MASTERE SPECIALISE EN REGULATION NUMERIQUE
(MS REGNUM) PROMOTION 2016

Sujet : Mise en place de Systèmes Nationaux d'Identité Digitale (SNID) : Quels sont les fondements essentiels à prendre en compte par les pays africains pour en tirer avantage tout en se prémunissant contre les risques y afférents ?

Samatar OMAR ELMI
Chargé de Projets TIC
à la Banque africaine de développement (BAD)

Octobre 2018

« ***Vous ne possédez rien, en dehors des quelques centimètres cubes de votre crâne.*** **»**

George Orwell, Romancier et essayiste anglais

Auteur, entre autres, du Roman « 1984 » publié en 1949

Inventeur du concept de « *Big Brother* » (Grand frère, en français), passé, depuis, dans le langage courant, pour qualifier toute entité ou action portant atteinte aux libertés fondamentales ou à la vie privée des individus ou des populations.

REMERCIEMENTS

A mon épouse Fathia,
mes filles Sohane et Deksane
et mon fils Ahmed

Je souhaiterais tout d'abord manifester ma gratitude à mon épouse et à mes trois enfants pour la patience et la joie, sans cesse, renouvelée de me voir rentrer de missions ou du bureau malgré mes absences répétées et surtout allongées du fait de ma charge de travail (et accessoirement de formation) dantesque.

Je voudrais donc naturellement leur dédier le travail abattu dans ce rapport qui traduit, s'il en faut, l'intérêt que je porte sur le sujet fondamental de l'identité digitale depuis plusieurs années à ma famille.

Je n'oublierai pas ma famille élargie (parents, frères et sœurs) qui me procurent tant de bonheur à interagir dans les moments de vie que nous partageons, hélas et la plupart du temps, via les réseaux sociaux principalement.

Mes remerciements, les plus sincères, vont aussi aux différents intervenants du Master RegNum qui m'ont tous inspiré dans l'élaboration de ce mémoire qui est la quintessence des riches échanges et interactions que j'ai eu avec eux.

Enfin, je souhaiterais, tout particulièrement, saluer le support déterminant de Laurent Gille qui est à l'origine de ce Master et qui l'a porté avec abnégation et professionnalisme tout au long de sa carrière au sein de Télécom ParisTech. Sa connaissance du secteur du digital force vraiment le respect de tou(te)s !

AVERTISSEMENT

Ce mémoire s'inscrit dans le cadre de la formation de Mastère en Régulation Numérique (MS RegNum) que j'ai suivi au sein de Télécom ParisTech et en collaboration avec l'ARCEP du Burkina Faso sur la période 2016-2018.

Le contenu de ce mémoire n'engage ni le Groupe de la Banque africaine de développement (BAD), mon employeur, ni Télécom ParisTech. A cet effet, l'entièreté du contenu de ce document relève de la responsabilité unique et exclusive de son auteur que je suis !

TABLE DES MATIERES

I. PROBLEMATIQUE GENERALE 8

II. CONTEXTE GENERALE 9

2.1. Introduction 9

III. PRESENTATION DES CONCEPTS GENERAUX 12

3.1. Concepts généraux 12

3.2. Principes de base 12

3.3. Architecture générale 13

3.4. Prérequis d'un SNID 14

IV. QUELQUES EXEMPLES DE PAYS 15

4.1. Introduction 15

4.2. Inde 15

4.2.1. Contexte 15

4.2.2. Risques 15

4.2.3. Modèle retenu 16

4.2.4. Principales applications du système Aadhaar 16

4.2.5. Avantages 18

4.2.6. Inconvénients 19

4.3. Pérou 19

4.3.1. Introduction 19

4.3.2. Registre National de la Population et de l'Etat Civil (RNPEC) 20

4.3.3. Intégration des données d'état civil 20

4.3.4. Avantages 20

4.3.5. Inconvénients 21

4.4. Estonie 22

4.4.1. Introduction 22

4.4.2. Caractéristiques du modèle estonien 22

4.4.3. Avantages 23

4.4.4. Inconvénients 23

4.5. Royaume-Uni 24

4.5.1. Introduction 24

4.5.2. Caractéristiques du modèle anglais 24

4.5.3. Avantages 25

4.5.4. Inconvénients 26

4.6. Malawi 26

4.6.1. Introduction 26
4.6.2. Caractéristiques du Système National d'Enrôlement et d'Identification (SNEI) 26
4.6.3. Retour d'expérience 27
4.7. Principales leçons pour les pays africains 29
V. OPPORTUNITES ET DEFIS 31
5.1. Opportunités 31
5.1.1. Introduction 31
5.1.2. Inclusion financière 32
5.1.3. Accès aux services sociaux de base 32
5.1.4. Transferts sociaux 33
5.1.5. Paiements digitaux gouvernementaux 33
5.2. Défis 33
5.2.1. Gouvernance 34
5.2.2. Protection la vie privée et des données personnelles 34
5.2.3. Risques d'exclusion 35
VI. PISTES DE RELEXION 35
6.1. Questionnements 35
6.2. Quid de l'usage des attributs détenus par les opérateurs privés? 36
6.3. Enseignements tirés 36
6.4. Ecosystème favorable au SNID 39
6.5. Différents modèles de système d'identité digitale 41
6.5.1. Introduction 41
6.5.2. Pays en développement digital 42
6.5.3. Pays digitalement avancés 43
6.6. Modèles de financement et rôles du secteur privé 45
6.7. Perspectives 46
ANNEXE I: PRESENTATION DES ODD – FOCUS SUR L'OBJECTIF 16 47
ANNEXE II: RESULTATS DE L'ENQUETE D'ID4AFRICA 48

SIGLES ET ABREVIATIONS

API	Application Programming Interface /Interface de Programme d'Application
CEDEAO	Communauté économique des États de l'Afrique de l'Ouest
CEMAC	Communauté économique et monétaire de l'Afrique centrale
COMESA	Common Market for Eastern and Southern Africa
CSIRT	Computer Security for Incident Response Team / Centre d'Alerte et de Réaction aux Attaques Informatiques
DMP	Dossier Médical Personnel
EAC	East African Community
HCR	Haut-Commissariat aux Réfugiés
IMF	Institution de Mirrofinance
INPDP	Instance Nationale de Protection de Données Personnelles
KYC	Know Your Customer
MGNREGS	Mahatma Gandhi National Rural Employment Guarantee Scheme
MRZ	Machine-Readable Zone
NIP	Numéro d 'Identification Personnel
ODD	Objectifs de Développement Durable
OEV	Orphelins et Enfants Vulnérables
OTP	One Time Password
ONG	Organisation Non Gouvernementale
PKI	Public Key Infrastructure / Infrastructure à Clés Publiques
PPP	Partenariat Public-Privé
PNUD	Programme des Nations-Unies pour le Développement
QR	Quick Response
RGDP	Règlement Général sur la Protection des Données Personnelles
RNB	Registre National Biométrique
RNEC	Registre National de l'Etat civil
RNP	Registre National de la Population
RNPEC	Registre National de la Population et de l'Etat Civil
SNID	Système National d'Identité Digitale
UIDAI	Unique Identification Authority of India (Autorité indienne de l'Identification Unique)

I. PROBLEMATIQUE GENERALE

La problématique de l'identité digitale constitue de nos jours une préoccupation majeure de la communauté internationale tant pour les progrès considérables qu'elle peut sous-tendre que les préoccupations réelles en termes de violation de la vie privée, d'exclusion des franges les plus vulnérables des populations considérées, d'instrumentalisation et de manipulation politique, etc. qu'elle suscite dans nombre de sociétés à travers le monde.

Tout d'abord, il convient de noter que l'identité d'un être humain est consubstantielle avec son existence qui est elle-même constitué de l'agrégation d'un certain nombre de caractéristiques, en l'occurrence, les traits physiques et comportementaux, la filiation, la nationalité, le genre, les croyances religieuses, les acquis culturels, etc. Depuis l'origine de l'humanité, la combinaison de l'ensemble de ces facteurs compte, de manière plus ou moins déterminante, dans nos interactions avec nos communautés, notre environnement immédiat, notre écosystème élargi, etc.

Au fil de l'histoire, les humains ont mis en place des systèmes sociaux, politiques, organisationnels, etc. plus ou moins complexes qui ont fini par supplanter petit à petit les communautés restreintes, autarciques et localisées des temps anciens. De cette organisation sont nés progressivement les droits et les devoirs pour chaque individu à travers une identité légale (reconnue clairement dans le corpus juridique de l'entité concernée) et cela tout au long de sa vie (depuis sa naissance jusqu'à son décès) ainsi que les délimitations spatiales que nous connaissons aujourd'hui et qui définissent les différentes entités territoriales existantes.

Dans les sociétés de l'information actuelles, l'identité se décline de plus en plus sous une forme digitale qui repose sur une ou plusieurs caractéristiques de la personne concernée. Dans le même temps et en fonction du degré d'avancement technologique, les pays du monde ne sont guère logés à la même enseigne en matière de démocratisation de l'identité légale. Le cas le plus extrême étant les apatrides (environ 10 millions[1]) qui regroupent l'ensemble de la population qui, à travers le monde, n'a ni nationalité(s) ni Etat qui les considère comme étant ses ressortissants.

