RAPPORT INTERMEDIAIRE

MINISTÈRE DE L'ÉCONOMIE NUMÉRIQUE ET DES TÉLÉCOMMUNICATIONS

REVUE DU CADRE JURIDIQUE POUR L'IDENTITE NUMERIQUE NATIONALE

Tableau des modifications

VERSION	REFERENCE	AUTEUR	DATE	OBJET DE LA MODIFICATION
01		GAINDE 2000	30/11/2021	Création du doument

VERIFIE PAR	APPROUVE PAR
Equipe Qualité GAINDE 2000	
Date :	**Date :**

RAPPORT INTERMEDIAIRE REVUE DU CADRE JURIDIQUE

SOMMAIRE

RAPPORT INTERMEDIAIRE REVUE DU CADRE JURIDIQUE

I. INTRODUCTION

Par suite de la sélection du cabinet GAINDE 2000 sur un appel d'offres de l'UNDP (United Nations Développent Programme) pour la réalisation de l'étude de faisabilité du Projet Identité Numérique Nationale (INN), nous avons été sollicités pour participer à l'équipe de projet mis en place pour apporter notre expertise en qualité d'Expert juriste.
Notre mission consiste à définir, pour les besoins de la réalisation du projet, les axes et options éventuels du cadre normatif de l'identité numérique, au regard du diagnostic exhaustif des textes légaux et règlementaires existants.
Sur la base de la feuille de route fournie par GAINDE 2000, nos tâches ont été définies ainsi qu'il suit :

- Faire le diagnostic du cadre juridique existant sur le sujet de l'identité numérique ;
- Procéder à l'analyse et le benchmark des lois existantes dans les autres pays sur le sujet ;
- Identifier les améliorations et amendements à apporter pour la mise en œuvre du projet d'identité numérique ;
- Définir les axes et orientations du cadre juridique et réglementaire cible

Dans le cadre de ce premier livrable, il s'agit de faire le diagnostic des textes légaux et réglementaires sur le sujet de l'identité numérique nationale.

Conformément aux principes et normes de la légistique, nous avons dans le cadre de ce projet qui nécessite l'encadrement juridique de l'identité numérique procédé à une revue globale des principaux textes pouvant impacter ou constituer des obstacles pour légiférer sur la question.

II. METHODOLOGIE DETAILLEE

En raison des différentes options qui existent en la matière et pour les besoins de la pertinence de la démarche et des options futures et pour la cohérence d'un éventuel dispositif législatif ou règlementaire dans le système juridique sénégalais, nous avons procédé à un diagnostic préalable du droit positif sénégalais dont les résultats permettront d'apprécier l'opportunité d'une reforme dans le sens soit d'une modification des textes existants soit pour l'adoption d'un nouveau texte répondant au besoin d'instituer d'organiser et de sécuriser l'identité nationale numérique.

Entretiens avec les parties prenantes

Pour ce faire, nous avons courant les mois de septembre et octobre procédé à divers entretiens avec les parties prenantes du projet sur l'organisation et le fonctionnement de leur structure et de leurs activités notamment sur les aspects juridiques liés à la tenue de fichiers automatisés qu'elles gèrent et sur leur vision sur l'opportunité et les aspects fondamentaux d'une éventuelle règlementation.

Revue documentaire

Nous avons également procédé à une revue documentaire à partir de différentes sources officielles du gouvernement et des institutions de la République pour une vaste collecte de textes permettant d'avoir une vue synoptique de la législation dans le secteur des Technologies de l'Information et de la Communication et dans les domaines connexes du cyber droit. Ces textes ont fait l'objet d'analyse sous le prisme de l'identité des acteurs dont ils régissent les activités pour la mise en exergue d'une éventuelle interaction avec les questions juridiques que soulève l'identité numérique.

Entretien avec des experts

Nous avons par ailleurs eu des entretiens avec les hommes de l'Art du domaine des TIC (ambassadeur ID4 Africa, ingénieur de GAINDE) pour des explicitations de concepts et de technologies pour mieux appréhender les enjeux techniques et opérationnels en relation avec l'encadrement juridique.

Exploitation de la doctrine

Par ailleurs l'exploitation de la doctrine (publications, ouvrages, articles, revues …) sur la question et le benchmark avec la législation d'autres pays cibles (Maurice, Rwanda…Benin) sur l'identité numérique ont permis de garantir une parfaite maitrise du concept pour une bonne approche juridique.

Traitement de La problématique de l'identité numérique

Concevoir une identité numérique suppose au préalable une approche taxinomique permettant de classer la notion dans les catégories juridiques connues. A ce titre, l'identité est avant tout un droit.

L'identité, un droit fondamental

En principe, toute personne a droit à une identité qui la désigne et l'individualise en tant que personne physique, mais également en tant qu'être social rattaché à une famille, une fratrie, une ethnie, une race, un territoire, une nation ou un Etat. Cette identification s'opère sur la base de divers facteurs ou éléments d'individualisation et de rattachement comme la filiation, la date et lieu de naissance, le sexe.

A cette identité sont attachées plusieurs conséquences de droit et des qualités et intérêts juridiquement protégés.

À défaut de cette identification, les personnes concernées sont considérées comme des personnes vivantes non identifiées avec toutes les difficultés à cerner leur personnalité juridique et à leur reconnaitre des droits et les soumettre à des obligations.

En effet, ceux qui ne peuvent pas prouver leur identité, quoiqu'étant des êtres vivants n'ont pas d'existence juridique et sont exclus de fait et de droit du commerce juridique en tant qu'acteurs juridiques sujets de droits et assujettis à des obligations.

Dans le monde actuel notamment dans les pays sous-développés, en situation de post conflit ou bien dans les pays d'immigration, on trouve de nombreuses personnes physiques qui ne parviennent pas à établir officiellement leur identité. Cette situation leur confère un état d'apatridie car perçues comme n'appartenant juridiquement à aucun État, aucune nation, aucune patrie.

Vu sous l'angle de la gouvernance, un État face à cette situation de non identifiabilité d'une partie de ses citoyens ou de sa population se confronte à la fois à des difficultés de programmation et de sécurité.

Sur le plan mondial, chaque année selon l'UNICEF 51 millions d'enfants naissent sans déclaration de leur naissance.

Au Sénégal, malgré l'existence d'un dispositif juridique de déclaration des naissances minutieusement organisé par le Code de la Famille, et la mise en place d'un système d'identification nationale depuis 1962 loi N 1962 – 14 du 20 Février 1962 instituant une Carte nationale d'Identité, l'Etat à l'instar de plusieurs pays du continent reste encore confronté aux défis de l'identification fiable de sa population ;

Apport du numérique dans l'identification

Face à cette situation, la solution numérique semble offrir une réponse au besoin de généralisation, de sécurisation et d'accessibilité de l'identité nationale sous le vocable d'identité numérique nationale (INN).

Le besoin de centralisation des références et des coordonnées des personnes justifie l'idée de la dématérialisation par la numérisation et la digitalisation de la gestion de l'identité nationale des assujettis.

En raison des enjeux qu'elle suscite, la question de l'identification nationale, pose le problème de sa fiabilité, de son accessibilité et de sa durabilité. Autant de questions qui semblent trouver solution dans le cadre de la Société de l'information avec les innovations introduites par les Technologies de l'information et de la communication.

Cette évolution frénétique marquée par la transnationalité de l'espace numérique, et la

rapidité des communications électroniques soumises à des mutations fulgurantes engendrant de nouvelles fonctionnalités, des nouveaux métiers et de nouveaux intervenants exige une adaptation permanente du Droit pour capter et encadrer juridiquement dans la durée, les concepts, les notions, les activités et les relations entre les acteurs. Il en est ainsi de la notion d'identité numérique.

Définition de l'identité numérique

Sur le plan définitionnel, le concept d'identité numérique en l'état de la doctrine, demeure une notion polysémique en raison de ses différentes approches et au regard de ses différents usages.

Une certaine opinion définit l'identité numérique « comme un lien technologique entre une entité réelle (personne, organisme ou entreprise) et des entités virtuelles (sa ou ses représentations numériques).

Cette définition générique qui se fonde sur une approche technique permet d'englober toutes les autres définitions fonctionnelles et processuelles reposant sur l'utilité, l'usage et le but de l'identité ; mais aussi sur la manière dont se construit l'identité. La question se pose de savoir s'il faudra en faire des éléments définitionnels ou non.

En effet, l'on retient que l'identité numérique permet l'identification de l'individu en ligne ainsi que sa mise en relation avec l'ensemble des communautés virtuelles présentes sur le Web. Cette approche fonctionnelle prend en compte l'interaction et sa facilitation que permet l'identité numérique au regard des différents et multiples services qu'elle favorise.

Au regard de son processus d'élaboration, la pratique révèle qu'elle se construit de manière générale aussi bien du fait de la personne concernée, que du fait des autres parties avec qui elle rentre en relation dans le WEB.

Concernant la construction personnelle, elle relève des coordonnées que se donne la personne concernée à partir de ses propres déclarations (identité civile réelle, pseudonyme vraisemblable ou fantaisiste et autres référents volontairement exprimés sans contrainte) en vue de se faire identifier. Ces coordonnées qui permettent d'entrer en contact avec la personne concernée peuvent porter sur des données numériques permettant de l'individualiser et même de la localiser en relation avec le lien technologique (ex : adresse électronique, numéro de téléphone, adresse IP, messagerie instantanée,).

Ces cordonnées volontairement construites peuvent également résulter d'éléments plus constants et fiables, car résultant de certificats qui permettent d'authentifier un utilisateur de manière certaine, unique et sécurisée, pour la transmission ou la réception d'informations numériques ou l'accès à des services.

Concernant l'autre approche qui repose sur la construction de l'identité à partir des relations avec les fournisseurs de services ou avec d'autres utilisateurs ou navigateurs du WEB, elle peut résulter, soit des coordonnées conventionnellement acceptées avec ces partenaires ou fournisseurs de services, soit des informations collectées par tout intéressé sur le WEB à partir des propres déclarations de la personne concernée, de ses opinions et avis émis sur les plateformes, de ses passions déclarées ou manifestées, de ses savoirs partagés (les fora, les blogs, les tutoriels…), de ses relations dans les réseaux, de ses consommations à partir des consultations et achats bref de la perception des autres. On parle d'E-réputation, de cyber-réputation, de web-réputation, de réputation numérique, ou encore de Social Networking. Cette identité est dite subjective.
A partir de cette polysémie qui donne lieu à une pluralité d'identités (identité civile portant sur des référents officiels, d'entité agissante qui trace le profil sur la base des actions sur l'échiquier numérique, Identité déclarative portant sur la propre présentation de soi, Identité virtuelle reposant sur une représentation fictive), il est important dans le cadre d'une approche juridique de définir de manière univoque l'objet de l'étude.

C'est pourquoi, en raison de la volatilité de la définition subjective fondée sur des intérêts ponctuels et une simple perception, l'identité numérique dont est question dans le cadre de ce projet porte sur l'identité objective fondée sur des référents officiels permettant d'individualiser physiquement une personne à partir de données numériques.

En tout état de cause, se pose nécessairement la question de l'encadrement et de la protection de l'identité en tant qu'attribut essentiel de la personne. La question est de savoir s'il faudra protéger l'identité au titre des données personnelles ou lui aménager une protection spéciale.

Sous cet angle partant de la définition de la donnée personnelle comme "*toute information relative à une personne physique identifiée ou identifiable directement ou indirectement par référence à un numéro d'identification ou à un ou plusieurs éléments propres à son identité*", l'on peut retenir que l'identité d'une personne est nécessairement une donnée à caractère personnel dans la mesure où elle permet d'individualiser ou de reconnaître ladite personne. Toute personne a le droit, sauf en cas d'exigence légale, de vivre inconnu, dans son intimité et dans la confidentialité de son jardin secret.

Or, que ce soit un numéro, une image, une signature ou une empreinte, le simple fait que sa singularité puisse permettre soit d'individualiser une personne, soit de rattacher une situation ou un acte donné à une personne, fait de ces références des éléments ou facteurs d'une identification. Par conséquent, cette ou ces références méritent d'être protégées au même titre que les autres éléments d'identité civile de la personne comme son nom, son prénom, son lieu de domicile ou sa filiation.

Cette approche se déduit plus aisément de la définition très simple de la donnée personnelle telle que retenue par le Conseil de l'Europe qui la conçoit comme « toute information concernant une personne physique identifiée ou identifiable » Or, il n'y a pas d'information

plus identifiant que la propre identité d'une personne.

En conséquence, l'on comprend à juste titre l'importance d'encadrer et de protéger l'identité numérique au même titre que l'identité fondamentale contre toute forme de malversations (usurpation, falsification, effacement, blocage etc.).

Pour ce faire, nous tâcherons d'analyser la problématique à la lumière de l'existant à travers la revue des textes régissant au Sénégal le domaine du numérique (2)

III. CADRE JURIDIQUE DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION AU SENEGAL

L'avènement de la Société de l'information a nécessité la prise en charge juridique du nouvel environnement numérique et des nouvelles problématiques engendrées par les échanges et transactions électroniques entre les acteurs de la cyber communauté.
Les textes qui ont été adoptés visent d'une part, la règlementation et la régulation du secteur (2.1) en vue d'assurer son développement et d'autre part, la protection des acteurs, des systèmes et des données circulant entre les intervenants sur les réseaux et les plateformes (2.2).

