).			
2021	Note Technique sur la mise à jour de la politique de confidentialité de WhatsApp adressée à Facebook Africa	-	4 contrôles : Mhi Equipment Services Africa (Mesa), Groupe Faouzie Layousse, Cactus Technology, Field Force Consulting (2F Consulting).	6 missions de contrôle : (1) Philip Morris Manufacturing Sénégal, (2) Pan Africa Entrepreneur Services Sarl (PAES), (3) Banque Atlantique Sénégal, (4) Sesam Informatics, (5) Spherex SA, (6) Dakaroise des Jeux	**10**
2020	-				
2019				(1) Mission de contrôle du 17 juillet 2019 effectuée au complexe TERROU-BI en vue de vérifier la conformité du système de vidéo-surveillance ainsi que du traitement portant sur le fichier du personnel. Ces vérifications ont permis de constater les manquements suivants : ▪ Le non-respect des formalités préalables auprès de la CDP pour les traitements relatifs au système de vidéo-surveillance et au fichier du personnel ; ▪ Les modalités d'exercice des	**02**

				droits des personnes ne sont pas formalisées ; ▪ Le nombre insuffisant de panneaux d'informations renseignant de l'existence du système de vidéosurveillance. (2) Mission de contrôle du 05 septembre 2019 effectuée auprès de SENTEL GSM	
2018	Mission de contrôle effectué au niveau de 2 structures : (1) La Poste par rapport au traitement relatif aux données des clients ; (2) AMERGER CASAMANCE par rapport au système de vidéosurveillance.				**02**
2017				Deux Missions de contrôle auprès de deux structures : **1.CBAO** **La mission a conclu que :** ▪ la durée de conservation de certaines données n'était pas explicite ; ▪ l'accès non autorisé aux données ; ▪ la présence et l'utilisation de quatre **2. Expresso Télécoms Sénégal** **Les conclusions révèlent:** ▪ la non-conformité	**02**

				des termes et conditions du site Web ; ▪ le non-respect des conditions de la prospection directe ; ▪ l'absence d'une durée claire de conservation des données des demandeurs d'emploi.	
2016				Mission de contrôle sur place de la CDP auprès de la MTOA ayant révélé que le système de vidéosurveillance déployé est conforme à la législation sur la protection des données personnelles. Mission de contrôle sur site le 15 décembre 2016 à la Société de conserverie en Afrique (SCA Sa). Procès-verbal et observations des contrôleurs à présenter aux commissaires.	**02**
2015				NEANT	
2014				NEANT	
Totaux					**32**

ProDP AFRICA

www.prodp-africa.com

LABORATOIRE D'ANALYSE DES SOCIETES ET POUVOIRS / AFRIQUE - DIASPORAS

LASPAD - Université Gaston Berger
Route de Ngallèle, BP 234 Saint-Louis, Sénégal
Tel. +221 78 469 39 31- www.laspad.org