Eu égard à ce qui précède, nombre de pays du Sud dont l'Inde, le Pakistan, le Pérou, etc. se sont lancé dans la mise en place de programmes nationaux ambitieux pour fournir une identité légale à tous les résidents et/ou citoyens grâce au digital. L'exemple le plus cité étant celui de l'Inde qui a réussi à attribuer un numéro unique d'identification à plus d'un milliard de personnes en l'espace de 5-6 ans. Cela a donc permis de favoriser l'inclusion digitale, améliorer considérablement la qualité et l'efficience des services publics, diminuer drastiquement les pertes de ressources publiques, etc.

Dans le même temps, ces progrès considérables atteints en matière de développement durable grâce, entre autres, à l'identité digitale, posent aussi des problématiques et des questionnements légitimes qui peuvent largement obérés (voire annulés) les avantages notables escomptés. Et à titre d'illustration, la décision récente (courant septembre 2018) rendue par la Cour suprême indienne sur le caractère obligatoire de la détention d'un numéro d'identification national (appelé numéro « Aadhaar ») pour l'accès à des services sociaux de base notamment, rappelle combien la vigilance doit être de mise pour éviter toute source de mésusage de ce puissant outil.

[1] Source : Haut-Commissariat aux Réfugiés (HCR)

Partant de là, il convient tout d'abord d'étudier très précisément les avantages indéniables de la mise en place d'une plateforme d'identité digitale dans les différents secteurs socio-économiques d'un pays à travers la présentation des expériences de certains pays (du Sud, en particulier, en guise d'études comparatives) tout en prenant le soin de séparer les systèmes fondamental et fonctionnels.

Ensuite, je m'attèlerai à présenter les inconvénients (risques, en particulier) d'un tel système en termes de violation possible des libertés fondamentales, de la vie privée, de cybersécurité, de droit à l'information, à l'oubli, etc. Eu égard à ce qui précède, je finirai par esquisser, dans les grandes lignes, des recommandations sur la mise en place d'un SNID robuste, sécurité et efficient dans le contexte africain, de manière différenciée sur la base du degré de préparation des pays concernés.

II. CONTEXTE GENERALE

2.1. Introduction

D'emblée, il convient de noter qu'il y a plus d'un 1,1 milliards de personnes à travers le monde qui sont incapables de prouver leur identité. Parmi ces personnes, les africains représentent une bonne moitié alors que la population du continent, estimée approximativement à 1,2 milliards ne représente qu'environ 16,5% de la population mondiale.

Sans identité légale, il est pratiquement impossible les populations concernées, d'accéder à une panoplie services du quotidien dans les secteurs primordiaux suivants, entre autres :

- ✓ Services sociaux : pensions, coupons alimentaires, transferts d'argent, etc. ;
- ✓ Soins de santé (assurance maladie, vaccinations, soins maternels, etc. ;
- ✓ Education : inscriptions des enfants dans les écoles, accès aux bourses, etc.) ;
- ✓ Services financiers : ouverture d'un compte bancaire, accès aux microcrédits, micro-assurances, etc. ;
- ✓ Droits politiques et juridiques : votes, pétitions, possession de biens, droit à un héritage, etc. ;
- ✓ Migration : droit d'asile, passage de frontières en toute légalité et sécurité, etc.

Il va s'en dire que les populations africaines vulnérables (femmes, jeunes filles, réfugiés et déplacés internes, OEV, etc.) sont les premières victimes des défis susmentionnés.

A contrario, la mise en place d'un Système National d'Identité Digitale (SNID)permet, entre autres : (i) la fiabilisation définitive de l'ensemble de la chaine de valeurs des documents administratifs (carte nationale d'identité, passeport, etc.) ; (ii) l'appui décisif au système national de statistiques ; (iii) l'économie des ressources allouées, entre autres, au recensement général de la population qui n'a plus lieu d'être grâce à la disponibilité en temps réel de données démographiques de l'ensemble de la population ; (iv) l'amélioration de l'inclusion financière en vue de l'accès à des produits financiers (mobiles, en particulier) au plus grand nombre ; (v) le ciblage des programmes nationaux d'appui à certaines catégories de population (par exemple, les exploitants agricoles pour les subventions en intrants agricoles) ; (vii) la mise en œuvre d'un système national de Dossiers Médicaux Personnels (DMP), pièce maitresse de l'accès à des soins de qualité partout sur les territoires nationaux de nos pays ; (viii) le support à la modernisation de la fonction publique avec une plus grande traçabilité de l'évolution de carrières de l'ensemble des fonctionnaires, conventionnés, contractuels, etc. de l'Etat ; (ix) l'amélioration du suivi du cursus scolaire des étudiants à travers une identification aisée des diplômes, certificats, etc. grâce à l'identifiant unique susmentionnée, etc.

Tout d'abord, il convient de souligner que la capacité d'un individu à prouver son identité légale est la clé pour la participation à la vie moderne peu importe le niveau considéré (local, national, sous régional, communautaire, etc.). A cet effet, la mise en chantier de plans nationaux d'identification digitale a été amorcé par de nombreux pays du monde, en particulier africains, sous l'angle de la modernisation de toute la chaine de valeurs de l'état civil à travers la fiabilisation des données portant sur les faits (naissances, décès, mariages et divorces) relatifs à l'état des personnes et de leurs caractéristiques dans un but administratif et juridique depuis la naissance jusqu'au décès.

Dans les pays développés, les initiatives d'identification digitale sont plus guidées, en règle générale, par une demande de plus en plus forte sur la mise en place d'économies digitalisées pour optimiser le recours aux ressources publiques dans des contextes marquées des contraintes budgétaires issues des crises économiques et financières auxquels ces pays font face depuis une dizaine d'années. Dans le même temps, ces pays ont dû mettre en place un environnement de confiance permettant l'accès à des services sécurisés en ligne.

L'objectif étant d'améliorer la qualité et l'efficience des services publics à l'endroit des citoyens qui souhaitent désormais être considérés comme des clients des administrations locales et nationales avec des besoins spécifiques à prendre en compte en fonction d'un certain nombre de critères socio-économiques, en l'occurrence les catégorie socio-professionnelles, le genre, le niveau d'étude, la localisation (urbain, rural, etc.), etc.

Par ailleurs, il y a lieu de souligner que l'intérêt pour l'identification digitale se produit concomitamment avec le développement de technologies disruptives portées en Afrique par l'explosion de la téléphonie mobile et de l'accès aux réseaux sociaux, aux objets connectés et au Big data pour ne citer que ceux-là. A cet effet, de plus en plus de Gouvernements africains se sont mis à développer des stratégies numériques dont les plus avancées ont abouti à la mise en ligne de services administratifs jusque-là traités uniquement manuellement.

Or, pour que ces services puissent se développer à grande échelle et soient, dans la mesure du possible, transactionnels, il faudra au préalable s'assurer de la disponibilité des trois modules suivants : (i) e-Authentification ; (ii) e-Signature ; et (iii) e-Paiement. Bien entendu, il va s'en dire que les autres prérequis infrastructurels (Datacenter et/ou cloud public ou privé, couverture filaire et/ou mobile, plateforme d'interopérabilité, etc.) et applicatifs (portail gouvernemental, SI de l'Etat, etc.) devront être en place avant de parler de services administratifs transactionnels.

A cet effet, il faut noter qu'en ce qui concerne l'e-Paiement, les pays africains ont largement tirés avantages de la monnaie/banque électronique qui permet aujourd'hui aux populations non bancarisées d'antan de pouvoir envoyer/recevoir de l'argent grâce aux services financiers mobiles sans compter qu'il est possible d'accéder à des services beaucoup plus élaborés grâce à l'e-Banking (comptes bancaires, épargnes, assurance, microfinance, etc.). Quant à l'e-Signature, elle fait plus référence aux plateformes de certification électronique pour s'assurer de l'authenticité, la confidentialité, l'intégrité et la non-répudiation des transactions électroniques.

Pour ce qui est de l'e-Authenticité, il faut noter qu'elle passe par un système d'identité digitale qui est lui-même basé sur un ensemble d'attributs (numéro d'identification national unique, données biométriques, etc.) permettant d'identifier clairement une personne afin qu'elle puisse émettre une requête quelconque et puisse être servi ensuite en retour. Pour ce faire, il est absolument primordial pour les pays intéressés, et en particulier africains, de mettre en place

des stratégies claires de développement de systèmes d'identification digitale sécurisés, robustes et fiables. Eu égard à ce qui précède, les pays africains se situent à des degrés différents d'avancement en fonction les quelques critères d'évaluation suivants : (i) couverture, (ii) robustesse, (iii) intégration, et (iv) usage.