A. Organisation et réglementation du secteur des TIC

Les textes portant organisation et règlementation des activités du secteur des communications électroniques touchent divers aspects du domaine d'intervention des TIC. Certaines normes sont édictées sur la base de conventions liant les Etats, au plan régional continental ou intercontinental, d'autres normes ont une portée nationale en tant qu'instruments juridiques émanant du Pouvoir législatif ou du Pouvoir exécutif.

B. Sources internationales

La plupart des textes ont pour ancrage l'espace communautaire des organisations économiques sous régionales ; l'Union africaine a pour sa part, adopté un peu plus tard un instrument de portée continentale.

1. Textes communautaires régionaux

Ce sont les textes qui émanent des communautés économiques régionales dont le Sénégal est membre à savoir : la Communauté des Etats de l'Afrique de l'Ouest (CEDEAO) et l'Union Economique et Monétaire Ouest Africaine (UEMOA).

Règlementation des activités des opérateurs et fournisseurs de service : Directive 02/2006/CM/UEMOA du 23 mars 2006 relative à l'harmonisation des régimes applicables aux opérateurs de réseaux et fournisseurs des services :

La directive se fonde sur les dispositions du Traité de l'UEMOA, notamment en ses articles 4, 6, 7, 16, 20 à 23, 25, 26, 42 à 45, 61,91 à 93, 101 et 102 et sur le Protocole additionnel n° II relatif aux politiques sectorielles de l'UEMOA, notamment en ses articles 7 et 8 ainsi que sur la Recommandation n° 03/2000/CM/UEMOA du 22 novembre 2000 relative à la mise en œuvre d'un programme d'actions pour l'amélioration des télécommunications dans l'UEMOA.
Elle a pour objet d'harmoniser les régimes juridiques applicables à l'activité des opérateurs de réseau et fournisseurs de services de télécommunications, de définir des types de régimes identiques pour chaque activité de télécommunications dans les Etats membres de l'Union et

de préciser les conditions et procédures concernant les différents régimes à savoir le régime de l'autorisation, celui de la déclaration et celui du libre exercice.
Il s'agit d'un dispositif auquel les Etats membres sont appelés à se conformer afin d'harmoniser les modalités d'exercice des différentes activités au sein de l'Union. Cependant son application en droit interne n'affecte pas les réglementations spécifiques adoptées par les Etats membres notamment sur le fondement du respect des exigences essentielles et autres exigences d'intérêt public.

Directive n°03/2006/CM/UEMOA du 23 mars 2006 relative à l'interconnexion des réseaux et services de télécommunications :

Cette directive a pour objet de constituer un cadre commun aux Etats de l'UEMOA pour la mise en œuvre de l'interconnexion entre réseaux et d'assurer l'interopérabilité des services de télécommunications.
Selon le législateur communautaire, elle constitue une base de référence commune minimale qui pourra être complétée par les Etats membres par des dispositions règlementaires nationales et par les prescriptions des Autorités nationales de régulation.
Pour promouvoir l'interconnexion des réseaux, le législateur communautaire prévoit que les opérateurs de réseaux de télécommunications ouverts au public sont tenus d'interconnecter leurs réseaux avec les réseaux ouverts au public techniquement compatibles. A cet effet, tout operateur dûment autorisé à établir un réseau public de télécommunications établit une interconnexion entre son réseau et au moins un autre réseau public de télécommunications, afin d'obtenir directement ou indirectement l'accès à l'ensemble des autres réseaux de télécommunications ouverts au public techniquement compatibles.

Harmonisation des politiques et du cadre règlementaire : Acte additionnel A /SA 1/01/07/ du 19 janvier 2007 CEDEAO relatif à l'harmonisation des politiques et du cadre réglementaire du secteur des Technologies de l'Information et de la Communication :

Cet Acte additionnel se réfère aux articles 7, 8, 9 du Traité de la CEDEAO et sur les dispositions de l'article 33 dudit Traité qui engagent les Etats membres, dans le domaine des télécommunications, à développer, moderniser, coordonner et normaliser les réseaux nationaux de télécommunications en vue de permettre une interconnexion fiable entre les Etats membres et de coordonner leurs efforts en vue de mobiliser les ressources financières au niveau national et international par la participation du secteur privé dans la prestation des services de télécommunications.
A cet effet, la décision A/DEC.14/01/05 a été prise aux fins d'adoption d'une politique régionale des télécommunications et du développement du Roaming GSM régional dans les pays membres de la CEDEAO ;
Dans le même sens, la Décision A/DEC.11/12/24 crée un comité technique consultatif de la CEDEAO sur la réglementation en matière de télécommunications ;
Cet Acte additionnel s'inscrit dans le cadre de la politique communautaire de libéralisation des services et infrastructures de Télécommunication et vise à mettre en place un cadre favorable

et attractif à l'investissement avec comme objectif de créer des marchés porteurs au sein de la communauté.
Il a également pour objectif d'instaurer et de promouvoir un cadre harmonisé des politiques des Technologies de l'Information et de la Communication (TIC) dans la sous-région ouest africaine.
Cet Acte additionnel a été adopté sur proposition des Ministres chargés des télécommunications réunis à Abuja, le 11 mai 2006 et sur recommandation des cinquante septièmes sessions du Conseil des Ministres qui s'est tenue à Ouagadougou du 18 au 19 décembre 2006

Réglementation des transactions électroniques : Acte additionnel A/SA.2/01/10 du 16 février 2010 portant transactions électroniques dans l'espace CEDEAO :

Cet Acte additionnel se fonde sur les articles 7, 8 et 9 du Traité révisé de la CEDEAO tel que amendé, et sur l'article 27 du traité relatif à la science et à la technologie ainsi que sur les dispositions des articles 32 et 33 dudit traité relatifs respectivement au domaine des communications et des télécommunications et principalement sur l'acte additionnel A/SA 1/01/07 du 19 janvier 2007 relatif à l'harmonisation des politiques et du cadre réglementaire du secteur des technologies de l'information et de la communication ;
Du point de vue de sa contextualisation, il prend en compte le développement des réseaux de communications électroniques, le nombre croissant des transactions électroniques portant sur la vente, la distribution de produits, la fourniture de services et les échanges par des réseaux.
Il tient également compte des contraintes liées au développement et à la promotion de ces transactions au regard principalement des insuffisances qui affectent la réglementation en matière de reconnaissance juridique des messages électroniques, la reconnaissance de la signature électronique, sous réserve de la réglementation des systèmes de paiement dans l'espace, de l'absence de règles juridiques spécifiques protectrices des consommateurs, de la propriété intellectuelle, des données à caractère personnel et des systèmes d'information, et particulièrement, de l'absence de législation propre aux transactions électroniques.
Le législateur communautaire retient également comme obstacle au développement des transactions les questions liées à l'application des techniques électroniques aux actes commerciaux, aux services et aux actes administratifs, aux éléments probants introduits par les techniques numériques notamment l'horodatage et la certification, aux règles applicables aux moyens et prestations de cryptologie, à l'encadrement de la publicité en ligne, mais aussi à l'absence de la législation fiscale et douanière appropriée au commerce électronique ;
D'où l'adoption de cet Acte additionnel qui vise la mise en place d'un cadre normatif approprié correspondant à l'environnement juridique, culturel, économique et social de la zone ouest africaine et favorable à l'émergence des transactions électroniques fiables dans la sous-région ;

Cet Acte additionnel comporte dans ses dispositions générales des définitions de certaines notions. Au plan de la légistique, il sera important de tenir compte de ces différentes définitions que le législateur communautaire donne à travers ces normes supranationales et qui doivent être conçues comme telles dans les dispositions nationales pour une cohérence d'ensemble du

système juridique communautaire. Plusieurs notions ont été définies comme par exemple, la communication électronique, le courrier électronique, la cryptologie, l'échange de données informatisées, l'écrit, les informations, le message électronique et la signature électronique. La signature électronique par exemple a été définie comme « toute donnée qui résulte de l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. »

Ce texte fait référence à des notions d'identification concernant toute personne qui exerce une activité entrant dans son champ d'application, notamment pour les personnes physiques les nom, prénoms, l'adresse électronique, le numéro de téléphone, l'enregistrement au répertoire des entreprises (le Registre du commerce), le numéro d'identification fiscale, le titre professionnel etc. Il prévoit également en matière de publicité, l'obligation de rendre clairement identifiable la personne physique ou morale pour le compte de laquelle la publicité est réalisée. L'article 11 interdit l'utilisation des coordonnées d'une personne physique qui n'a pas exprimé son consentement préalable à recevoir de prospection directe par le moyen d'un automate d'appel, d'un télécopieur, d'un courrier électronique ou tout autre moyen de communication électronique. L'article 13 fait obligation d'indiquer ses coordonnées valables auxquelles le destinataire de tout envoi des messages par voie électronique à des fins de prospection directe peut s'adresser pour faire cesser la transmission. Il est également interdit par l'article 14 la dissimulation d'identité de la personne pour le compte de laquelle la communication est émise.

2. B-Texte à portée continentale

Convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014

Les États membres de l'Union africaine ont adopté une convention a vocation continentale portant sur diverses problématiques du numérique, à savoir la cyber sécurité, la protection des données à caractère personnel.

Il s'est agi au titre de cette Convention africaine portant adoption d'un cadre juridique sur la cybersécurité et la protection des données à caractère personnel, de faire prendre en charge par les Etats membres de l'Union africaine, des engagements pris tant au plan sous régional, régional, qu'international, en vue de l'édification de la Société de l'Information ;

Elle définit les objectifs et les grandes orientations de la société de l'Information en Afrique et, à renforcer les législations actuelles des États membres et des Communautés Économiques Régionales (CER) en matière de Technologies de l'Information et de la Communication.

Elle rappelle, parallèlement à cette dynamique de digitalisation, l'attachement des États membres aux libertés fondamentales et aux droits de l'homme et des peuples contenus dans les déclarations, conventions et autres instruments adoptés dans le cadre de l'Union Africaine

et de l'Organisation des Nations Unies ;

Ainsi, tient elle compte dans le cadre de la mise en place d'un cadre normatif sur la cybersécurité et la protection des données à caractère personnel, des exigences fondamentales de respect des droits des citoyens, prévues par les instruments nationaux et internationaux relatifs aux droits de l'Homme, particulièrement par la Charte africaine des droits de l'Homme et des Peuples ;

La convention entend mobiliser l'ensemble des acteurs publics et privés (États, collectivités locales, entreprises du secteur privé, organisations de la société civile, médias, institutions de formation et de recherche etc.) en faveur de la cyber sécurité.

Elle pose des règles dites essentielles dans le secteur, en raison du caractère fortement évolutif du domaine technologique, du besoin permanent de réponses juridiques aux attentes des acteurs aux intérêts souvent divergents, et de la nécessité de mettre en place un espace numérique de confiance pour les transactions électroniques, avec une protection adéquate des données à caractère personnel et un dispositif efficace de lutte contre la cybercriminalité ;

Elle place la sécurité au centre du dispositif juridique en tant que facteur d'impulsion de la confiance et de l'adhésion des acteurs. Dans cette dynamique, le législateur communautaire indexe dans son préambule de manière exhaustive les obstacles juridiques au développement du commerce électronique en Afrique liés notamment aux insuffisances qui affectent la réglementation en matière de reconnaissance juridique des communications de données et de la signature électronique et en l'absence de règles juridiques spécifiques protectrices des consommateurs, des droits de propriété intellectuelle, des données à caractère personnel et des systèmes d'information. Elle fait également état des défis liés à l'application des techniques électroniques aux actes commerciaux et administratifs à la prise en charge des éléments probants introduits par les techniques numériques (horodatage, certification, etc.), à l'adoption de règles applicables aux moyens et prestations de cryptologie et du besoin d'encadrement de la publicité en ligne et de l'adoption de législations appropriées au commerce électronique en matière fiscale et douanière.

Ce contexte particulier justifie la mise en place d'un cadre normatif approprié correspondant à l'environnement juridique, culturel, économique et social africain.

Parallèlement aux préoccupations juridiques de promotion du commerce juridique, le législateur communautaire vise à protéger les données à caractère personnel des usagers ainsi que leur vie privée ; d'où l'équilibre recherchée entre l'usage des technologies de l'information et de la communication pour une libre circulation des informations dans les pays membres de l'Union Africaine et la protection de la vie privée des citoyens dans leurs activités quotidiennes ou professionnelles.

L'objectif de la convention est triple. Elle vise d'abord à répondre aux besoins de d'harmonisation de la législation dans le domaine de la cyber sécurité dans les États membres

de l'Union africaine. Elle vise, ensuite, à mettre en place, dans chaque État partie, un dispositif protectionel contre les atteintes à la vie privée engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel. Puis, elle propose un type d'ancrage institutionnel afin de garantir dans le cadre d'une veille permanente, que tout traitement de données, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques tout en préservant les prérogatives régaliennes des États, les droits des collectivités locales et les intérêts des entreprises. Enfin, dans la même logique de sécurité et de protection des systèmes informatiques et des réseaux, elle fixe les grandes orientations de la stratégie de répression, dans les pays membres de l'Union Africaine, pour lutter efficacement contre la cybercriminalité en général et le blanchiment de capitaux en particulier. Cette stratégie vise en droit pénal substantiel d'une part à moderniser les instruments de répression de la cybercriminalité, par l'élaboration d'une politique d'adoption d'incriminations nouvelles spécifiques aux TIC et d'autre part l'adaptation de certaines incriminations classiques, des sanctions et du régime de responsabilité pénale en vigueur dans les États Membres aux exigences des technologies de l'information et de la communication.

Sur le plan procédural, elle fixe d'une part le cadre de l'aménagement de la procédure classique relativement aux technologies de l'information et de la communication et précise d'autre part les conditions d'aménagement de procédures spécifiques à la cybercriminalité.