Ainsi, l'on peut classifier les pays africains selon les trois catégories suivants :

1. Pays relativement avancés : ils se distinguent par le fait qu'ils disposent déjà de systèmes digitaux suffisamment opérationnels pour sous-tendre l'éclosion d'une économie (industrie) numérique. Néanmoins, même ces pays nécessitent quelques appuis ciblés en termes de couverture, d'intégration avec toutes les entités publiques et des aspects liés à la protection des données personnelles qui restent généralement perfectibles, notamment, du point de vue du Règlement Général sur la Protection des Données Personnelles (RGDP) de l'Union Européenne qui est entré en vigueur depuis mai 2018 dans l'espace communautaire.
2. Pays intermédiaires : ils nécessitent des appuis plus consistants sur l'ensemble des critères susmentionnés.
3. Pays les moins avancés : ils sont suffisamment nombreux pour justifier, à eux seuls, la nécessité de la mise sur pied et de la réalisation d'un large appui concerté des bailleurs de fonds bilatéraux et multilatéraux sur la promotion de l'identité digitale.

Par ailleurs, le ralentissement économique observé dans la plupart des pays africains ces dernières années et couplé avec les difficultés économiques liées à la baisse des prix des matières premières a mis sérieusement en difficulté nombre de gouvernements africains qui n'ont eu d'autres options que le retour à l'austérité budgétaire. La cohésion sociale s'en trouve impacter négativement dans ces pays. Ce qui pourrait conduire à des cycles d'instabilité socio-politiques plus ou moins marqués.

Or, tous les bailleurs internationaux préconisent depuis des décennies des programmes de diversification des économies africaines pour se soustraire définitivement à ces chocs exogènes récurrents. Par ailleurs, il y a lieu de souligner qu'en dépit de son dynamisme, le secteur des TIC ne représentent, en règle général, qu'environ 5 % des PIB des pays africains alors que ce ratio peut grimper jusqu'à 15-20% très rapidement pour peu que les fondements infrastructurels et applicatifs ainsi que l'environnement favorable soient mis en place.

Il faut rajouter à cela les défis réels posés par la problématique du terrorisme dans nombre de contrées du continent (Sahel, Afrique de l'Est et du Nord, etc.) ainsi que la migration illégale (notamment vers l'Europe). Tous ces facteurs nécessitent donc une réponse énergique des Etats africains avec l'appui de la communauté internationale pour trouver des solutions pérennes afin de permettre aux populations africaines d'avoir des conditions de vie décentes dans leurs pays grâce à l'économie digitale, en particulier, eu égard aux atouts dont ils disposent à travers la jeunesse de leurs poppulations.

Et cela passe notamment par une amélioration sensible de la gouvernance des services publics et privés afin d'utiliser à bon escient et de manière efficiente les deniers publiques. Par conséquent, les technologies digitales (biométrie, cloud, téléphonie mobile, etc.), accompagné d'un écosystème favorable, présentent les trois principaux avantages suivants : (i) Innovation ; (ii) Efficience ; et (iii) Inclusion. A contrario (sans écosystème favorable), elles sont susceptibles de générer plutôt les risques suivants : (i) Concentration, (ii) Inégalité ; et (iii) Contrôle.

III. PRESENTATION DES CONCEPTS GENERAUX

3.1. Concepts généraux

Tout d'abord, il convient de souligner qu'une identité est un ensemble d'attributs qui permet d'identifier de façon unique un individu (personne physique) ou une entité (personne morale). Cette identification peut se faire soit à travers les supports physiques traditionnels (actes officiels, cartes d'identité, etc.), physiques et digitaux à la fois (cartes électronique, biométrique, etc.) ou complètement digitaux (intégrée dans la carte SIM, par exemple).
Par conséquent, le Système National d'Identité Digitale (SNID) constitue l'ensemble des outils digitaux utilisés pour identifier et authentifier une personne physique.

Partant de là, il convient de souligner, d'emblée, que certains pays ont associés dans leurs systèmes nationaux d'identification les statuts de citoyenneté et de résidence, à l'instar du Pérou et du Malawi qui sont étudiés dans la suite de ce document. D'autres, au contraire, ont souhaité dissocié les concepts d'identification et de citoyenneté en se focalisant uniquement le critère de résidence. C'est le cas de l'Inde qui, à travers son système Aadhaar, a réussi, en l'espace de quelques années à enrôler 1,2 milliards de personnes essentiellement pour servir de base à la fiabilisation de la fourniture des services publics et privés, comme étudié également plus loin dans le document.
A ce sujet, il convient de souligner que l'Objectif de Développement Durable n° 16.9 vise à « garantir d'ici 2030, à tous, une identité juridique, notamment grâce à l'enregistrement des naissances ». Or, cela introduit immanquablement le concept de citoyenneté en application du droit du sol.

Une fois en place, les systèmes nationaux d'identification servent à de nombreuses applications dont la plus utilisée reste sans doute l'authentification. En effet, la difficulté primaire de toute fourniture de service est liée à la précision du ciblage du ou des bénéficiaire(s) réel(s). L'importance de cette exigence est d'ailleurs fonction de la masse critique des bénéficiaires potentiels, de la fréquence et des ressources (notamment financières) requises. Ainsi, grâce à ce mécanisme, il devient possible pour les Gouvernements des pays concernés de s'attaquer à la fois aux détournements de grande ampleur mais aussi aux phénomènes de capture de moindre envergure mais plus insidieux qui, cumulés et répétitifs, donnent les mêmes effets.

3.2. Principes de base

Compte de l'engagement de la communauté internationale pour fournir une identité légale à tous, comprenant l'enregistrement des naissances (ODD n°16.9), plus d'une dizaine d'organisations internationales (UNICEF, PNUD, Fondation Bill & Melinda Gates, Banque mondiale, Banque africaine de développement, etc.) ont élaboré et adopté en 2017 les dix principes généraux suivants sur l'identification pour un développement durable[2] :

- ✓ ***Inclusion : Couverture universelle et accessibilité***
  - *Assurer la couverture universelle des personnes de la naissance à la mort, sans discrimination ; et*
  - *Supprimer les obstacles à l'accès et à l'utilisation et les disparités dans la disponibilité de l'information et de la technologie.*
- ✓ ***Architecture robuste, sécurisée, souple et durable***
  - *Etablissement d'une identité solide, unique, sécurisée et précise ;*

[2] http://pubdocs.worldbank.org/en/199991509656714948/web-French-ID4D-IdentificationPrinciples.pdf

- *Création d'une plateforme interopérable et qui répond aux besoins des différents utilisateurs ;*
- *Utilisation de normes ouverte et neutralité du fournisseur et de la technologie ;*
- *Protection de la vie privée et du contrôle des utilisateurs grâce à la conception du système ; et*
- *Planification de la viabilité financière et opérationnelle sans compromettre l'accessibilité.*

✓ ***Gouvernance : Bâtir la confiance tout en protégeant la vie privée et les droits des utilisateurs***

- *Protection de la confidentialité des données, de la sécurité, et des droits des utilisateurs grâce à un cadre juridique et réglementaire profond ;*
- *Mise en place de mandats institutionnels et de responsabilités clairs ; et*
- *Application d'un cadre juridique de confiance à travers un système de surveillance et de traitement des griefs indépendant.*

Compte tenu de l'intérêt grandissant des pays, des partenaires au développement (bailleurs de fonds, organisations régionales et intergouvernementales, ONG, etc.) et des entreprises privées, il est apparu évident de travailler dans le sens d'une compréhension commune de la problématique de l'identification dans les pays en développement pour définir les meilleurs moyens d'y parvenir à travers une vision holistique et concertée.

3.3. Architecture générale

Tout d'abord, il convient de distinguer les deux types de SNID :

✓ Fondamental : il s'agit du cœur du système qui permet l'identification et l'authentification des résidents et éventuellement des citoyens suivants le schéma adopté (prise en considération simultanée de la citoyenneté et de la résidence ou pas).

✓ Fonctionnel : il regroupe l'ensemble des applications du SNID fondamental et qui concerne un domaine d'activité précis (fichier électoral, permis de conduire, passeport, etc.).

Ainsi le SNID fondamental ne vise pas à fournir un service spécifique mais sert plutôt aux systèmes fonctionnels de pouvoir le faire dans des secteurs bien identifiés.

Avant tout, le SNID fondamental est construit généralement autour du Registre National de la Population (RNP). Celui-ci constitue le creuset des données démographiques de la population. L'unicité des données personnelles enregistrées est basé un Numéro d'Identification Personnel (NIP) unique. Dans le cas où les statuts de résidence et de citoyenneté sont couverts en même temps, le RNP est complété par le Registre National de l'Etat-Civil (RNEC). En plus des populations disposant d'un extrait de naissance du pays concerné (citoyens ou pas d'ailleurs) qui devront être référencé dans le RNEC, le RNP intègre l'ensemble des populations en situation régulière dans celui-ci. Dans un pays donné, les principales catégories de personnes inscrites dans le RNP sont les suivantes :

(i) Citoyen vivant en permanence dans le pays ;
(ii) Citoyen vivant à l'étranger et inscrit dans le RNP à travers les représentations diplomatiques ou consulaires du pays à l'étranger ;
(iii) Etranger en situation régulière dans le pays (résidents, réfugiés, etc.).

Il y a lieu de rajouter à cela le Registre National Biométrique (RNB) dans les pays utilisant la biométrie comme moyen d'authentification. Ce registre est le troisième pilier du triptyque de l'identité digitale et doit être complètement séparé des précédents afin d'assurer la sécurité des données et éviter les risques réelles liées à la protection des données personnelles.

Afin d'assurer une cohérence et une interopérabilité de ce triptyque, il est essentiel de disposer d'un Numéro d'Identification Personnel (NIP). Ce numéro garantit l'unicité des données enregistrées dans les trois registres susmentionnés tout en étant le principal moyen (couplé avec des données biométriques plus ou moins élaborées) pour fiabiliser les procédures d'authentification d'un requérant d'un service, d'un droit (civique, notamment), etc.
Afin d'assurer une interopérabilité de ces trois registres entre aux mais aussi avec les autres SI (publics ou pas) autorisés, il y a lieu de souligner l'importance d'une plateforme d'interopérabilité, support de l'administration électronique.

Pour assurer le lien avec les opérateurs privés, il s'avère nécessaire de développer des interfaces de programmation d'applications (API) qui leur permettent de pouvoir s'interfacer avec les différentes composantes du SNID afin de pouvoir authentifier les requérants des services publics à l'instar du système « GOV.UK Verify » du Royaume-Uni qui est présenté dans la suite du document.

3.4. Prérequis d'un SNID

Avant de lancer un projet de mise en place d'un SNID dans un pays, il est primordial d'analyser l'existant technologique, organisationnelle, institutionnelle, juridique, légale, etc. dans lequel s'inscrit cette démarche.

Sur la base du retour d'expérience de plusieurs pays qui ont expérimentés la réalisation de SNID, les prérequis incontournables sont les suivants pour éviter un renchérissement des coûts du projet (voire son échec) :

- ✓ Inscrire la démarche d'identité digitale (fondamentale et fonctionnelle) dans le cadre du plan national de développement et des plans stratégiques sectoriels (santé, éducation, agriculture, secteur financier, etc.) du pays concerné aux fins de la contribution de chaque secteur à son niveau.
- ✓ Définir les rôles et responsabilités de chacun afin de chaque partie prenante nationale en vue de la création d'une entité (de type Autorité Autonome Indépendante) qui devra assurer la gestion, la maintenance et l'évolutivité du SNID fondamental, au moins.
- ✓ Inscrire le SNID dans une stratégie plus globale d'administration communicante qui lui assure un ancrage institutionnel (collaboration entre les entités en charge du SNID et de l'administration électronique) et technologique renforcé à travers la mise en place d'infrastructures digitales mutualisées (connectivité nationale, centre de données, supports de formation, communication, etc.).
- ✓ Anticiper la mise en place des applications fonctionnelles, en privilégiant les « quick-wins » afin de favoriser l'adoption de l'identité digitale par l'usage.
- ✓ Adopter une démarche intégrée permettant de faciliter la mise en place d'un écosystème nationale favorable à la mise à profit de l'identité digitale par les entreprises, l'administration et les individus.

Partant de là, il faudra élaborer une vision claire couplée avec un plan directeur donnant les grandes orientations à suivre avec en ligne de mire la généralisation de l'usage de l'identité digitale. Pour ce faire, le troisième élément de la stratégie nationale d'identité consiste à identifier et étudier dans les détails (technique, économique, financière, etc.) les projets prioritaires avec une description précise des activités à réaliser, les moyens requis, les délais d'exécution, les risques et les mesures d'atténuation, etc.

IV. QUELQUES EXEMPLES DE PAYS

4.1. Introduction

De par le monde, il y a plusieurs modèles de systèmes d'identité digitale qui chacun semble être adapté au pays considérée. Sans doute, en raison de son ampleur, de ses finalités (preuve de résidence sans autres considérations), son montage innovant et la simplicité de ses applications, le système Aadhaar occupe une place à part dans ce paysage. D'ailleurs, les contraintes liées à l'analphabétisme qu'a du géré l'Inde à travers ce système sont assez instructifs pour le continent africain.

Toutefois, celui-ci est loin d'être la panacée surtout par rapport à l'évacuation de la problématique de la citoyenneté qui, malgré son caractère controversé et souvent sources de tensions socio-politiques sur le continent, doit être traité dans le cadre du large agenda de fourniture d'une identité légale à toute personne d'ici 2030 (ODD n° 16.9). Partant de là, il s'avère donc nécessaire de passer en revue quelques-uns des systèmes d'identité digitale les plus cités afin de tirer quelques leçons globales pour le continent africain et qui seront utiles pour toute action nationale, régionale et continentale dans ce domaine.

4.2. Inde

4.2.1. Contexte

Le principal objectif du projet d'identité digitale, connue sous le nom d'« Aadhaar », est de fournir à tout résident en Inde d'une identité unique à travers une plateforme digitale pour authentifier à tout moment et en tout lieu.

Pour ce faire, le Gouvernement a mis en place en 2009 l'Autorité indienne de l'Identification Unique (UIDAI). Celle-ci est placée sous la tutelle du Ministère de l'Electronique et des Technologies de l'information. Ce système garantit l'unicité des identités grâce aux attributs biométriques (empreintes digitales/iris) des personnes enregistrées. Le système couvre pratiquement 100% des personnes résidentes en Inde. Il propose principalement des services d'authentification et d'e-KYC. La plate-forme d'authentification en ligne est capable de traiter 100 millions de requêtes par jour.

Plutôt que d'engager des milliers de personnes et de créer une infrastructure entièrement publique, l'UIDAI a décidé de faire appel à des tiers aux fins de l'enrôlement des résidents. Le premier numéro Aadhaar a été attribué en septembre 2010 dans le village de Tembhili, dans le district de Nandurbar situé dans l'Etat du Maharashtra. À ce jour, plus d'un milliard de personnes ont été enregistrées (dont environ les deux tiers par des entreprises privées).

Afin de favoriser la diffusion généralisée du système Aadhaar, le Gouvernement indien a décidé de lier le NIP à la fourniture de nombre de services publics et privés (subsides de l'Etat, ouverture d'un compte bancaire, obtention d'une carte SIM, etc.) L'objectif étant de connecter de plus en plus de services à la détention dudit numéro.

4.2.2. Risques

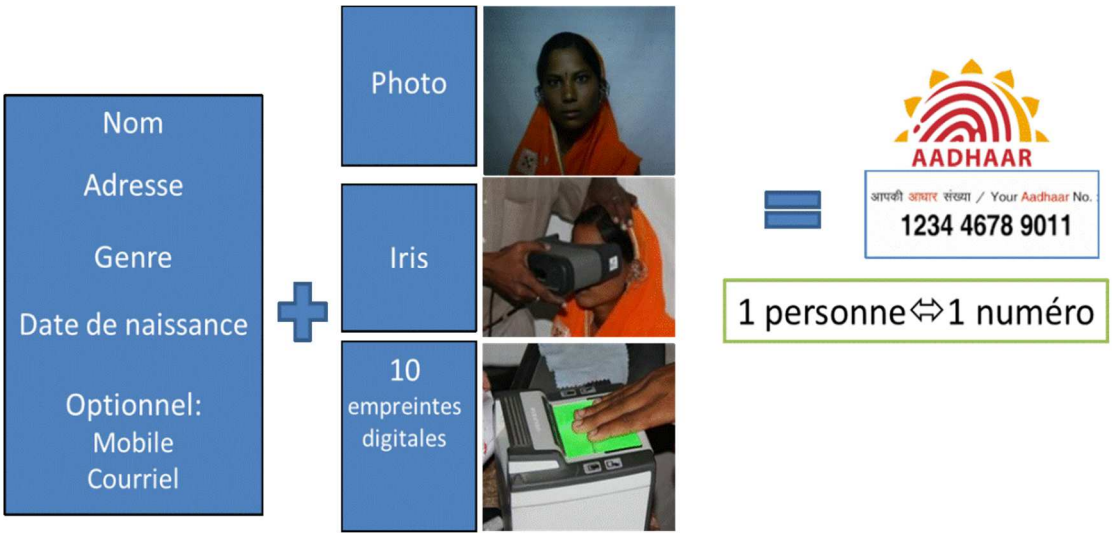
Bien que le Pakistan l'ait devancé sur ce domaine, l'Inde s'est lancée en 2009 dans son programme d'identité digitale (Aadhaar) sans précédent du fait de la taille de sa population. Par conséquent, les risques encourus étaient tout aussi considérables. L'on peut citer, entre autres :

(i) les difficultés liées au nombre considérable de personnes à enrôler qui risquait d'hypothéquer l'opération ; (ii) le support politique escompté à la fois du gouvernement central que des gouvernements locaux ; (iii) le nombre de points d'enrôlement surtout dans le milieu rural ; (iv) la capacité de stockage des données relatives à plus d'un milliard d'individus ; (v) les risques technologiques liées à l'obsolescence des infrastructures utilisées ; (vi) les violations de la vie privée et des données personnelles, etc.