C. Sources nationales

Le législateur sénégalais, conformément aux engagements internationaux de l'Etat et dans la dynamique de mise à niveau du droit positif national, a adopté en interne diverses dispositions d'ordre stratégique et opérationnel

Loi d'orientation sur la société de l'information : Loi numéro 2008-10 du 25 janvier 2008 portant loi d'orientation sur la société de l'information (LOSI)

Cette loi pose les fondements et les grandes orientations de la Société de l'information au Sénégal. Elle se réfère à la Résolution 56/183 du 21 décembre 2001 de l'Assemblée générale des Nations Unies qui a lancé au début de ce 21ème siècle le Sommet Mondial de la Société de l'Information (SMSI).

La loi sénégalaise d'orientation sur la société de l'information (LOSI) rentre dans la cadre de l'appropriation de cette vision sur le plan national traduisant une volonté manifeste des autorités de prendre en charge les engagements internationaux du Sénégal tant au plan sous-régional, régional et qu'international en vue de l'édification de la société de l'information.

Cette loi décline cette vision à travers la définition des objectifs et les grandes orientations de la Société Sénégalaise de l'Information et la mise à niveau de la législation actuelle dans le domaine des technologies de l'information et de la communication.

L'importance des enjeux que suscitent les technologies de l'information et de la communication s'apprécient au regard des opportunités qu'offre l'énorme potentialité de production de richesse par le biais du commerce électronique et des innovations apportées dans divers secteurs prioritaires disposant d'une grande marge de développement comme les secteurs des télécommunications, de la santé, de l'éducation, de l'administration (e-gouvernement,). Cette loi répond au besoin d'encadrement de ce secteur en pleine évolution.

Au titre des normes consacrées, la loi précise en son article 3 que la société de l'information est une société à dimension humaine, inclusive et solidaire, ouverte, transparente et sécurisée, qui œuvre en vue de l'accélération du développement économique, social ainsi que culturel, de l'élimination de la pauvreté et de la modernisation de l'Etat

Le législateur y consacre un certain nombre de principes comme la liberté d'action des individus et des peuples pour leur développement et leur épanouissement, le principe d'égalité à l'accès aux ressources composées des connaissances et des informations, la liberté d'expression, le principe de sécurité a tous les niveaux d'intervention garanti par l'Etat, le principe de solidarité entre l'Etat, les entreprises, les collectivités locales et la société civile pour faciliter l'accès aux services universels aux individus et au peuple et pour produire des technologies pour le développement de la société de la SIC. Concernant les financements, le législateur prévoit l'institution d'un fonds de solidarité qui sera associé à d'autres fonds pour la réalisation des objectifs de la SIC. Le législateur y prévoit des réformes fiscales douanières en vue de promouvoir le développement de la SIC. Ces réformes visent à adopter des nouvelles règles plus appropriées à la SIC mais également l'adaptation des règles existantes aux exigences de la société de l'information. Des secteurs prioritaires y sont vises dont celui des fichiers de population et de l'état civil.

Loi 2018–28 du 12 décembre 2018 portant Code des communications électroniques :

Après avoir défini son champ d'application et donné les définitions des concepts employés dans la loi, le législateur a précisé les objectifs de la loi qui vise essentiellement à promouvoir le développement et la modernisation des réseaux et services de communications électroniques à travers un cadre juridique efficace transparent et flexible. Elle promeut la convergence des réseaux et services dans les secteurs des communications électroniques, de l'audiovisuel et de l'informatique. Enfin, elle vise à favoriser une concurrence effective dans la fourniture de réseaux et se services au profit des utilisateurs.

Règlementation de la cryptologie : Loi 2008–41 du 20 août 2008 portant sur la Cryptologie ;

En raison de la centralité de la confiance des utilisateurs dans l'utilisation des technologies de l'information et de la communication, le législateur sénégalais soucieux du développement de la Société de l'information mise sur la maîtrise globale de la sécurité des systèmes d'information et des données.

A cet effet, la cryptologie étant jugée comme la solution technique indispensable pour protéger

les échanges et les systèmes d'information sur les nouvelles technologies contre d'éventuelles violations de leur intégrité, le législateur a entendu réglementer cette solution technologique en vue de garantir son intangibilité.

Cette solution vise à garantir la confidentialité des systèmes, des données stockées, échangées ou circulant sur l'Internet, sur l'Intranet voire sur un simple réseau privé.

Du point de vue de son utilité, la cryptologie est utilisée dans plusieurs domaines d'activités notamment dans l'administration et le secteur des télécommunications et de l'informatique, plus précisément dans les opérations de paiements électroniques et au niveau des centres d'appels et des structures de transfert d'argent,

La nouvelle loi définit désormais les conditions générales d'utilisation, de fourniture, d'importation et d'exportation des moyens et des prestations de cryptologie.

Décret 2010–1209 du 13 septembre 2010 pris en application de la loi 2008–41 du 20 août 2008 sur la cryptologie au Sénégal

Ce décret d'application vise à compléter les dispositions de la loi n° 2008-41 du 20 août 2008 sur la cryptologie au Sénégal. Il apporte des précisions relatives notamment :

- Aux dispositions générales portant sur l'objet et les définitions des principaux termes techniques utilisés ;
- À la composition, aux modalités d'organisation et de fonctionnement de la Commission nationale de cryptologie ;
- Aux régimes juridiques des moyens et prestations de cryptologie ;
- Aux conditions de délivrance des agréments aux organismes exerçant des prestations de cryptologie ;
- Aux sanctions envisagées en cas de non-respect de la législation en vigueur en matière de cryptologie.

Notons l'importance de la cryptologie et de sa règlementation dans l'identité numérique nationale au regard de la dépendance de sa fiabilité et de sa sécurité à la solution de la cryptologie. Par conséquent, le dispositif juridique qui gouverne cette technologie participe de la sécurité des prestations de cryptologie et incidemment de celle de l'identité numérique.

Promotion des start-ups : Loi numéro 2020 01 du 6 janvier 2020 relative à la création et la promotion de la start-up au Sénégal

Ayant pris conscience du rôle des Start up dans la promotion des innovations, moteurs de la diversification et de la multiplication des offres de services dans le domaine du numérique, le législateur sénégalais conformément aux objectifs du plan Sénégal émergent (PSE) et de la Stratégie Sénégal numérique 2025, s'est inscrit dans une dynamique de promotion des Start up

notamment en vue de développer l'économie nationale.
Il s'agit à travers ces innovations d'impulser la productivité et l'accroissement de la compétitivité pour garantir la qualité et la diversité de l'offre des biens et services.
L'Etat du Sénégal, entend pleinement œuvrer à l'édification d'un environnement juridique et institutionnel propice au développement de la start-up capable de dynamiser l'écosystème numérique au Sénégal.
Cette loi comprend cinq chapitres :

- Le chapitre Premier est relatif aux dispositions générales ;
- Le chapitre 2 traite du cadre institutionnel et organisationnel du dispositif d'appui, de régulation et de promotion de la start-up ;
- Le chapitre 3 est consacré aux mesures incitatives consenties aux start-ups ;
- Le chapitre 4 a trait à la responsabilité et aux sanctions ;
- Le chapitre 5 concerne les dispositions finales.

Règlementation des transactions électroniques : Loi 2008- 08 du 25 janvier 2008 sur les transactions électroniques

Cette loi adoptée par l'Assemblée nationale en sa séance du vendredi 30 novembre 2007 et le Senat en sa séance du mardi 15 janvier 2008 a été votée le 25 janvier 2008.

Conformément aux objectifs, axes et principes dégagés par la loi d'Orientation sur la Société de l'Information (LOSI), la loi relative aux transactions électroniques vise, à favoriser le développement du commerce électronique à travers les Technologies de l'Information et de la Communication (TIC).

Il s'est agi essentiellement de prendre en charge les préoccupations des acteurs quant à la reconnaissance juridique des réalités et besoins du numérique encore laissées en friche comme :

- La valeur juridique de la signature électronique ;
- La reconnaissance juridique de la preuve électronique ;
- La sécurité des échanges électroniques ;
- La protection du consommateur ;
- La valeur juridique des documents électroniques par rapport aux documents papiers ;
- L'application des techniques électroniques aux actes commerciaux et administratifs ;
- La valeur probante issue des techniques numériques (horodatage, certification, etc.).

La loi adopte une approche neutre face à la technologie en promouvant les transactions électroniques et en précisant notamment les exigences en matière de preuve et de signature électronique.

En vue d'écarter les contraintes juridiques qui font obstacle au développement de ces transactions, la loi consacre le principe de l'équivalence des dossiers électroniques aux documents papiers.

L'objectif principal de cette loi est d'assurer **la sécurité des transactions par l'instauration d'un cadre juridique adapté aux modalités et spécificités de l'environnement numérique**

A cet effet, elle prévoit notamment des définitions claires des notions de communication électronique, et du commerce électronique et prévoit un régime de responsabilité du commerçant électronique ainsi que l'encadrement des sollicitations commerciales par l'interdiction notamment de la transmission non consentie de la publicité par message électronique. **Elle consacre le principe de la liberté de communication en ligne tout en instituant un régime de responsabilité des prestataires techniques**. Est considéré comme prestataire technique tout prestataire utilisant les protocoles de l'Internet qui met à la disposition des personnes physiques ou morales, publiques ou privées, des biens et services. Le décret met à la charge des prestataires des obligations minimales de surveillance sur les contenus et leur participation à la lutte contre l'acceptation, le traitement et la diffusion de contenus illicites.

Par rapport à la problématique de l'identification, retenons que la loi donne une place importante à la question dans les transactions électroniques. Elle prévoit à ce titre que les personnes fournisseurs d'accès et hébergeurs telles que mentionnées aux points 1 et 2 de l'article 3 de la présente loi détiennent et conservent les données de nature à permettre l'identification de tout contributeur à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.

Vis-à-vis de leurs clients, ces prestataires fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues à l'article 5 de la présente loi. Il s'agit :

- Pour les personnes physiques : leur nom, prénoms, domicile et numéro de téléphone et, si elles sont assujetties aux formalités d'inscription au registre du commerce et du crédit mobilier, le numéro de leur inscription ;
- Pour les personnes morales : leur dénomination ou leur raison sociale et leur siège social, leur numéro de téléphone et, s'il s'agit d'entreprises assujetties aux formalités d'inscription au registre de commerce et du crédit mobilier (RCCM) ou au répertoire national des entreprises et associations, le numéro de leur inscription, leur capital social, l'adresse de leur siège social ;
- Le nom du directeur ou du codirecteur de la publication, du service de communication au public par voie électronique et, le cas échéant, celui du responsable de la rédaction ;
- Le nom, la dénomination ou la raison sociale, l'adresse et le numéro de téléphone du prestataire mentionné au point 2 de l'article 3 de la présente loi.
- Pour les personnes éditant à titre non professionnel un service de communication au public en ligne, elles peuvent ne tenir à la disposition du public, pour préserver leur anonymat, que le nom, la dénomination ou la raison sociale et l'adresse du prestataire, sous réserve de lui avoir communiqué des éléments d'identification personnelle prévus par la présente loi.

L'autorité judiciaire peut requérir la communication auprès de ces prestataires des données. Tout traitement de données reste soumis aux dispositions de la loi sur la protection des données à caractère personnel.

Les personnes mentionnées au point 2 de l'article 3 de la loi sont assujetties au secret professionnel dans les conditions prévues à l'article 363 du Code pénal, pour tout ce qui concerne la divulgation de ces éléments d'identification personnelle ou de toute information permettant d'identifier la personne concernée. Ce secret professionnel n'est pas opposable à l'autorité judiciaire.

Règlementation du Commerce électronique : Décret 2008–7 18 du 30 juin 2018 relative au commerce électronique

Le commerce électronique est défini comme l'activité économique par laquelle une personne propose ou assure, à distance et par voie électronique, la fourniture de biens et la prestation de services.

Ce texte fait de l'identification une question essentielle dans l'exercice du commerce électronique. C'est ainsi qu'il est exigé de toute personne exerçant l'activité définie aux articles 8 et 10 de la loi sur les transactions électroniques, de respecter l'obligation de fournir au consommateur les informations sur le nom du directeur de publication, l'adresse électronique et postale pour des réclamations éventuelles, le numéro de téléphone ou de fax ainsi que d'autres indications sur le bien ou le service, les prix et les modalités de la transaction.

Le fournisseur électronique de biens ou de services doit également préciser de manière univoque les différentes modalités des transactions à partir de la page d'accueil de son site web.

Ces informations doivent être accessibles et reproduites, en cas de besoin, par le consommateur en vue de leur conservation. La responsabilité contractuelle du fournisseur électronique de biens et services, mentionnée à l'article 11 de la loi sur les transactions électroniques, est automatiquement engagée en cas d'inexécution de ses obligations. La publicité doit être conforme aux exigences de décence et de respect de la dignité de la personne humaine. Elle ne doit pas être de nature à induire le consommateur en erreur sur l'offre réellement proposée et en particulier sur l'entreprise à l'origine de l'offre conformément à l'article 13 de la loi sur les transactions électroniques.

Décret 2008–719 du 30 juin 2008 relatif aux communications électroniques

Ce décret pris en application de la loi sur les transactions électroniques explicite les règles en matière de communications électroniques. Il a pour objet de fixer les conditions d'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques, notamment celles relatives à la sécurité des transactions électroniques.