4.2.3. Modèle retenu

Eu égard à ce qui précède, les Autorités indiennes ont adopté la démarche suivante par rapport au système Aadhaar :

4 données démographiques + biométriques = un unique numéro Aadhaar



Pour ce faire, le système Aadhaar a les caractéristiques suivantes :

- ✓ Attributs d'identité standardisés ;
- ✓ Pas de duplication (vérification auprès de la base de données disponible) ;
- ✓ Nombre minimum de données démographiques collectées.

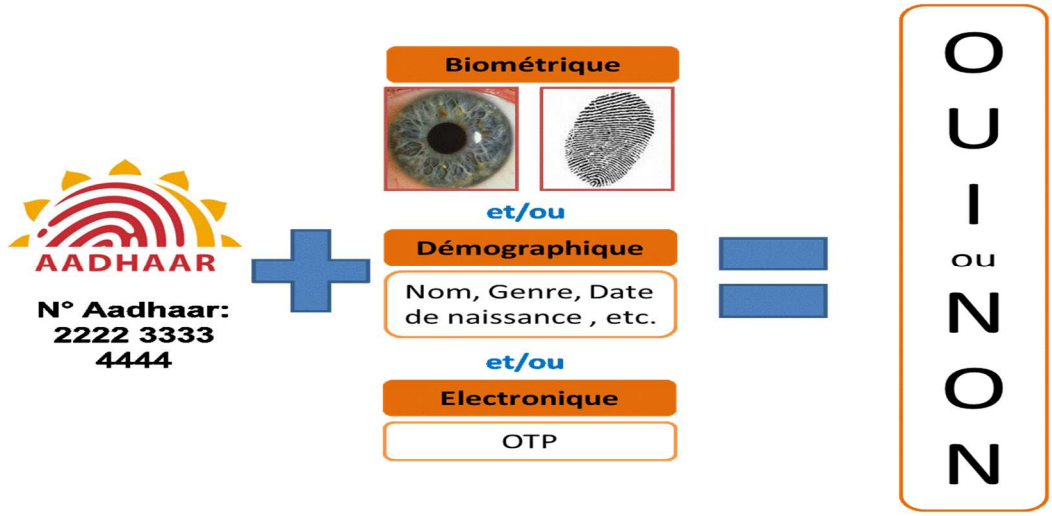
Le système enregistre les données démographiques et biométriques dans deux bases de données séparées. Tous les détails (démographiques, biométriques et photo) peuvent être mis à jour la personne concernée par différents canaux de communication (poste et en ligne).

En résumé, le système Aadhaar est donc une plateforme robuste d'identité digitale qui permet de fiabiliser l'ensemble des services publics et privés et de favoriser considérablement l'inclusion sociale à travers la réduction drastique (voire l'annulation) des facteurs d'exclusion sociales (castes, en particulier, niveau de revenus, etc.).

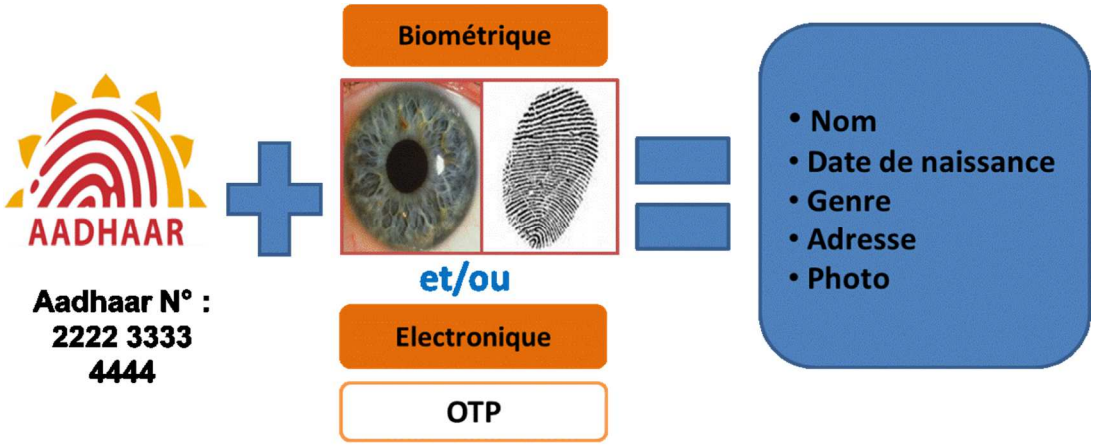
4.2.4. Principales applications du système Aadhaar

Afin d'éviter les risques liés à une complexité du système, les Autorités indiennes ont privilégié une approche simplifiée et pragmatique qui se base sur quelques applications usuelles. Il convient aussi de rappeler que l'unicité des individus est assurée grâce à la combinaison des données biométriques et un numéro à vie composée de 12 digits.

Parmi ces applications, l'on peut citer :
Authentification : cette opération consiste à confirmer l'identité d'une personne au moyen de plusieurs attributs propres (données biométriques (empreintes digitales et/ou iris), démographiques, OTP, etc.).



e-KYC : cette plateforme permet la vérification électronique des identités et des adresses grâce aux attributs des personnes enregistrées. Ce service est particulièrement demandé par les institutions financières (banques commerciales, IMF, etc.) pour s'assurer des identités et des adresses de leurs clients, par exemple. Il convient de noter que l'Inde a mis en place en place la NPCI (National Payments Corporation of India), organisation à but non lucratif formé par les principales banques commerciales sous la supervision de la Banque centrale indienne, qui permet, entre autres, de faire le lien entre les différents comptes bancaires (y compris du même titulaire) grâce au numéro Aadhaar.



Distribution des subsides de l'Etat : Compte tenu des besoins importants en aide alimentaire de l'Etat pour réduire les effets de la pauvreté et de la précarité, le Gouvernement indien a lié au numéro Aadhaar aux différents programmes d'aide sociaux du pays dont les coûts sont estimés à 60 milliards de dollars EU chaque année. Le système Aadhaar a permis de réduire considérablement les phénomènes de capture sur cette énorme manne sachant qu'il a été prouvé par exemple à travers des études détaillées qu'en 2008 (avant l'installation du système) qu'environ 40% des quantités de céréale dévolues aux pauvres n'arrivaient jamais chez leurs destinataires et que plus de la moitié des quantités distribués finissaient dans des circuits de revente.

Programme d'emplois aidés : il s'agit d'un programme dénommé, MGNREGS (Mahatma Gandhi National Rural Employment Gurantee Scheme), qui garantit un salaire pour 100 jours à l'année en contrepartie de travaux ne nécessitant pas de compétences spécifiques. Grace à la liaison établie entre le numéro Aadhaar, le numéro de compte bancaire basique (connu sous le nom de « Jhan Dan ») et le numéro de téléphone (trinité JAM (Jhan Dan, Aadhaar et Mobile)), plus de 200 millions de compte nouveaux ont été ouverts au profit des plus pauvres pour favoriser l'inclusion financière au moyen des paiements des pensions, des aides de l'Etat, des bourses, etc.

A l'instar des principales applications susmentionnées, le système Aadhaar est utilisé avec plus de 500 services aux usagers dont le contrôle de la présence des employés de l'Etat, le paiement des taxes et droits de douane, etc. Afin d'améliorer continuellement sa qualité, chaque enregistrement comprend les données démographiques et biométriques. De plus, les informations sur la qualité de l'enregistrement sont également transmises à un centre d'analyse qui permet de s'assurer de la qualité du processus d'enrôlement par rapport aux standards établis.

4.2.5. Avantages

Les avantages du système Aadhaar sont les suivants :

- ✓ Simplicité des données collectées.
- ✓ Large éventail de documents utilisés (preuve de résidence ou d'identité) pour l'enrôlement avec en dernier recours l'intervention d'une personne respectée au sein de la communauté et dont le témoignage pouvant faire foi.
- ✓ Rapidité de mise en œuvre (1 milliards d'enregistrement en 5 ans, mieux que Facebook qui a été le même chiffre en huit ans) avec plus de 90% de la population couverte jusqu'à date.
- ✓ Utilisation dans nombre de services de l'Etat avec des rendements considérables par rapport aux investissements initiaux consentis.
- ✓ Système convenant à une population largement analphabète sachant que le processus d'enrôlement et d'authentification est basé uniquement sur des attributs physiques (empreintes digitales.
- ✓ Montage innovant dans la collecte des données à travers un partenariat de l'Etat avec des opérateurs privés qui a abouti à un coup par enrôlement de 1,16 dollars EU par personne alors que les mêmes coûts culminent à plus de 2 dollars EU pour les opérateurs télécoms dans le cadre des campagnes d'identification des abonnés en Afrique.
- ✓ Mise en place d'une certification et de standards stricts qui permettent de s'assurer d'une qualité optimale des outils technologiques utilisées (notamment pour l'enrôlement et l'authentification) afin de réduire au maximum le taux d'échec.

4.2.6. Inconvénients

Les inconvénients de ce système sont les suivants :

- ✓ Système servant uniquement à l'identification et ne constituant pas une preuve pour autre chose (nationalité, situation matrimoniale, localisation, etc.) ;
- ✓ Cadre juridique n'ayant pas permis depuis le début la séparation des données sensibles (biométriques, en particulier) des autres plutôt liés à la démographie ainsi que le NIP lui-même ;
- ✓ Risques liés aux pannes qui peuvent stopper l'utilisation du système du fait de la centralisation des données biométriques servant à l'authentification ;
- ✓ Gestion non prise en compte jusqu'à présent des enfants (et des nourrissons) pour couvrir les programmes destinés à l'enfance et la petite enfance (transferts sociaux pour les enfants, subventions pour les frais de scolarité des enfants, etc.) ;
- ✓ Pas d'exit du système en cas de décès ; et
- ✓ Enregistrement non filtré (y compris pour les criminels, terroristes, etc.) sous une fausse identité.

Par ailleurs, il convient de souligner que la Cour suprême indienne a rendu un jugement historique fin septembre 2018 sur les problématiques relatives aux usages et aux périmètres du système Aadhaar suite à de nombreuses plaintes, préoccupations et pétitions exprimées à travers le pays. Ainsi, elle a d'abord estimé que celui-ci n'est pas à remettre en cause. Par ailleurs, la Cour a reconnu au Gouvernement indien le droit d'imposer l'obtention du numéro Aadhaar pour obtenir certains services publics qui ont pour objectif de distribuer les subventions et autres subsides de l'Etat. Par contre, elle s'est clairement prononcé contre l'obligation faite aux utilisateurs d'avoir un numéro Aadhaar pour ouvrir un compte bancaire ou avoir une ligne de téléphonie mobile. D'une manière générale, interdiction a été faite aux opérateurs privés d'exiger un numéro Aadhaar pour les services proposés. Par ailleurs, les bénéficiaires ne pourront plus se voir contester les services demandés en cas de panne de l'authentification biométrique. Tout cela permet donc de limiter au maximum les phénomènes d'exclusion, y compris technologiques. Par ailleurs, la décision de la Cour consacre le principe de « proportionnalité » entre les usages faits du système Aadhaar et la nécessité de préserver la vie privée et la protection des données personnelles des personnes.

4.3. Pérou

4.3.1. Introduction

Le système d'identification péruvien est né d'une ferme volonté politique depuis l'avènement de la démocratie au tournant des années 2000 dans ce pays après des décennies de violence et d'instabilité. Le système est basé sur un registre national de la population qui permet la génération d'un document national d'identité avec un NIP. Ce registre intègre toute la population et permet donc une authentification en temps réel sur la base de la présentation du document d'identité national.

L'autre grande caractéristique du SNID péruvien réside dans le fait que le NIP (attribué à la naissance) se retrouve sur tous les documents administratifs. Ce NIP permet donc d'authentifier les personnes à travers tous les registres publics ainsi que les usages commerciaux (e-KYC notamment).

4.3.2. Registre National de la Population et de l'Etat Civil (RNPEC)

Le Gouvernement péruvien a décidé de commencer en 1993 avec la création d'un RNP qui a ensuite été complété avec un RNEC en 1995 pour aboutir au RNPEC. Contrairement au modèle indien, le Pérou a donc mutualisé les efforts pour mettre en place une base de données centralisée aux fins de l'identification de l'entièreté de la population (résidents et citoyens).

Malgré des débuts lents, le RNPEC comprend aujourd'hui les attributs de pratiquement 100% de la population (jeunes et adultes). Le succès de cette opération étant certainement dû au mode de gouvernance mis en place. En effet, les Autorités péruviennes ont mis en place une agence autonome (type AAI, en France) pour gérer tout le processus d'enrôlement avec des interférences limitées des organes publics en charge des systèmes d'identité fonctionnels (passeport, protection sociale, santé, éducation, etc.).

L'autonomie financière de cette Agence est, en grande partie, assurée par les frais générés par les services qu'elle rend aux usagers qu'ils soient publics ou privés (authentification dans le cadre des processus d'e-KYC, d'actes notariaux, etc.). Le reste de son budget émane de l'Etat à travers des subsides votés annuellement par le parlement dans le cadre de la loi de finance afin de réduire les coûts d'accès des services pour les populations les plus pauvres et/ou isolées géographiquement. D'ailleurs, il convient de souligner que les coûts réels d'enrôlement et d'établissement du document d'identité nationale est d'environ 10 Dollars EU dans les zones urbaines et que ce coûts peut grimper jusqu'à 80 Dollars EU dans les zones les plus reculées.

4.3.3. Intégration des données d'état civil

Comme indiqué plus haut, le Gouvernement péruvien s'est d'abord lancé dans un vaste programme d'identification des personnes résidentes. Par la suite et compte tenu du succès de celui-ci, l'Agence en charge du registre national de la population s'est vu confier la responsabilité d'incorporer aussi dans sa base de données les attributs d'état civil qui relevait auparavant des administrations locales. Or, celles-ci, généralement sous-équipées et peu performantes, n'étaient pas capables d'assurer le travail d'enrôlement quotidien au moyen de registres papiers décentralisés.

Par conséquent, l'Agence s'est dans un premier temps lancé dans un processus d'enrôlement et de reprise des antériorités sans coordination avec les administrations locales. Ce fut un échec. Par la suite, elle a dû changé de stratégie grâce à un appui énergique du Ministère des Finances qui a fini par conditionner les transferts de fonds aux administrations locales sur la base des documents d'état civil transmis. De plus, l'Agence a mis en place une structure en charge de la coordination des activités liées à l'état civil en collaboration avec les administrations locales à travers des programmes de renforcement des capacités de celles-ci afin qu'elles puissent être pleinement outillées. Cette nouvelle stratégie a abouti à la mise en place d'un RNPEC robuste et centralisée qui permet de réunir sous une seule entité l'entièreté du SNID fondamental du Pérou.

4.3.4. Avantages

Indiscutablement, le modèle péruvien d'identité digitale se distingue par son caractère innovant alliant, pratiquement depuis le début, le RNP et le RNEC dans le cadre d'une base de données nationale unifiée (RNPEC). Cela permet de s'affranchir de l'écueil de la solution « de facilité »

consistant à ne se préoccuper que des résidents dans le pays en se focalisant sur les applications fonctionnelles d'un tel système.

L'autre spécificité majeure de ce modèle réside dans le mode de gouvernance qui a été choisi notamment à travers l'autonomie, la clarté des missions assignées et la maitrise technique de l'Agence nationale chargée de la gestion du RNPEC.
Par ailleurs, le cadre de collaboration établi au niveau national avec les administrations locales a permis de fiabiliser toute la chaine de valeur des documents d'état civil avec des données complètes et désormais transmises, en temps réel, par les différents points d'enrôlement (maternités, municipalités, etc.) dépendant d'autres organismes partenaires.

A cet effet, l'attribution du NIP se fait désormais automatiquement et dès la naissance ; ce qui permet de générer pratiquement instantanément le document d'identité nationale ainsi que tous les autres documents administratifs en découlant (acte de naissance et plus tard carte d'identité nationale, passeport, permis de conduire, etc.).

Par ailleurs, il convient de souligner que le premier document d'identité nationale est gratuit afin de réduire la barrière d'accès à celui-ci pour les plus précaires. Pour atténuer les risques d'exclusion géographique, des équipes mobiles d'enrôlement ont été constitués à l'endroit des zones reculées pour assurer la couverture du couteux « last mile ». Afin de maintenir la dynamique, le Gouvernement péruvien a décidé progressivement de lier la fourniture de la majeure partie des services publics avec l'obtention du NIP.

4.3.5. Inconvénients

Compte tenu de la limitation de l'utilisation de la biométrie, l'authentification se faisait jusqu'à récemment grâce à la photo qui est apposée sur le carte d'identité. Toutefois, cela est en train de changer puisqu'il a été décidé de mettre en place une carte d'identité biométrique qui va stocker les empreintes digitales des porteurs. Cela permettra donc de demander des services en ligne grâce à la plateforme de certification électronique.

Les mesures incitatives adoptées par le Gouvernement pour faciliter l'accès au système ont permis d'illustrer les effets pervers éventuels. En effet, en 2012, les Autorités ont lancé un programme d'assurance gratuite qui était conditionné par la détention d'un document d'identification d'un enfant pour les familles concernées.

Cela a pour conséquence une réduction drastique des déclarations des nouveau-nés dans les communautés les plus pauvres. Ceci démontre donc que le gap de communication en amont est assez désastreux ensuite sur la perception du SNID pour les populations peu ou pas éduqué. Par la suite, le Gouvernement péruvien a dû rectifier le tir.

En outre, la concentration de tous les attributs permettant d'identifier directement ou indirectement des personnes au sein d'un seul organisme pose clairement des défis réels en matière de protection de la vie privée et des données personnelles.

4.4. Estonie

4.4.1. Introduction

Au début des années 2000, l'Estonie s'est lancé dans un ambitieux programme d'administration électronique qui avait pour objectif de rapprocher les citoyens de leurs administrations locales et centrales et améliorer l'efficience et la performance des services publics en éliminant les coûts superflus dus au mode de fonctionnement papier traditionnel hérité de l'époque soviétique.