Il met en exergue les exigences techniques afin de sécuriser les transactions numériques notamment avec l'usage de moyens technologiques appropriés, efficaces et accessibles permettant de garantir une navigation sécurisée. Le texte vise particulièrement la faculté d'identifier les erreurs commises dans la saisie des données et de les corriger et veille sur la

sureté de la navigation des mineurs par la restriction d'accès à l'Internet, la facilitation d'un contrôle parental performant et sans surcoût pour l'utilisateur avec une mise à disposition de mesures techniques de filtrage.

Du point de vue de la responsabilité des prestataires, les utilisateurs peuvent l'engager en cas d'absence de ces mesures techniques sécuritaires. Il pèse sur ces prestataires une obligation de contrôle spécifique afin de détecter d'éventuelles infractions. A ce titre, ils effectuent à la demande de l'autorité judiciaire toute activité de surveillance ciblée ou temporaire des informations qu'ils transmettent ou stockent en vue de prévenir ou de faire cesser un dommage occasionné par le contenu d'un service de communication par voie électronique.

Ces prestataires techniques ont également une obligation d'information des autorités compétentes, dans les meilleurs délais, de tout contenu en ligne manifestement illicite.

Ils ont aussi une obligation de prompt retrait des contenus ou de fermeture d'accès, conformément aux dispositions légales en vigueur.

Dans le domaine administratif, en application de l'article 43 de la loi sur les transactions électroniques, les actes des autorités administratives peuvent faire l'objet d'une signature électronique.

Le décret admet également le principe de validité de la réponse administrative par voie électronique lorsque l'autorité administrative a été saisie d'une demande d'information qui lui a été adressée par la même voie par un usager ou par une autre autorité administrative.

Sauf dispositions contraires, lorsqu'une personne doit communiquer à une autorité administrative une information et que cette information émane d'une autre autorité administrative, cette communication peut, à condition que l'intéressé l'ait préalablement acceptée de manière expresse, être directement opéré par voie électronique.

Cependant, il est exigé de toute autorité administrative mettant en place un système d'information de prendre les mesures de sécurité nécessaires pour protéger ledit système.

L'exigence d'un accuse de réception par voie électronique est consacrée en cas de saisine de l'autorité administrative par un usager d'une demande, d'une déclaration, d'un paiement ou d'une information par voie électronique.

L'accusé de réception doit préciser la date de réception de la demande, le service saisi et la date à laquelle cette demande sera acceptée ou rejetée. Le cas échéant, elle doit mentionner le délai de réponse.

Afin de marquer l'équivalence, l'autorité administrative doit traiter la demande sans exiger, de l'usager, la confirmation ou la répétition de l'envoi de sa correspondance sous une autre forme, notamment en support papier.

La forclusion pour expiration du délai de recours ne peut être opposée au requérant lorsque l'accusé de réception ne lui a pas été transmis ou ne comporte pas les indications mentionnées à l'article 29 du décret.

Cependant, l'autorité administrative n'est pas tenue d'accuser réception des envois abusifs, notamment du fait de leur nombre, leur caractère répétitif ou systématique.

Nous relèverons par rapport à l'objet de notre revue que ce décret d'application évoque notamment en ses articles 11 et suivants la question de l'identification des prestataires techniques, telle qu'exigée par l'article 5 de la loi sur les transactions électroniques.

Ces prestataires techniques doivent mettre en œuvre un dispositif technique permettant de conserver les éléments d'information visés par l'article 5 de la loi sur les transactions électroniques.

A cet effet, ils défèrent aux réquisitions des autorités judiciaires tendant à obtenir, soit les données d'identification de l'auteur d'un contenu qu'ils hébergent, soit les données portant sur l'identification des personnes utilisatrices des services qu'ils fournissent.

Ces prestataires ont une obligation de résultat en matière de conservation des données permettant l'identification de celui qui a contribué à la création du contenu en ligne.

Ils engagent leur responsabilité par négligence, conformément à l'article 431-44 de la loi sur la cybercriminalité, si les données qu'ils détiennent sont manifestement fantaisistes et ne permettent pas l'identification envisagée. Nous entrevoyons l'apport d'une identification numérique nationale dans l'exécution stricte de cette obligation des prestataires techniques.

Les données conservées portent exclusivement sur les éléments permettant l'identification des utilisateurs des services fournis par les prestataires techniques.

Cependant, ces données ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées.

Ces prestataires techniques doivent permettre aux autorités compétentes un accès facile, direct et permanent aux informations de l'art 5. A défaut de mise à disposition au public des informations prévues par ces textes, ces prestataires sont passibles des sanctions prévues par l'article 431-46 de la loi sur la cybercriminalité.

Règlementation de la Certification électronique : Loi numéro 2008–08 du 25 janvier 2008 relative à la certification électronique prise en application de la loi n 2008–08 et 25 janvier 2008 sur les transactions électroniques

La cryptologie a pour objet la garantie de la confidentialité des systèmes, des données stockées, échangées ou circulant sur les réseaux Internet, Intranet ou privé. Ainsi, elle a vocation à établir

et à renforcer la sécurité des communications électroniques et à instaurer la confiance des utilisateurs dans la navigation numérique.

En effet, le développement de la Société de l'information ne peut se réaliser sans la confiance des usagers. Pour ce faire, une maîtrise parfaite de la sécurité des systèmes d'information et des données est requise.

A ce titre, la cryptologie propose une solution technique fiable pour protéger les échanges et les systèmes d'information sur les nouvelles technologies contre d'éventuelles violations de leur intégrité.

Au Sénégal, la cryptologie est utilisée dans plusieurs secteurs notamment au sein de l'administration, dans le domaine des télécommunications, de l'informatique et plus précisément au niveau des Centres d'appels, des sociétés de transfert d'argent, ainsi que pour les paiements électroniques.

Sur le plan juridique, la loi n° 2001-15 du 27 décembre 2001 portant Code des télécommunications prévoyait en son article 37 le régime de la cryptologie, mais ne prenait pas en compte certains aspects fondamentaux notamment, la fourniture, le transfert et les conditions d'homologation liées à l'importation ou l'exportation de moyens ou de prestations de cryptologie.

Au plan pénal, la portée de l'article 67 du même Code, qui prévoyait les peines applicables en cas de violation des règles sur la cryptologie, était très restrictive car les sanctions envisagées ne portaient que sur les exportations ou les importations de moyens de cryptologie sans autorisation.

Face à ces insuffisances, il est prévu, d'une part, l'abrogation de ces dispositions et d'autre part, la mise en place d'une loi sur la cryptologie.

Cette loi plus générale a pour objectif de définir les conditions d'utilisation, de fourniture, d'importation et d'exportation des moyens et des prestations de cryptologie.

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.

Elle se fonde sur le chiffrement et le déchiffrement et l'utilisation d'algorithmes permettant de générer des clés secrets et publics et de codes secrets pour garantir la confidentialité des échanges, les rendant inintelligibles.

La cryptologie permet l'authentification qui est une procédure dont le but est de s'assurer de l'identité d'une personne pour contrôler l'accès à un logiciel ou à un système d'information ou de vérifier l'origine d'une information ; *d'où le rapport étroit entre le projet d''identité*

numérique et la règlementation de la certification.

A ce sujet notons que le décret 2008-720 du 30 juin 2008 prévoit les modalités de la certification.

Décret 2008- 720 du 30 juin 2008 relatif à la certification électronique pris pour l'application de la loi numéro 2008–08 du 25 janvier 2008 relative à la certification électronique ;

En termes d'authentification des personnes et des documents, le Sénégal a opté pour un système de certification. Il a institué dans ce sens, une Autorité de certification en charge de la délivrance des agréments, en l'occurrence l'Agence de l'informatique de l'Etat.

Ce décret fixe les conditions et les procédures d'exercice de l'activité de certification électronique conformément aux dispositions de la loi n° 2008-08 du 25 janv. 2008 relatives aux transactions électroniques. Notons que le Certificat au sens des dispositions de ce décret est une attestation électronique qui lie des données afférentes à la vérification d'une signature ou de tout autre document numérique à une personne. Le certificat confirmant l'identité d'une personne ou la conformité d'un document, est un lien entre l'entité physique et l'entité électronique. Quant à la certification, elle consiste en une procédure qui sert à faire valider la conformité d'un système selon certaines normes par un organisme. Elle permet de donner une assurance écrite par l'intervention d'un tiers, qu'un produit, un processus ou un service est conforme aux exigences spécifiques.

Le législateur a donné à l'Agence de l'Informatique de l'Etat (ADIE) des compétences de délivrance pour octroyer des agréments aux organismes assurant une activité de certification électronique et des missions de contrôle par rapport au respect par les organismes de certification des dispositions en vigueur en matière de certification et des certificats mis par les organismes de certification de signatures électroniques. Elle a également pour mission de fixer les caractéristiques du dispositif de création et de vérification de la signature électronique et de tenir un registre des organismes de certification agrées.

Ce décret prévoit également les obligations de l'organisme certificateur concernant la garantie de ses compétences techniques, de la sécurité de son dispositif et de sa procédure, des diligences quant à la tenue des registres des certificats et la gestion de la confidentialité.

Ce texte règlemente également les modalités et les garanties sécuritaires de la signature électronique. Aux termes de l'article 39 dudit décret, la signature électronique consiste en un ensemble de données qui doivent permettre d'identifier le signataire ; elle doit être liées uniquement au signataire ; elle doit être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ; elle doit reposer sur un certificat électronique.

Notons que l'Agence de l'informatique de l'Etat et les organismes de certification sont tenus au respect des dispositions légales régissant le traitement de données à caractère personnel.

Concernant les questions d'identité, lorsque le titulaire du certificat utilise un pseudonyme, l'organisme de certification ayant délivré le certificat est tenu de communiquer toute donnée relative à l'identité du titulaire aux autorités judiciaires compétentes.

IV. Les textes ayant une vocation protectionnelle

Certains textes émanent des instances internationales ou communautaires, d'autres textes tirent leurs sources des instances nationales.

A. Sources internationales

1. Sources communautaires

Sur la Cybersécurité et la lutte contre la cybercriminalité : Directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace CEDEAO 17-19 août 2011

Cette Directive qui a une valeur supranationale fixe les orientations pour l'harmonisation de la législation en matière de lutte contre la cybercriminalité. Il se réfère à l'Acte Additionnel A/SA.1/01/10 relatif à la protection des données à caractère personnel dans l'espace CEDEAO et à l'Acte Additionnel A/SA.2/01/10 relatif aux transactions électroniques dans l'espace CEDEAO. Il met en exergue le besoin et la nécessité de coopération et d'entraide dans ce domaine de lutte contre la cybercriminalité fortement caractérisée par sa transnationalité. Il se réfère également à la Convention A/P1/7/92 de la CEDEAO relative à l'entraide judiciaire en matière pénale et à la Convention A/P1/8/94 de la CEDEAO relative à l'Extradition.

Mesurant l'importance de l'efficacité des enquêtes pour la réussite de cette lutte, il cite comme référence, l'Accord de coopération en matière de police criminelle entre les Etats membres de la CEDEAO qui prescrit la mise en commun des compétences et partage d'expériences par les services de sécurité en vue d'accélérer de façon efficace les enquêtes policières.

Du point de vue de la contextualisation, le législateur communautaire fait état de la recrudescence d'actes répréhensibles de tous ordres engendrés par l'utilisation des Technologies de l'Information et de la Communication entre autres l'Internet ou la cybernétique.

Cette cybercriminalité en tant que phénomène nouveau a nécessité la définition des infractions spécifiques, lesquelles doivent être rattachées consubstantiellement aux infractions classiques, telles que le vol, l'escroquerie, le recel, le chantage en raison de la nature du préjudice causé au moyen de l'utilisation de l'Internet.

Il en déduit que les actes répréhensibles commis au moyen de l'Internet nécessitent une qualification sur le plan légal et une répression appropriée en raison de la gravité des préjudices qu'ils engendrent.

Dans le même ordre d'idées, il estime important d'adopter un cadre de répression pénale adapté en vue de lutter efficacement contre la cybercriminalité et de promouvoir une coopération efficace et viable à l'échelle internationale.