Pour ce faire, l'Estonie a lancé depuis 2002 le SNID le plus complet et le plus abouti en termes de couverture et de services fournis aux utilisateurs au monde. En effet, celui-ci propose aujourd'hui plus de 2.600 services en ligne pour les usagers de l'administration. Ce système se distingue par l'utilisation d'une carte électronique à laquelle est associé un code unique personnel constitué de 11 digits.

En termes de gestion données, le système comprend une base de données centralisées qui contient l'ensemble des attributs des résidents en Estonie avec le code unique personnel précité. Toutefois, ces attributs sont limités au strict minimum en conformité avec le respect du cadre de protection des données personnelles, à savoir : (i) Nom et prénom ; (ii) Date de naissance ; (iii) Genre ; (iv) Adresse ; (v) Citoyenneté ; et (vi) Relations légalement reconnues.
Chaque personne enregistrée se voit également automatiquement attribuée une adresse électronique. Sur cette base, les opérateurs publics et privés sont autorisés à utiliser le SNID mis en place pour identifier et authentifier les utilisateurs pour les services proposés qui sont pratiquement exhaustifs, à l'exception de quelques cas précis demandant la présence physique du requérant.

4.4.2. Caractéristiques du modèle estonien

En plus d'être pionnier dans l'identité digitale, l'Estonie a adopté une approche progressive pour diffuser le SNID. En effet, le Gouvernement estonien n'a généralisé l'usage du SNID qu'au bout de cinq ans après son lancement avec la mise en ligne des 75 services publics les plus utilisés. Cela souligne donc l'importance de l'usage dans l'adoption et l'appropriation d'une technologie aussi disruptive à la fois pour les administrations et les administrés.

Pour ce qui est de l'enrôlement, le SNID estonien se base sur les données biométriques (dix empreintes digitales et reconnaissance faciale) pour les personnes âgées de plus 15 ans. Quant à l'authentification, elle se fait plutôt sur deux certificats électroniques enregistrés sur la puce insérés dans la carte d'identité électronique et qui se basent sur: (i) un premier code PIN de quatre digits qui permet d'authentifier la personne ; et (ii) un second de cinq digits au minimum et qui sert à la signature électronique des détenteurs des cartes. Ces deux codes sont de la responsabilité exclusive des utilisateurs.
Eu égard à ce qui précède, le SNID estonien est basé sur le duo suivant : (i) la carte d'identité électronique avec les deux codes PIN qui y sont rattachés ; et (ii) la base de données contenant les attributs et les données biométriques des personnes référencées.

Par conséquent, il y a lieu de noter la séparation entre les cartes d'identité électroniques et les codes personnels associés qui restent sous la responsabilité exclusives des utilisateurs et la base des données démographiques et biométriques qui relèvent de la responsabilité de l'administration estonienne. Les utilisateurs peuvent accéder à leurs données en ligne soit à

travers des ordinateurs (au moyen d'un lecteur de la carte électronique) ou via mobile en utilisant des SIM compatibles avec le SNID.

Par ailleurs, l'Estonie a pu greffer sur le SNID un programme d'e-Résident qui permet à des personnes qui ne sont guère physiquement présents dans le pays de pouvoir appliquer à ce statut qui leur procure un certain nombre de services en ligne dont la création d'une entreprise en fournissant les éléments requis à distance.

4.4.3. Avantages

Aujourd'hui, quasiment tous les services publics sont proposés en ligne et en mode transactionnel (traitement automatique depuis la soumission de la requête jusqu'à la fourniture du service). Ces services incluent même la signature des documents, le vote électronique, consultations médicales, achat de médicaments, etc.

A ce sujet, il convient de noter que le Gouvernement estonien estime que les gains réalisés en termes de dépenses publiques évitées grâce à l'administration électronique se chiffrent à environ 2% du PIB du pays chaque année, ce qui équivaut à environ 500 millions de Dollars EU.

En termes de cybsercurité et conformément au modèle X-ROAD, l'Estonie a fait un clair distinguo entre le SNID fondamental d'une part et les applications de ce système d'autre part avec des liens uniquement sécurisés entre eux. Ce qui encadre strictement l'accès aux données des utilisateurs qui concerne principalement l'authentification des personnes. A cet effet, les utilisateurs peuvent vérifier les détenteurs des données les concernant ainsi que les motivations sous-jacentes pour limiter au strict requis les transferts et le traitement de celles-ci, à l'exception des cas relevant de la criminalité ou de la sécurité nationale.

4.4.4. Inconvénients

D'un point de vue africain (subsaharien qui plus est), il y a lieu de noter que le modèle estonien ne peut être applicable que dans un contexte d'alphabétisme élevé ainsi qu'une base technologique (connectivité, stockage, applications, etc.) suffisante. De ce fait, ce modèle ne pourrait être évoqué, à priori, que pour les pays africains qui se situent principalement en Afrique du Nord, de l'Est et australe.

D'ailleurs, l'Estonie n'a pas pu faire l'économie d'une opération de formations à l'échelle nationale pour accompagner le processus de diffusion du programme d'administration électronique au tout début et sur deux ans. Cela a permis la formation sur les TIC de 100.000 estoniens chaque année grâce un partenariat public-privé.

Malgré ses performances reconnues par tous, la plateforme d'administration électronique n'est pas à l'abri de défaillances techniques. Ainsi, suite à une faille de sécurité sur un type de puce utilisé, les cartes d'identité électroniques sont restées bloquées sur plusieurs jours en novembre 2017. Ce qui a induit l'arrêt de l'accès aux services pour environ 760.000 utilisateurs sur une population totale d'environ 1,3 millions. Cela pose donc la question du tout numérique dans des services essentiels à la population avec les conséquences potentiellement désastreuses de pannes techniques malgré leurs fréquences relativement réduites, en règle générale en raison des niveaux de disponibilité garantie élevée.

Une autre limite du modèle estonien (d'un point de vue toujours africain) concerne le fait que la base de données biométriques ne concerne que les personnes âgées de plus de 15 ans. Or, au regard des avancées technologiques récentes, il est désormais possible de recueillir les attributs biométriques des enfants jusqu'à un certain âge. Au fait, certains avancent même qu'il est possible d'étendre cela jusqu'au nouveau-né. Partant de là et considérant les programmes sociaux visant à fournir des aides ciblées aux enfants scolarisés par exemple, il serait opportun de s'enquérir des progrès réalisés dans ce domaine pour pouvoir les utiliser suite à une analyse couts/avantages précise.

4.5. Royaume-Uni

4.5.1. Introduction

Afin de permettre l'accès en ligne des utilisateurs aux services publics dans le cadre de la cadre de la Stratégie « Digital par défaut », le Gouvernement anglais a lancé une plateforme depuis 2016 dénommé « GOV.UK Verify » qui est basé sur une multitude de données détenus par le public et le privé pour les processus de vérification d'identité. Le modèle anglais est donc décentralisé et non exclusivement basé sur des attributs émanant des bases de données publiques, contrairement aux modèles indien et péruvien. L'objectif affiché étant de réduire de pratiquement 3 milliards les dépenses publiques grâce au digital.

Par ailleurs, il convient de souligner que le Royaume-Uni, pour des raisons historiques, ne disposent d'aucun document officiel dévolu à l'identification des personnes. Des démarches entreprises au milieu des années 2000 pour mettre en place une base de données centralisée a tourné court du fait d'une forte résistance invoquant le caractère intrusif de cette opération dans la vie privée et le risque de mésusage potentiel.

4.5.2. Caractéristiques du modèle anglais

Eu égard à ce qui précède, et aux fins de la mise en place du système national de vérification des personnes (GOV.UK Verify), le principal défi a consisté à pouvoir se baser sur une multitude de sources de données (publiques et privées) pour constituer un moyen d'identification fiable.

Pour ce faire, le Gouvernement a décidé de garder le rôle de source d'identification/vérification primaire à travers les différents registres qu'il détient (état civil, passeport, permis de conduire, etc.). Combinées, ces différentes sources d'identité constituent la base de l'identité fondamentale dans le pays. Le Gouvernement définit aussi les standards d'accès à ces registres et les normes guidant les processus de vérification d'identité.
Sur cette base et dans le cadre d'un Partenariat Public-Privé (PPP), le Gouvernement a passé des accords avec des sociétés privés certifiés qui peuvent collecter des preuves d'identité à la fois à travers les registres publiques et privés (banques, assurances, opérateurs mobiles, etc.). Toutefois, il convient de noter que très peu d'informations sont transmises sachant que pour l'essentiel les réponses reçues sont juste binaires (oui/non) afin de prévenir les risques liés à un mésusage des données accessibles. Une fois la vérification faite, l'utilisateur peut demander une vingtaine de services publics en ligne.
La séparation de la fonction de fourniture de services et de vérification/authentification de l'identité du requérant permet de limiter tout risque de traçage des activités de celui-ci. En effet, chacune des deux parties prenantes (publique et privée) n'a accès qu'aux informations relatives au volet qu'elle traite.