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

Cet Acte additionnel adopté à la 37e session de la Conférence des chefs d'État et de gouvernement à Abuja, le 16 février 2010, se fonde sur les articles 7, 8 et 9 du Traité révisé de la CEDEAO tel qu'amendé, portant création de la Conférence des chefs d'État et de gouvernement et définissant sa composition et ses fonctions.
Cet Acte additionnel s'attache au respect, à la promotion et à la protection des droits de l'homme et des peuples, conformément aux dispositions de la Charte africaine des droits de l'homme et des peuples. Il se réfère, par ailleurs, aux articles 27, 32 et 33 dudit traité relatifs à la science et à la technologie et au domaine de la communication et les télécommunications.
Il fait référence à l'Acte additionnel A/SA 1/01/07 du 19 janvier 2007 de la CEDEAO relatif à l'harmonisation des politiques et du Cadre réglementaire du secteur des technologies de l'information et de la communication.
Du point de vue du contexte, le législateur communautaire indexe les progrès importants réalisés dans le domaine des technologies de l'information et de la communication (TIC) ainsi que l'Internet dont l'utilisation inappropriée dans la vie quotidienne des usagers suscite des menaces relativement à la vie privée et professionnelle des utilisateurs. Il met en exergue les fonctionnalités avancées de la technologie de l'Internet marquées par ses facilités de profiler et de tracer des individus sur la base de collecte et de traitement des données à caractère personnel. Il invoque, par ailleurs, les potentiels préjudices que peuvent provoquer l'utilisation croissante des technologies de l'information et de la communication dans la vie privée et professionnelle des utilisateurs.
Le législateur communautaire relève que nonobstant l'existence des législations nationales relatives à la protection de l'intimité des citoyens dans leur vie quotidienne ou professionnelle et à la garantie de la libre circulation des informations, il s'avère important de combler un vide juridique créé par la naissance de ce nouvel instrument de communication qu'est l'Internet.
L'adoption cet Acte additionnel vise à combler ce vide juridique et à créer en conséquence un cadre légal harmonisé dans le traitement des données à caractère personnel.
L'Acte additionnel sera pris après avis du Parlement de la Communauté en date du 23 mai 2009 et sur recommandation de la 63éme session ordinaire du Conseil des ministres, tenue à Abuja les 20 et 21 novembre 2009.
Cet Acte additionnel prévoit les règles essentielles que doivent prendre les Etats membres en vue de garantir une protection efficace des données personnelles de leurs ressortissants.
Après avoir défini les notions clés employées dans le cadre de ce dispositif normatif, le législateur communautaire de la CEDEAO a défini son champ d'application en désignant les données soumises à la protection et celles qui en sont exclues. Il a défini, suivant la nature des données les formalités requises suivant le régime applicable : régime de déclaration, de demande d'avis, d'autorisation, d'exonération de déclaration et de dispense de formalités.
Notons que l'autorisation est requise pour tout traitement relatif à un numéro national d'identification ou à des données comportant de la biométrie.
Au plan institutionnel, le législateur communautaire exige pour le traitement des données à caractère personnel, la création au niveau des Etats d'une autorité administrative

indépendante en charge de la protection des données à caractère personnel. Il a défini sa composition avec les incompatibilités et les immunités dont jouissent ses membres et l'obligation de secret professionnel à laquelle ils sont assujettis. Il fixe avec précision ses compétences, les modalités de sa saisine et les sanctions qu'elle peut prononcer dans l'exercice de ses attributions. Dans un souci de moralisation des activités de traitement des données à caractère personnel, le législateur communautaire a fixé un certain nombre de principes applicables lorsque le traitement est autorisé. Il s'agit des principes de légitimité, de licéité, de loyauté, de finalité, de pertinence, d'exactitude, de transparence, de confidentialité, et de sécurité. Ces principes visent à garantir un comportement responsable et respectueux de la vie privée des personnes concernées. À ce titre, un principe majeur interdit le traitement des données dites sensibles en raison de la délicatesse de leur objet à savoir, les questions liées à l'origine raciale, ethnique ou régionale ainsi que les questions relatives à l'opinion politique, aux convictions religieuses et philosophiques, à l'appartenance syndicale ou bien les questions qui touchent à la vie sexuelle, aux données génétiques et à la santé de manière générale.
Le texte prévoit à côté de ces principes, des droits conférés à la personne concernée en vue de lui octroyer les moyens nécessaires pour assurer la surveillance de ses données et l'exercice de ses prérogatives. Ainsi, la personne dont les données font l'objet de traitement, dispose d'un droit à l'information, d'un droit d'accès, d'un droit d'opposition, et d'un droit de rectification et de suppression.
Quant au responsable du traitement l'Acte additionnel exige qu'il soit soumis à un certain nombre d'obligations à savoir : l'obligation de confidentialité afin de préserver l'intangibilité des données et la non-accessibilité aux tiers, l'obligation de sécurité qui permet d'assurer l'infaillibilité du système de traitement et l'intégrité des données, l'obligation de conservation pour la durée légale et l'obligation de pérennité.

2. Texte à portée continentale :

La Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014.

Cette Convention de l'Union africaine portant adoption d'un cadre juridique sur la cybersécurité et la protection des données à caractère personnel s'inscrit dans le cadre de la consécration des engagements des États membres de l'Union Africaine tant au plan sous régional, régional, qu'international en vue de l'édification de la Société de l'Information.
Elle définit les objectifs et les grandes orientations de la société de l'Information en Afrique et vise à renforcer les législations des États membres et des Communautés Économiques Régionales (CER) en matière de Technologies de l'Information et de la Communication.
Le législateur africain y réitère l' attachement des États membres aux libertés fondamentales et aux droits de l'homme et des peuples contenus dans les déclarations, conventions et autres instruments adoptés dans le cadre de l'Union Africaine et de l'Organisation des Nations Unies et rappelle que la mise en place d'un cadre normatif sur la cyber sécurité et la protection des données à caractère personnel exige le respect des droits des citoyens, garantis en vertu des textes fondamentaux de droit interne et des Conventions et Traités internationaux relatifs aux droits de l'Homme particulièrement la Charte africaine des droits de l'Homme et des Peuples.

Une approche inclusive des acteurs publics et privés (États, collectivités locales, entreprises du secteur privé, organisations de la société civile, médias, institutions de formation et de recherche etc.) est préconisée en faveur de la Cybersécurité.
Le domaine technologique étant un secteur particulièrement évolutif, la convention détermine les règles de sécurité essentielles à la mise en place d'un espace numérique sécurisé garantissant la confiance dans les transactions électroniques, la protection des données à caractère personnel et la lutte contre la cybercriminalité ;
Cette convention intervenait dans un contexte juridique assez morose pour l'encadrement et la promotion du numérique en raison de nombreuses insuffisances pour le développement du commerce électronique en Afrique. Ces lacunes sont observées notamment en matière de reconnaissance juridique des communications de données, de signature électronique, de protection des consommateurs, de propriété intellectuelle, des données à caractère personnel et des systèmes d'informations.
D'autres insuffisances sont également relevées dans le droit positif comme l'absence de normes relatives au téléservice et au télétravail, à l'application des techniques électroniques aux actes commerciaux et administratifs, à la prise en charge de la valeur probante des éléments introduits par les techniques numériques comme l'horodatage, la certification, à l'encadrement juridique des moyens et prestations de cryptologie, de la publicité en ligne Et l'absence de législations fiscale et douanière appropriées au commerce électronique.
La protection des données à caractère personnel ainsi que de la vie privée se présente donc comme un enjeu majeur de la Société de l'information, tant pour les pouvoirs publics que pour les autres parties prenantes ;
Elle nécessite un équilibre entre le développement des technologies de l'information et de la communication (TIC) et la protection de la vie privée et la libre circulation des informations.
L'objectif final est d'harmoniser la législation dans le domaine de la cybersécurité dans les États membres de l'Union africaine avec la mise en place, dans chaque État partie, d'un dispositif permettant de lutter contre les atteintes à la vie privée
En vue de garantir une bonne application des normes, elle propose un type d'ancrage institutionnel, avec comme objectif de veiller sur tout traitement, sous quelque forme que ce soit, au regard du respect les libertés et droits fondamentaux des personnes physiques dans les limites des prérogatives des États, des droits des collectivités locales, des intérêts des entreprises ;
En vue de renforcer cette protection face à l'actualité de la cybercriminalité qui constitue une véritable menace pour la sécurité des réseaux informatiques et le développement de la société de l'information en Afrique, au regard du système de valeurs de la société de l'information, certains comportements ont nécessité une incrimination avec la mise en place de normes en matière de cybercriminalité et de blanchiment de capitaux.
Il s'est agi d'élaborer les grandes orientations de la stratégie de répression de la cybercriminalité par l'adoption de nouvelles incriminations spécifiques aux TIC, l'adaptation de certaines incriminations, des sanctions et du régime de responsabilité pénale en vigueur dans les États Membres à l'environnement des technologies de l'information et de la communication.

Sur le plan procédural, elle fixe d'une part le cadre de l'aménagement de la procédure classique relativement aux technologies de l'information et de la communication et précise d'autre part les conditions de l'institution de procédures spécifiques à la cybercriminalité.

B. Autres sources (Conseil EU)

Protection des données à caractère personnel : STCE 108 : Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel Strasbourg, 28.I.1981

Cette convention signée par les Etats membres du Conseil de l'Europe vise à réaliser une union plus étroite entre ses membres, dans le respect de la prééminence du droit en général et des droits de l'homme et des libertés fondamentales en particulier.

Cette convention intervient plus spécifiquement dans le cadre de la protection des droits et des libertés fondamentales des citoyens, notamment le droit au respect de la vie privée face au développement des transactions transfrontalières et des transferts des données à caractère personnel faisant l'objet de traitements automatisés. Tout en promouvant la liberté d'information sans limite des frontières, les signataires de la convention veillent au respect scrupuleux des droits fondamentaux des citoyens. Il s'agit d'un équilibre sensible et ténu à sauvegarder entre le respect des valeurs fondamentales de la protection de la vie privée et la libre circulation de l'information entre les Etats et les peuples.

Ainsi, il résulte des dispositions de l'article 1er de ce texte que « le but de la Convention est de garantir, sur le territoire de chaque Partie, à toute personne physique, quelles que soient sa nationalité ou sa résidence, le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant. »

La Convention donne une définition très simple des données à caractère personnel : selon l'article 2 de la Convention, « données à caractère personnel » signifie : toute information concernant une personne physique identifiée ou identifiable ;

Notons que sur beaucoup de questions relatives au numérique, le Conseil de l'Europe a pris des normes ouvertes à la ratification d'autres pays même situés dans d'autres continents. Cette convention sur la protection des personnes contre le traitement automatisé de données à caractère personnel (STE numéro 108) (complétée par un protocole additionnel concernant les autorités de contrôle et les flux transfrontaliers de données (STE n 181) adoptée le 28-1-1981 à Strasbourg est actuellement le seul instrument juridique international à vocation universelle en matière de protection des données à caractère personnel. Elle a été ratifiée par le Sénégal suite à l'adoption par le Conseil des ministres le 8 juin 2016 du projet de loi autorisant le Président de la République à ratifier la Convention. La loi a été votée par l'Assemblée nationale le 24 juin 2016 et les instruments de ratification signés le 3 août 2016 et déposés comme instruments d'adhésion *le jeudi 25 août 2016*. Cette ratification fait du Sénégal le 50e Etat membre adhérant à la Convention 108 du Conseil de l'Europe.

Par cette ratification le Sénégal a mis à niveau sa législation sur la protection des données à caractère personnel par rapport aux standards internationaux. Cette ratification, en renforçant le cadre juridique national dans le domaine du numérique, ouvre le Sénégal à l'espace commun d'échanges et de facilitation des transactions électroniques transfrontalières entre tous les Etats membres de cette convention. Par l'allégement des procédures, il s'exempte des contraintes procédurales et s'offre un avantage déterminant sur la compétitivité de son environnement juridique et l'attractivité de son espace vis-à-vis des investissements étrangers relatifs à la fourniture de services numériques.

Lutte contre la cybercriminalité : Convention du Conseil de l'Europe sur la Cybercriminalité dite convention de Budapest du 23 novembre 2001 ratifiée par le Sénégal le 16 décembre 2016

Le Conseil de l'Europe a dès le début des années 2000 adopté une convention sur la cybercriminalité ouverte à d'autres Etats non européens. L'objectif de la convention est de consolider les liens entre les Etats membres et promouvoir la coopération entre les signataires.

Face aux grandes innovations introduites par la numérisation et la mondialisation des réseaux informatiques et aux risques induits par ces nouvelles technologies, il s'est avéré nécessaire de mener une politique pénale commune destinée à protéger la société contre la criminalité organisée dans le cyberespace. Les enjeux de la menace se mesurent à l'aune de l'emploi des réseaux informatiques et de l'information électronique dans la commission des infractions pénales et dans le stockage et la transmission des éléments de preuve dans les réseaux.

L'objectif de la convention est l'adoption d'une législation appropriée et l'amélioration de la coopération internationale condition sine qua non pour une réponse pénale adaptée, rapide et efficace.

Quant au fond du droit, il s'agit de prévenir d'une part les actes portant atteinte à la confidentialité, à l'intégrité des données personnelles et à la disponibilité des systèmes informatiques, des réseaux et des données et d'autre part l'usage frauduleux de tels systèmes, réseaux et données.

Il est également question dans cette convention de procéder à l'incrimination de ces comportements et d'adopter des pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales ; la finalité étant de faciliter la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international par l'élaboration de dispositions matérielles pertinentes et la mise en place d'une coopération internationale rapide et fiable.

Il convient cependant d'assurer un équilibre entre les objectifs de l'action répressive et le respect des droits humains tels que consacrés par l'ensemble des instruments européens.

La convention se réfère au droit à la protection des données personnelles, tel que spécifié par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

Elle se réfère également aux conventions existantes du Conseil de l'Europe sur la coopération en matière pénale.

Elle prend en compte les Recommandations relatives à l'entraide judiciaire en matière pénale, aux commissions rogatoires pour la surveillance des télécommunications, aux mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, à l'utilisation de données à caractère personnel dans le secteur de la police, à la protection des données à caractère personnel dans le domaine des services de télécommunication, à la criminalité en relation avec l'ordinateur et aux principes directeurs pour définir certaines infractions informatiques. Elle s'attache à la recherche de réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe.

La convention après avoir défini des notions clés dans son chapitre premier préconise des mesures à prendre sur le plan national par les législateurs étatiques aux fins d'ériger des infractions au plan matériel relatives à la confidentialité, l'intégrité et la disponibilité des données d'une part et des systèmes informatiques d'autre part comme la falsification et la fraude informatiques. Elle érige également en infraction, la pornographie infantile et les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes. Parallèlement du droit matériel, la convention prévoit des modalités d'engagement de la responsabilité pénale tant pour les personnes physiques que pour les personnes morales. Elle fixe aussi les champs d'inculpation en incriminant aussi bien la tentative que la complicité. La convention a prévu au niveau des sanctions la nature de celles-ci et le contenu des règles de procédure concernant les pouvoirs d'investigation en matière de perquisition, de saisie et de conservation de données ainsi que les règles de compétence et de coopération internationale.

La ratification de cette convention par le Sénégal en 2016 a hissé le pays au rang des Etats offrant dans le domaine du numérique un niveau de protection juridique arrimé au rang des standards internationaux. La convention vient compléter, celle relative aux transactions électroniques.

C. Sources nationales

Protection du droit d'auteur et des droits voisins : Loi numéro 2008–09 du 25 janvier 2008 portant sur le droit d'auteur et les droits voisins.

Cette loi prévoit les droits exclusifs reconnus à l'auteur notamment celui de jouir du droit exclusif d'exploiter son œuvre sous quelque forme que ce soit et d'en tirer un profil pécuniaire. Ce droit d'exploitation appartenant à l'auteur comprend le droit de communication au public, le droit de reproduction, le droit de distribution et le droit de location.

L'on peut se poser la question de savoir quelle interaction peut exister entre le numérique et le droit d'auteur et les droits voisins. La réponse semble évidente car l'Internet par ses

propriétés particulières semble être devenu le théâtre amplifié de toutes les opérations illicites portant atteinte aux droits des particuliers notamment aux droits de la propriété intellectuelle et notamment de la création artistique. Les œuvres musicales sont reproduits et vendus sur la toile en téléchargement ou en vente en ligne sur les supports contrefaits.
On peut également s'interroger sur la relation entre l'identité et le droit d'auteur et les droits voisins. Pareillement, la relation semble évidente car avec le développement du nouveau dispositif d'identification il sera possible d'individualiser de manière fiable les titulaires des droits protégés, les usagers et consommateurs des œuvres musicales et artistiques avec possibilité de traquer toutes formes d'usurpation et de fraudes sur les identités.

Protection contre la Cybercriminalité : Loi 2008–11 du 25 janvier 2008 portant sur la Cybercriminalité

Cette loi sur la cybercriminalité s'inscrit dans la logique de l'internalisation des dispositions supranationales adoptées au niveau des organisations internationales dont le Sénégal est membre. Le même contexte du développement des Technologies de l'Information et de la Communication (TIC) et du réseau Internet, avec la diversité des services offertes et le nombre d'utilisateurs en Afrique et dans le monde, justifie l'adaptation du système de répression à la nature et à la nomenclature des infractions.

En effet, la complexité de la répression se mesure à l'aune des grandes innovations introduites par l'interconnexion permanente des réseaux informatiques et les grandes possibilités qu'offrent les technologies de l'information et de la communication en faveur du développement des transactions commerciales, au regard notamment des facilités qu'offre l'espace numérisé pour commettre des agissements répréhensibles, attentatoires tant soit aux intérêts des particuliers soit à ceux de la communauté.

En effet, l'apparition du nouveau phénomène criminel qu'est la cybercriminalité au regard de sa transnationalité, de l'immatérialité des agissements, de la volatilité des commissions et des omissions répréhensibles, mais surtout de l'anonymat qui peut couvrir l'identité des acteurs, a révélé l'inadaptation des réponses du système pénal classique essentiellement conçues pour un environnement matérialisé et national.

Le besoin de s'adapter aux spécificités de la délinquance numérique est vite ressenti tant en droit pénal substantiel qu'en droit procédural.

En droit pénal substantiel, certaines infractions ont pour cibles les systèmes informatiques, les données informatisées, les réseaux informatiques tandis que d'autres comportements consistent à utiliser les technologies de l'information et de la communication comme moyens aux fins d'agissements répréhensibles.

Au plan procédural, les règles classiques de la procédure pénale se sont montrées inadéquates pour organiser efficacement les enquêtes, les poursuites, l'instruction et le jugement en cybercriminalité.

C'est ainsi qu'il s'est agi dans le cadre ce texte de cette loi de procéder à une adaptation du système pénal, articulée autour de la modernisation des incriminations du droit pénal classique et de l'aménagement des instruments procéduraux traditionnels par rapport aux technologies de l'information et de la communication.

La loi comprend deux parties :

- La première partie est consacrée au droit pénal substantiel et comporte trois titres traitant d'abord des infractions spécifiques aux technologies de l'information et de la communication ensuite de l'adaptation de certaines incriminations et de certaines sanctions aux technologies de l'information et de la communication ;
- La deuxième partie est relative au droit pénal procédural. Elle est composée de deux titres portant d'une part, sur l'aménagement de la procédure classique par rapport aux technologies de l'information et de la communication et d'autre part, sur l'adoption d'une procédure spécifique aux infractions liées aux données à caractère personnel.

Protection pénale contre les infractions liées aux TIC : Loi n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal

Ce texte adopté par l'Assemblée nationale, en sa séance du vendredi 28 octobre 2016 s'inscrit dans la dynamique du respect des engagements internationaux du Sénégal, et de la nécessité de mettre en conformité la législation nationale avec les dispositions supra nationales, notamment par la mise en place d'un dispositif incriminant et sanctionnant les malversations qui échappent aux qualifications classiques. Ainsi, le législateur sénégalais a initié en 2016 une reforme de mise en harmonie de la loi pénale nationale avec les conventions internationales et régionales en sanctionnant des faits répréhensibles non pris en compte par le corpus pénal en vigueur.

Ce texte qui aborde plusieurs thématiques sanctionne à côté des infractions numériques, l'atteinte à la vie privée et à la représentation de la personne par captation d'image ou de son, la mise en danger d'autrui, la fausse alerte ainsi que des infractions liées au terrorisme par la modification de certaines infractions et l'incrimination de nouveaux faits pénalement répréhensibles. C'est ainsi que sont désormais incriminés lorsqu'ils sont en lien avec le terrorisme : le recrutement de personnes pour faire partie d'un groupe ou pour participer à la commission d'un acte terroriste, la fourniture de moyens, l'entente, l'organisation ou la préparation d'actes terroristes, la non-dénonciation d'actes terroristes, le recel de terroriste, la participation à un groupe terroriste.

Concernant spécifiquement la thématique du numérique, il a paru nécessaire de renforcer la lutte contre le cyber terrorisme ainsi que de toute autre forme de délinquance perpétrée par le biais de moyens électroniques et de son utilisation possible à des fins terroristes. Enfin, pour rendre plus effectives certaines mesures alternatives à l'incarcération et réduire ainsi la surpopulation carcérale, il est opportun de donner la possibilité au juge de substituer aux courtes peines d'emprisonnement, le travail au bénéfice de la société.

Notons que ce texte de loi comporte à son chapitre premier des définitions au titre de la terminologie employée dans ses dispositions. Ainsi, nous avons la définition de plusieurs concepts qui se trouvent définis par des dispositions communautaires et qui ont vocation à s'appliquer directement dans l'ordre juridique national. Le risque est lié à la contrariété ou des différences ou nuances dans les définitions.

Concernant spécifiquement la question de l'identité, la loi pénale sanctionne désormais en son *article 431-57.* (*Chapitre VI) l'usurpation d'identité numérique. Elle dispose que : « Celui qui usurpe l'identité d'un tiers ou une ou plusieurs données permettant de l'identifier, en vue de troubler sa tranquillité ou celle d'autrui ou de porter atteinte à son honneur, à sa considération ou à son patrimoine est puni d'un emprisonnement de trois ans à sept ans et d'une amende de 500.000 francs à 2.000.000 de francs ou de l'une de ces peines. »*

Adaptation de la procédure pénale à la cybercriminalité : Loi numéro 2016–30 du 8 novembre 2016 modifiant la loi numéro 65–61 du 21 juillet 1965 portant code de procédure pénale

En vue d'accompagner les réformes introduites dans le cadre de l'incrimination des infractions numériques, le législateur a réorganisé la procédure pénale en permettant aux enquêteurs et instructeurs de mener de larges investigations dans l'espace numérique en tant que réceptacles d'indices, de charges et de preuves contre les cybers délinquants. Il est ainsi prévu, pour lutter plus efficacement contre ces formes nouvelles de délinquance, le renforcement des pouvoirs du juge d'instruction et des prérogatives de l'officier de police judiciaire (OPJ) dans la collecte des preuves en cas d'infraction en matière de cybercriminalité. Cette option s'est manifestée notamment par l'institution de mesures d'investigation au moyen des technologies de l'information et de la communication et par l'organisation des procédés d'interception de correspondances téléphoniques ou émises par voie électronique.

Dans ces nouvelles prérogatives des enquêteurs et instructeurs, l'identité numérique occupera une place importante dans la mesure où, la certification et l'authentification de l'identité des personnes poursuivies permettra après la matérialisation des faits incriminés d'imputer lesdits faits aux acteurs clairement identifiés à partir des référents numériques en leur qualité d'auteurs, de co-auteurs et de complices.

En cas d'usurpation d'identité, la fiabilité de l'identité numérique et des moyens d'authentification devrait permettre d'établir les actes d'usurpation et de distinguer entre l'usurpateur et l'usurpé. L'identité numérique nationale devrait en principe favoriser la prévention de cette forme très fréquente de malversation dans la manipulation des supports papiers.

V. 4. CADRE JURIDIQUE SPECIFIQUE A L'IDENTITE NATIONALE

L'analyse du cadre juridique de l'identité nationale se fera d'une part au regard de l'identité civile dite identité fondamentale et d'autre part de l'identité numérique.

A. Encadrement juridique de l'identité fondamentale

Le droit à une identité civile est consacré par divers instruments internationaux en tant qu'obligation qui pèse sur toutes personnes physiques responsables d'une part de leur propre déclaration et d'autre part de celles des personnes placées sous leur responsabilité. Ce droit tire également sa source des engagements internationaux des Etats.
Cet enregistrement obligatoire des naissances est le socle de toute identité sociale, car elle permet d'individualiser une personne dès sa naissance par un nom et une filiation qui échappent en principe à son libre arbitre comme le prénom choisi à titre définitif par ses parents, un sexe inné, une date et un lieu de naissance, par essence immuables.
Cette identité primaire composée des références fondamentales est censée constituer la source originelle de toutes autres identités dérivées, qu'elle soit de portée générale, nationale ou sectorielle.
La portée existentielle de la déclaration de naissance fait de cette formalité à la fois un droit et une obligation. Un droit pour tout être humain mis au monde et une obligation pour tout parent a l'endroit de ses enfants. Cette portée, face au défi du nombre important d'enfants non enregistres a fini par faire de la question une problématique universelle. Sous l'égide des Nations unies, les Objectifs de Développement Durable, notamment, l'objectif n16, fait de l'enregistrement systématique des naissances une modalité de garantie à tous d'une identité juridique à réaliser d'ici 2030.
Le Convention internationale des Droits de l'enfant en ses articles 7 et 8 consacre le droit à une identité pour tout enfant et engage les Etats signataires à respecter ce droit. Elle est suivie dans cet élan par la Charte africaine des droits et du bien-être de l'enfant qui prévoit en son art 6 trois droits fondamentaux de l'enfant : droit à un nom dès sa naissance, droit à un enregistrement immédiat après sa naissance et enfin le droit d'acquérir une nationalité.
La Constitution du Sénégal, conformément aux prescriptions des textes internationaux ci-dessus, érige l'enregistrement des naissances en une obligation constitutionnelle qui pèse sur tout citoyen tant pour lui-même que pour sa famille.
Du point de vue organisationnel, le législateur prévoit dans la Loi N 72-61 du 12 juin 1972 portant Code de la famille le système sénégalais de l'Etat civil prévoit en sa section II sur les Actes d'Etat civil, notamment en son article 51 et suivants.
Les déclarations peuvent émaner du père, de la mère, d'un ascendant, d'un proche parent, du médecin, de la sage-femme, de la matrone ou de toute personne ayant assisté à la naissance ou bien encore par la personne chez qui la mère est accouchée. À défaut de déclaration par ces assujettis, les chefs de village où les délégués de quartier sont tenus d'y procéder.
Après 45 jours, les déclarations tardives peuvent encore être reçues par l'Officier d'Etat Civil pendant une année sur production par le déclarant (qui) muni d'un certificat délivré par un

médecin ou une sage-femme, ou sur attestation de deux témoins majeurs.
Passé ce délai d'un an, l'Officier d'Etat Civil ne peut dresser l'acte de naissance que sur décision du juge d'instance. Ces déclarations tardives de naissance, sont recueillies soient au niveau des juridictions d'instance statuant en audiences publiques en leur siège, soit en audiences foraines pour rapprocher les juridictions aux justiciables. Comme autre soupape de sécurité, la loi prévoit que le Procureur, peut à toute époque et en dehors des délais légaux, faire une déclaration de naissance dont il aurait eu connaissance et qui n'aurait pas été constatée à l'état civil
Ces dispositifs quoiqu'étant une soupape palliative de la non-déclaration des naissances n'empêchent pas des dysfonctionnements du système de l'Etat civil en raison des abus des justiciables et du manque de suivi des jugements rendus. Ainsi du point de vue de la sécurité des déclarations de naissance se pose effectivement comme dysfonctionnements récurrents :

- Les naissances non déclarées
- Les déclarations multiples de naissances par voie de jugements ;
- Les fausses déclarations : fausses dates, fausses filiations, faux lieux de naissance, etc.
- Les déclarations fictives, non inscrites dans les registres, mais sur des feuillets volants

Face à cette situation, une réelle volonté de prise en charge de cette problématique par les autorités gouvernementales est manifeste au niveau du continent. En effet, à la troisième Conférence des ministres de l'état civil et de la santé publique, tenue à Yamoussoukro les 12 et 13 février 2015, les États africains ont été invités à faire de l'état civil une priorité de l'agenda politique régional notamment par l'adoption de mesures fortes et des réformes tendant à l'amélioration des systèmes d'état civil et des statistiques démographiques (CRVS). Un ambitieux projet d'appui au renforcement du système d'information de l'état civil et à la consolidation d'un fichier national d'identité biométrique est lancé depuis 2018 et est en cours de réalisation.

SOURCE	REFERENCES	OBJET DU TEXTE	OBSERVATIONS
Les Objectifs de Développement Durable (ODD)	ODD N°16	Paix, justice et institutions efficaces 16.9 D'ici à 2030, garantir à tous une identité juridique, notamment grâce à L'enregistrement des naissances	À l'échelle mondiale, un quart des enfants de moins de cinq ans n'ont jamais été enregistrés à la naissance ; ils ne disposent d'aucune preuve d'identité juridique leur permettant de protéger leurs droits et de garantir l'accès universel aux services sociaux.
La Convention internationale des droits de l'enfant (CIDE)	Art. 7 et Art. 8	Art. 7 : La Convention consacre le droit à une identité Art. 8 : L'engagement des	

		Etats à préserver l'identité de tout enfant	
La Charte Africaine des droits et du bien-être de l'enfant	Art. 6	Obligation d'enregistrement immédiat de tout enfant après sa naissance.	
La Constitution du Sénégal	Art. 25-3	Devoir pour tout citoyen de s'inscrire à l'état civil et d'inscrire les actes relatifs à sa famille.	Le droit à l'enregistrement a l'Etat civil une obligation et un droit constitutionnels
Le Code de la famille	Art. 51 et suivants	Organisation du système de déclaration des naissances	Risques-aléas : Existence de dysfonctionnements du système

B. Encadrement juridique de l'identité numérique :

On distingue d'une part les initiatives de portée nationale et d'autre part les initiatives sectorielles.
En matière d'identité numérique, le Sénégal a connu diverses expériences allant d'initiatives de portée sectorielle à des initiatives de portée nationale.
Nous notons que si les initiatives à portée nationale initiées par le Gouvernement ont essentiellement été encadrées par des textes (Lois et décrets d'application), il n'en est pas de même concernant les initiatives sectorielles.
Nous notons ainsi que la notion d'identité numérique est aussi bien connue dans la pratique que dans la législation Sénégalaise même si elle ne fait pas l'objet d'une définition ni d'un encadrement général.
A ce titre, la loi de 2016 modifiant le Code pénal en fait expressément référence à l'usurpation d'identité numérique au titre des infractions liées aux TIC.

1. Une série d'expériences à portée nationale

a) Le Répertoire national des Personnes physiques (RNPP) :

Décret numéro 85–1139 du 5 novembre 1985

Ce Répertoire national qui est l'ancêtre des fichiers nationaux automatisés au Sénégal avait fait l'objet d'un encadrement juridique avec l'adoption du Décret numéro 85–1139 du 5 novembre 1985 portant constitution d'un Répertoire national des Personnes physiques. Déjà en 1985, cette initiative se référait à un Schéma directeur de l'informatique du Sénégal entrepris depuis décembre 1978. Ce qui révèle ce souci permanent des pouvoirs publics de fiabiliser le dispositif

d'immatriculation des populations en vue de stabiliser leur identification et de sécuriser la conservation et l'exploitation des données. Cette initiative avait pour objectif de mettre en place un Système généralisé d'identification nationale unique et obligatoire tel que recommandé par le Comité national informatique en janvier 1984. La gouvernance du système est confiée à la Direction de l'automatisation des fichiers (DAF) du ministère de l'Intérieur. Les assujettis à cette identification sont d'une part, tous les nationaux et d'autre part les étrangers inscrit dans les fichiers des services associés. L'identification, outre les éléments de l'État civil portait sur un numéro d'identification à onze (11) chiffres.

La carte nationale d'identité numérisée : LOI n°2005-28 du 6 septembre 2005 instituant la carte nationale d'identité sénégalaise numérisée

Cette loi de 2005 vient abroger les dispositions de la loi sur la carte nationale d'identité en format papier n° 62-14 du 20 février 1962, et institue pour la première fois une carte nationale d'identité numérique qui comporte des données électroniques pour l'identification des citoyens sénégalais.

Cette nouvelle carte nationale d'identité au-delà de son format numérisé comporte des éléments biométriques qui renforcent les référents d'individualisation de la personne avec des attributs physiques propres à la personne.

Elle comporte une photographie faite avec une caméra numérique scannée sur la carte de même que la signature du titulaire.

Le support est matérialisé par une carte miniaturisée par rapport au format traditionnel avec des filets de sécurité censé rendre la carte infalsifiable.

Cette nouvelle conception de l'identification numérique s'inscrit dans le contexte de la société de l'information marquée par une évolution technologique remarquable des Outils de l'information et de la communication.

Pour le législateur sénégalais, Cette ère de numérisation marquait une évolution fondamentale sur la fiabilisation et la sécurisation des documents et écritures publics et devrait impacter la sécurité des autres titres officiels comme les passeports et autres cartes de la vie civile du fait de la stabilisation en amont de l'état civil des personnes compte tenu de la liaison de la biométrie avec les données personnelles. :

Cette carte a pour objet de certifier et fixer l'identité de son titulaire.

Aux termes de l'article 2 de la loi, cette carte nationale d'identité n'est délivrée qu'aux seuls nationaux sénégalais et est obligatoire pour tous les citoyens âgés d'au moins 15 ans. Elle est facultative pour tout citoyen âgé de 5 ans révolus. Sa durée de validité était fixée pour une période de dix (10) ans renouvelables.

Ainsi l'on peut noter que la titularité de la carte nationale numérisée est fondée sur la nationalité et la citoyenneté ; ce qui exclue de son domaine, les étrangers et les personnes morales.

Le décret n° 2005-787 du 6 septembre 2005 sera pris pour fixer le modèle de la carte nationale d'Identité numérisée

Les libellés du contenu de la carte nationale d'identité numérisée, les conditions de sa délivrance et de son renouvellement sont prévues par ce décret. La délivrance de la carte nationale d'identité numérisée (CNIN) reposait sur la production de l'ancienne Carte nationale d'Identité ou d'un extrait de naissance datant de moins de trois mois ou toute pièce en tenant lieu ou en cas de perte, de la production d'un certificat de perte et d'un extrait de naissance datant de moins de trois mois. En cas de renouvellement, les mêmes pièces sont requises avec la production de la carte expirée.

De ces conditions de délivrance se dégage le lien étroit entre le fichier de l'Etat civil et celui de la Carte nationale d'identité tenue par la DAF.

Cette même relation s'induit entre le fichier de l'Etat civil et le fichier électoral dont la refonte totale avait été prescrite par la loi n° 2004-32 du 25 août 2004 portant annulation de toutes les listes électorales et de toutes les inscriptions figurant dans le fichier général des électeurs et prescrivait l'établissement de nouvelles listes.

En raison de la centralité de l'état civil dans l'élaboration du fichier électoral, il avait été tenu compte des contraintes de délivrance des actes d'état civil pour augmenter la durée de validité de l'extrait de naissance qui passait ponctuellement de trois mois a un an. Ce qui donne tout son sens à la politique de numérisation du fichier de l'Etat civil dans le sens de faciliter sa délivrance et son accessibilité notamment aux sénégalais résidant à l'étranger souvent confrontés aux contraintes liées à l'éloignement et aux lenteurs bureaucratiques.

Le décret n° 2005-1252 du 23 décembre 2005 modifiant l'article 5 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, a été pris à cet effet.

Ce texte prévoit qu'« *en cas de doute sur la nationalité du requérant, la production d'un certificat de nationalité est exigée* ».

Cette disposition doit susciter une réflexion dans la relation entre la Carte nationale d'identité et la nationalité proprement dite. Car dès lors que la carte n'est délivrée qu'aux nationaux sénégalais, l'on peut se demander si la production d'un simple extrait de naissance devrait suffire pour la délivrance d'une carte d'identité nationale, étant entendu que cet acte qui établit la filiation, la date et le lieu de naissance n'a pas pour objet d'établir la nationalité du requérant, même s'il peut comporter des éléments permettant d'établir ou d'analyser l'acquisition de la nationalité sénégalaise. Le fait de se référer aux noms de famille ou à un facies, en raison des brassages ethniques, ne peuvent plus servir d'indices pour une présomption de nationalité sénégalaise. Par ailleurs, le doute fondé sur le nom qui sonne étranger outre son caractère artificiel est de nature à susciter une certaine frustration à

l'égard d'un citoyen. Par ailleurs la légèreté des indices de contrôle, risque de cristalliser de simples présomptions de nationalité, avec la numérisation.

La carte nationale biométrique : Loi n° 2016-09 du 14 mars 2016 instituant une carte d'identité biométrique CEDEAO

L'adoption d'une carte nationale d'identité biométrique dans l'espace communautaire résulte d'une décision prise par les Chefs d'Etat et de Gouvernement de la Communauté économique des Etats de l'Afrique de l'Ouest (CEDEAO) à l'occasion de la quarante sixième (46ème) session ordinaire de la conférence tenue à Abuja le 15 décembre 2014. Cette carte qui vise à faciliter la circulation des ressortissants des Etats membres de la Communauté par l'unification des modalités d'identification de ces derniers. Elles servent également de document de voyage à l'intérieur de l'espace CEDEAO.

Cet instrument communautaire vise ainsi à faciliter la mobilité transfrontalière au niveau de la sous-région au moyen d'un titre sécurisé permettant de lutter contre la criminalité transnationale organisée notamment les trafics de migrants, la traite des personnes et le terrorisme.

L'adoption de cette carte biométrique communautaire, coïncide avec la date d'expiration des cartes numérisée et répond au souci de se conformer à l'engagement du Sénégal au sein de cette communauté économique régionale. D'où l'abrogation et le remplacement de la loi n° 2005-28 du 06 septembre 2005 et son décret d'application n° 2005-787 du 06 septembre 2005.

Cette carte d'identité biométrique CEDEAO réalisée avec les données biométriques n'est délivrée qu'aux citoyens sénégalais.

Comme la carte numérisée, elle est obligatoire pour tous les citoyens âgés d'au moins quinze (15) ans et est facultatif pour tout sénégalais âgé de moins de cinq (05) ans révolus. Elle est délivrée pour une durée décennale et est renouvelable.

Elle est conçue avec la technologie des cartes à puce électronique avec possibilité de diverses applications et divers d'usages, suivant des modalités fixées par décret.

Les conditions de délivrance et de renouvellement de ladite carte de même que les éléments concernés par la biométrie et sa date de prise d'effet, ainsi que la date limite de validité de l'ancienne carte d'identité sont fixés par décret. Cette loi abroge les dispositions contenues dans la loi n° 2005-28 du 06 septembre 2005 instituant la carte nationale d'identité sénégalaise numérisée.

Décret n° 2016-1536 du 29 septembre 2016 portant application de la loi n° 2016-09 du 14 mars 2016 instituant une carte d'identité biométrique CEDEAO

La carte d'identité biométrique CEDEAO est conçue pour servir à la fois de carte nationale d'identité dont les mentions sont portées au recto et de carte d'électeur dont les indications figurent au verso.

Le numéro de la carte d'identité contient dix-sept (17) chiffres dont la codification du sexe (1 pour le sexe masculin, 2 pour le sexe féminin), la codification de la région en deux chiffres, l'indication de la naissance en 8 chiffres la date de naissance du requérant, sous le format année/mois/ jour de naissance, 5 chiffres générés automatiquement par l'ordinateur et 1 dernier chiffre de contrôle calculé par l'ordinateur.

Au titre des données biométriques traitées, la carte comporte le relevé des empreintes des dix (10) doigts du requérant. Le prénom du père ainsi que les prénoms et nom de la mère sont enregistrés dans la puce électronique.

Cette carte fait office de carte d'électeur pour les citoyens inscrits sur les listes électorales. Elle est délivrée sur production de l'ancienne carte nationale d'identité numérisée ou la carte d'électeur numérisée accompagnées de photocopie ou bien sur production d'un extrait de naissance datant d'au moins un an et d'un certificat de résidence ou tout autre document en tenant lieu.

Titres de voyage : Passeport CEDEAO et Cartes d'identité biométrique : décision A/déc.2/7/85 un carnet de voyage des Etats membres de la CEDEAO

Dans le souci de mettre en œuvre le principe de la libre circulation des personnes et des biens objet de l'article 3 du Traite, ainsi que le droit de résidence et d'établissement objet du Protocole A/SP1/7/85 portant Code de conduite pour l'application du Protocole sur la Libre Circulation des personnes, le Droit de Résidence et d'Etablissement, les Etats membres de la CEDEAO ont mis en place suivant décision A/déc.2/7/85 un carnet de voyage des Etats membres de la CEDEAO afin d'harmoniser les titres de voyage au sein de la communauté et de faciliter la mobilité des ressortissants de la communauté au sein de l'espace CEDEAO.

Décision A/DEC.1/5/2000 portant institution du passeport des Etats membres de la CEDEAO

Plus tard, en 2000, il a été institué le passeport CEDEAO suivant Décision A/DEC.1/5/2000 portant institution du passeport des Etats membres de la CEDEAO. Il s'agit d'un titre de voyage de portée communautaire avec des propriétés biométriques permettant de sécuriser l'identité des voyageurs.

Décision A/déc.01/12/14 en date du 15 décembre 2014, la décision A/déc.2/7/85

En 2014 suivant Décision A/déc.01/12/14 en date du 15 décembre 2014, la décision A/déc.2/7/85 portant institution d'un carnet de voyage des Etats membres de la CEDEAO a été

modifiée en son article premier pour faire de la Carte nationale d'Identité biométrique CEDEAO un titre de voyage au sein de la CEDEAO.

En effet, il a été constaté que le carnet de voyage qui était en usage dans certains Etats membres était devenu désuet, ne correspondant plus aux normes internationales en la matière.

C'est pourquoi, dans l'objectif de conformer tous les titres de voyage au sein de la communauté aux nouvelles technologies de l'information et de la communication déjà adoptées dans les passeports biométriques, les cartes d'identités biométriques harmonisées au sein de la communauté ont été instituées en même temps comme titre de voyage au sein de la CEDEAO. Elle a pour avantage de renforcer la sécurité dans la région en matière d'identification, de faciliter et de simplifier la circulation des citoyens de la Communauté aux frontières des Etats membres.

Suivant ce texte, les ressortissants des Etats membres font l'objet de recensement biométrique dans les Etats membres d'accueil. Les autorités compétentes des pays d'origine transmettent les données biométriques de leurs ressortissants aux autorités compétentes des pays d'accueil, dans le strict respect de la protection des données à caractère personnel.

Les services de police, de douane et d'immigration procèdent au partage d'informations dans le cadre de la coopération policière et ce conformément au mécanisme du Système d'information Policière de l'Afrique de l'Ouest (SIPAO) visant le partage de l'information entre les services des polices nationales des Etats membres.

Le Permis de conduire numérique : Loi n° 2002-30 du 24 décembre 2002 portant Code de la Route et le Décret n° 2004-13 du 19 janvier 2004 fixant les règles d'application de la loi n° 2002-30 du 24 décembre 2002 du code de la route.

Le permis de conduire trouve son fondement juridique dans la Loi n° 2002-30 du 24 décembre 2002 portant Code de la Route et le Décret n° 2004-13 du 19 janvier 2004 fixant les règles d'application de la loi n° 2002-30 du 24 décembre 2002 du code de la route.

Depuis 2018 le permis de conduire a pris la forme d'une carte numérisée miniaturisée (de la taille d'une carte de crédit) qui vient remplacer l'ancien permis rose sous forme cartonnée.

La date limite pour le remplacement des anciennes cartes était fixée au 31 décembre 2019 pour les Dakarois et le 27 juillet 2020 pour les détenteurs habitant dans les autres régions. Un des objectifs de cette numerisation est de lutter contre la fraude et l'insécurité car les anciens permis de conduire faisaient l'objet de contrefaçon et de falsification.

2. Une pluralité d'initiatives sectorielles en matière d'identité numérique

Diverses initiatives ont été prises dans différents secteurs des services publics et privés. Mais la revue juridique n'a pas permis de retrouver les textes qui organisent et encadrent leur édition.

C. Tableau de synthèse de la revue du cadre juridique INN

1. Identité fondamentale

Domaine	Référence	Nature de la référence
Identité fondamentale : Etat civil	La Convention internationale des droits de l'enfant (CIDE Art. 7 : La Convention consacre le droit à une identité) Art. 8 : L'engagement des Etats à préserver l'identité de tout enfant	Supranationale
	La Charte Africaine des droits et du bien-être de l'enfant Art. 6 Obligation d'enregistrement immédiat de tout enfant après sa naissance.	Supranationale
	La Constitution du Sénégal Art. 25-3	Loi
	Loi N 72-61 du 12 juin 1972 portant Code de la famille Art. 51 et suivants (Organisation du système de déclaration des naissances)	Loi
	Décret n 72-1521 du 29 décembre 1972 fixant modèles des registres et formulaires	Décret
Nationalité	Loi n° 61-10 du 7 mars 1961 déterminant la nationalité sénégalaise	Loi
	Loi n° 2013-05 du 8 juillet 2013 portant modification de la loi n° 61-10 du 7 mars 1961 déterminant la nationalité sénégalaise, modifiée	Loi
Identité nationale : - Carte d'identité nationale - Répertoire national des Personnes physiques - Carte nationale d'identité numérisée - Carte nationale d'identité biométrique	Loi n° 62-14 du 20 février 1962, instituant la carte nationale d'identité	Loi
	Loi n° 2005-28 du 6 septembre 2005 instituant la carte nationale d'identité sénégalaise numérisée	Loi
	Loi 2016-09 du 14 mars 2016 instituant la carte biométrique CEDEAO	Loi
	Décret numéro 85–1139 du 5 novembre 1985 portant constitution d'un Répertoire national des Personnes physiques	Décret
	DECRET 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	Décret

	DECRET n° 2005-1252 du 23 décembre 2005 modifiant l'article 5 du décret précité	Décret
	Décret n° 2016-1536 du 29 septembre 2016 portant application de la loi n° 2016-09 du 14 mars 2016 instituant une carte d'identité biométrique CEDEAO	Décret
Permis de conduire - Permis de conduire ordinaire - Permis de conduire numérisé	Loi n° 2002-30 du 24 décembre 2002 portant Code de la Route	Loi
	Décret n° 2004-13 du 19 janvier 2004 fixant les règles d'application de la loi n° 2002-30 du 24 décembre 2002 du code de la route	Décret
Titres de Voyage - Passeport biométrique - Passeport de service - Passeport diplomatique	Décision A/DEC.1/5/2000 portant institution du passeport des états membres de la CEDEAO	Supranationale
	Décision A/déc.01/12/14 en date du 15 décembre 2014 modifiant la décision A/déc.2/7/85 portant institution d'un carnet de voyage des Etats membres de la CEDEAO carte d'identité biométrique CEDEAO	Supranationale
	Certificat d'immatriculation pour passeport en rapport avec la DAF	Autre
Titres d'étranger et de refugié • Carte d'identité d'étranger • Carte d'identité de refugié		

2. Identité sectorielle ou fonctionnelle

Domaine	Référence	Nature de la référence
Fonction publique : - Immatriculation	Pas de texte sur l'immatriculation. Une pratique héritée ; Gouvernance assurée par la Direction de la Solde. Innovation : on se réfère à la CIN	N/A
Activité économique : - RCCM - Carte de commerçant -Carte import-export	RCCM : OHADA : Acte uniforme portant organisation du droit commercial général : Article 45-3 Acte uniforme portant organisation des sûretés Acte uniforme sur les sociétés commerciales	Supranationale
	Carte commerçant : Code Général des Impôts : Article 733-740 du Code Général des Impôts	Loi

	Loi 2005-26 relative à la modernisation des procédures administratives applicables aux investissements	Loi
	Carte commerçant : Décret d'application n°2006-744 de la loi n°2005-26 relative à la modernisation des procédures administratives applicables aux investissements	Décret
Banque : - IBAN - Carte bancaire	Règlement n°15/2002/CM/UEMOA du 19 septembre 2002 relatif aux systèmes de paiement dans les Etats membres de l'Union Economique et Monétaire Ouest Africaine (UEMOA)	Supranationale
	Instruction n°127-07-08 du 9 juillet 2008 fixant les modalités de mise en œuvre de la surveillance par la BCEAO des systèmes de paiement dans les Etats membres de l'UEMOA	Supranationale
	Directive n° 08/2002/CM/UEMOA du 19 septembre 2002 portant sur les mesures de promotion de la bancarisation et de l'utilisation des moyens de paiement scripturaux	Supranationale
	Instruction n° 01/2003/SP du 8 mai 2003 relative à la promotion des moyens de paiement scripturaux et à la détermination des intérêts exigibles en cas de défaut de paiement	Supranationale
	Instruction n° 008-05-2015 du 21 mai 2015 régissant les conditions et modalités d'exercice des activités des émetteurs de monnaie électronique dans les Etats membres de l'Union Monétaire Ouest Africaine (UMOA)	Supranationale
	Instruction n° 009/07/RSP/2010 du 26 juillet 2010 relative au dispositif de centralisation et de diffusion des incidents de paiement de l'Union Economique et Monétaire Ouest Africaine (UEMOA)	Supranationale
	Loi uniforme relative à la répression des infractions en matière de chèque, de carte bancaire et d'autres instruments et procédés électroniques de paiement	Supranationale
Facturiers - Sonatel - Senelec - Seneau	Décret n°2007-937 du 07 août 2007 portant identification des acheteurs et utilisateurs des services de téléphonie mobile offerts au public.	Décret
	Identification des abonnés téléphoniques en rapport avec la DAF	Autre
Identité fiscale - NINEA : Numéro d'Identification Nationale des Entreprises et Associations - e-taxe	Code général des impôts	Loi
Assurance - CMU - CMU-élèves	Conseil des ministres de l'UEMOA a adopté le 26 juin 2009 le Règlement n°07/2009/CM/UEMOA	Supranationale

	Règlement n°07/2009/CM/UEMOA portant règlementation de la mutualité sociale au sein de l'UEMOA, du 26 juin 2009	Supranationale
	Décret n° 2015-21 du 7 janvier 2015 portant création et fixant les règles d'organisation et de fonctionnement de l'Agence de la Couverture Maladie Universelle. (article 7)	Décret
	Arrêté interministériel n° 1448 en date du 26 janvier 2017 portant création et fixant les règles d'organisation et de fonctionnement d'un régime d'assurance maladie pour élèves	Autre
Solde - e-solde		
Enseignement-Education - SIMEN : Identification nationale de l'Etudiant (INE) - CAMPUSEN		
Sécurité sociale-Prévoyance sociale - Carte sécurité sociale - Carte IPRES		

3. Secteur numérique

Domaine	Référence	Nature de la référence
Société de l'information	LOI n° 2008-10 du 25 janvier 2008 portant loi d'orientation sur la Société de l'Information (LOSI	Loi
Organisation et développement du secteur des télécommunications	UEMOA- Directive 02 harmonisation régimes des opérateurs de réseaux - Acte additionnel A /SA 1/01/07/ du 19 janvier 2007 CEDEAO relatif à l'harmonisation des politiques et du cadre réglementaire du secteur des Technologies de l'Information et de la Communication - Directive n°03/2006/CM/UEMOA du 23 mars 2006 relative à l'interconnexion des réseaux et services de télécommunications	Supranational
	LOI n°2018-28 du 12 décembre 2018 portant Code des Communications électroniques (abrogeant et remplaçant le Code des Télécommunications de 2011)	Loi
	Loi numéro 2020 01 du 6 janvier 2020 relative à la création et la promotion de la start-up au Sénégal	Loi

Protection des données personnelles	Conseil de l'Europe : STCE 108 - Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel	Supranational
	Union africaine : Convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel, Malabo 27 juin 2014	Supranational
	CEDEAO : Acte-additionnel-A- SA 01- 10-du-16-février-2010-relatif-à-la-protection-des-données-à-caractère personnel	Supranational
	LOI n° 2008-12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel.	Loi
	DECRET n° 2008-721 du 30 juin 2008 PROTECTION DONNÉES	Décret
	Commission des données personnelles : circulaire 240614 portant désignation de points focaux CDP	Autre
	Commission des données personnelles : circulaire primature 12 fév. 2015 obligation de déclaration des fichiers et des bases de données	Autre
Transactions électroniques	CEDEAO : Acte-additionnel-A-SA.2-01-10 du 16 février 2010 portant transactions électroniques dans l'espace CEDEAO	Supranational
	LOI n° 2008-08 du 25 janvier 2008 sur les transactions électroniques	Loi
	Décret n° 2008-719 du 30 juin 2008 relatif aux communications électroniques pris pour l'application de la loi n ° 2008-08 du 25 janvier 2008 sur les transactions électroniques	Décret
Commerce électronique	DECRET n° 2008-718 du 30 juin 2008 relatif au commerce électronique pris pour l'application de la loi n° 2008 -08 du 25 janvier 2008 sur les transactions électroniques.	Décret
Cybercriminalité	Union africaine : Convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel, Malabo 27 juin 2014	Supranational
	CEDEAO : Directive C/DIR/1/08/11 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO	Supranational
	Conseil de l'Europe : - Convention sur la cybercriminalité - convention de Budapest 23 novembre 2001 (ratifiée par le Sénégal le 16 décembre 2016)	Supranational
	LOI n° 2008-11 du 25 janvier 2008 portant sur la Cybercriminalité	Loi
Infractions numériques	LOI n° 2016-29 du 08 novembre 2016 modifiant la loi n° 65-60 du 21 juillet 1965 portant Code pénal	Loi
	LOI n° 2016-30 du 08 novembre 2016 modifiant la loi n° 65-61 du 21 juillet 1965 portant Code de procédure pénale	Loi

Cybersécurité	Convention de l'union africaine sur la cybersécurité et la protection des données à caractère personnel, Malabo 27 juin 2014	Supranational
Cryptologie	LOI n° 2008-41 du 20 août 2008 portant sur la Cryptologie	Loi
Certification	DECRET n° 2008-720 du 30 juin 2008 relatif à la certification électronique pris pour l'application de la loi n° 2008-08 du 25 janvier 2008 sur les transactions électroniques	Décret
Développement du secteur du numérique		
Droits d'auteur	Accord de Bangui du 02 mars 1977 portant création de l'organisation africaine de la propriété intellectuelle (OAPI), révisé une première fois le 24 février 1999 à Libreville	Supranational
	Accord de Bangui révisé le 14 décembre 2015 À Bamako, entré en vigueur le 14 novembre 2020	Supranational
	Loi n°2008-09 du 25 janvier 2008 portant loi sur le droit d'auteur et les droits voisins	Loi