Le partenariat susmentionné prévoit aussi le paiement par l'Etat de frais de services auprès des fournisseurs d'identité privés qui, au regard de leur grand nombre, se font concurrence sur la qualité des processus employés pour faire aboutir, dans des délais extrêmement réduits, les requêtes d'authentification. En plus de l'utilisation gouvernementale de ce système d'authentification, il est aussi envisagé que les opérateurs privés puissent l'utiliser dans leurs interactions avec leurs clients, dans un cadre strictement encadré. Il revient à l'utilisateur final de choisir le fournisseur d'identité privé parmi une liste d'opérateurs privés (https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify). Pour ce faire, les utilisateurs peuvent créer un compte personnel qui leur permet, par la suite, de s'informer sur les usages faits de leur identité auprès de l'opérateur choisi.

En guise de garde-fou additionnel, le Gouvernement anglais a aussi introduit une appréciation sur la « qualité » de l'identité souhaitée afin de calibrer les vérifications demandées en fonction de la finalité poursuivie. Ainsi, il a créé quatre niveaux de qualité qui sont les suivants :

(i) *Niveau 1* : il n'y a pas besoin de prouver l'identité présenté par le requérant. Les vérifications d'usage sur la base des(s) document(s) présenté(s) suffisent.
(ii) *Niveau 2* : il est demandé au requérant de présenter des documents prouvant son identité dans le cadre d'une situation réelle (au-delà d'un document d'identité figé uniquement). Et la vérification de l'identité se fait donc sur cette base.
(iii) *Niveau 3* : Idem que le cas précédent mais avec des vérifications plus poussées (physiques notamment).
(iv) *Niveau 4* : Il s'agit du niveau de vérification le plus élevé et qui sied donc à des contextes exposant le requérant ou un groupe de personnes (ou éventuellement pour toute la population) à un danger éventuel, par exemple. L'accès à un site nucléaire dans le contexte sécuritaire actuelle en est un parfaite illustration de la pertinence de ce niveau de vérification. Ce niveau requiert donc la prise en compte d'attributs sensibles tels que la biométrie pour éviter tout risque d'usurpation d'identité, en particulier.

A titre d'illustration, le Gouvernement a décidé que la vérification pour l'accès aux services gouvernement relève du niveau 2. Ainsi, il paie 1,2 livre à chaque fois qu'un opérateur privé certifié réussit à authentifier l'identité d'un requérant. Ce taux est beaucoup plus bas pour les vérifications de niveau 1.

En termes d'assurance qualité, le système « GOV.UK Verify » doit respecter les normes définis dans le cadre des standards des services digitaux (Digital Service Standard). Ainsi, il est recommandé, entre autres, de superviser constamment les performances du système, d'utiliser des outils ouverts et communs, vérifier en ligne les usages faits de l'identité des personnes, se baser sur un nombre réduit d'attributs pour les opérations d'authentification, etc.

4.5.3. Avantages

Dans un contexte hostile à la centralisation des données personnelles, le Royaume-Uni a mis en place un système ingénieux qui permet de vérifier l'identité sur la base d'un puzzle à constituer. Cela permet donc au maximum de limiter les risques de violation de la vie privée car il est quasiment impossible de rassembler toutes les bribes de l'identité d'une personne en dehors d'un cadre très réglementé (agrément entre l'Etat et des fournisseurs d'identité privés) et de la séparation fonctionnelle entre les fournisseurs de service(s) et d'identité.

4.5.4. Inconvénients

D'un point de vue africain, le modèle anglais présente un défi majeur qui consiste à vouloir se baser sur une multitude de sources de vérification qui sont parfois de qualité discutable surtout du côté public. En effet, il n'est pas rare que, dans certains pays, les données clients constitués par les opérateurs mobiles dans le cadre de l'identification des détenteurs des cartes SIM soient beaucoup plus étoffés et exhaustifs que l'ensemble des systèmes d'identité nationaux fondamentaux et fonctionnels réunis. C'est pourquoi, il faudra d'abord mettre à niveau le SNID public avant d'envisager de mettre en place un système similaire.

4.6. Malawi

4.6.1. Introduction

Le Malawi ne disposait pas jusqu'à 2017 d'un système national d'identification des personnes, contrairement aux autres pays d'Afrique australe. Par conséquent, il a demandé l'assistance au Programme des Nations Unies pour le Développement (PNUD) avec l'aide de la coopération anglaise (UKAid/DFID), irlandaise (Irish Aid), américaine (USAID), européenne et norvégienne aux fins de la mise en place d'un SNID. Le manque de système d'identification nationale a induit des conséquences néfastes sur la qualité et la redevabilité de l'administration publique en l'absence d'un moyen efficace pour assurer l'adéquation entre la demande et la fourniture des services publics.

Parmi les difficultés auxquelles le Gouvernement malawite faisait face, l'on peut citer : (i) abus de la gratuité des soins dans le pays ; (ii) déperdition de ressources dans les systèmes de transferts sociaux, salaires, pensions, bourses, etc. ; (iii) manque de données sur les populations à risque par rapport aux catastrophes naturelles, en particulier, etc.

Avant l'assistance de cette opération, le pays ne disposait que de quelques dizaines de millier de personnes enregistrés dans les systèmes d'état civil et d'identité fonctionnels (carte d'identité, passeport, permis de conduire, etc.) sur une population totale de 18 millions. Comme souvent, à chaque élection, il investissait des sommes considérables dans la constitution des fichiers électorales jusqu'à l'élection suivante ou il faut tout reprendre.

4.6.2. Caractéristiques du Système National d'Enrôlement et d'Identification (SNEI)

La mise en œuvre du SNEI a, avant tout, tiré avantage d'une large concertation nationale qui a abouti à une vision claire, un plan d'actions précis et un résolu appui politique qui s'est matérialisé par la prise en charge de la moitié des coûts du projet (52 millions de Dollars EU) par le Malawi.

De plus, le Gouvernement malawite a fait le nécessaire pour mettre en place le cadre juridique et règlementaire à travers la « *Malawi National Registration Act* ». Celui-ci a permis, entre autres, la création du Bureau National d'Identification (BNI) qui a la charge uniquement du Registre National de la Population et Biométrique (RNPB) dont découle les documents d'identité (carte national d'identité, passeport, carte d'électeur, permis de conduire, etc.). Il exige aussi que tout malawite âgé de 16 ans ou plus doit être enregistré dans ces registres nationaux aux fins de l'obtention d'une carte d'identité nationale portant un numéro d'identifiant unique.

La perspective des revenus potentiels générés par le système a été de nature à galvaniser toutes les parties prenantes nationales qui étaient convaincues de la durabilité du modèle économique mis en place. L'intérêt s'est même propagé au-delà des secteurs publics et privés (principalement les banques, les opérateurs mobiles et les producteurs de tabac) sachant que les partenaires au développement, et en particulier les ONG, ont également vu les possibilités offertes en matière de ciblage des populations bénéficiaires dans le cadre de la réalisation de leurs projets/programmes sociaux.

4.6.3. Retour d'expérience

Sur la base du contexte susmentionné, l'expérience malawite est assez instructive sur les prérequis organisationnels dans l'optique de l'enrôlement de 9 millions environ de personnes dans le RNP sur un laps de temps très réduit. L'objectif affiché initialement était de finaliser l'enrôlement sur trois mois (1er trimestre 2017) avec une distribution finalisée des cartes d'identité nationales en juin 2018 et un système complètement opérationnelle avant la fin 2018. L'équipe projet comprenait 19 membres et l'enrôlement a été fait par 4.200 étudiants malawites. Le total du staff impliqué étant de 4.500 tout au long de l'exécution de l'opération. Au final, l'enrôlement de 9,1 millions de personnes ont été bouclées en six mois seulement (mai à novembre 2017).

Pour vaincre le scepticisme ambiant, l'équipe-projet a lancé une campagne de communication à travers les divers média locaux. Elle a également mis en place une campagne de promotion qui visait en priorité les leaders politiques, religieux, et d'opinion ainsi que les fonctionnaires à qui ils ont remis rapidement les cartes d'identité dès l'enregistrement de leurs attributs biométriques. Pour ce faire, le maitre-mot de toute cette campagne aura été la transparence afin d'avoir la confiance de tous, y compris les différents partis politiques (opposition comprise).

Le manque d'infrastructures digitales et énergétiques a été un défi considérable à gérer dans le cadre de ce projet car seul 30% du territoire a accès à l'énergie. Par ailleurs, l'ensemble des points de collecte était sous équipé. A cet effet, l'équipe-projet a du acquérir 2.000 kits d'enrôlement biométrique solaire qui a permis d'adresser les difficultés susmentionnées. Afin de ne pas se disperser et tirer avantage de l'ensemble des équipements disponibles, l'équipe-projet a décidé de procéder à l'enrôlement dans toutes les régions les unes après les autres.

En parallèle, l'équipe-projet a mis en place un centre d'appel couplée avec une plateforme SMS/USSD pour apporter une aide en ligne aux clients avec la possibilité d'une transmission direct des éventuels griefs, réclamations, suggestions, etc. La logistique du projet a pu compter sur 120 véhicules fournis (sur 800 promis initialement) par le Gouvernement en guise de contribution en nature, entre autres, au projet en échange d'une contribution de sa contribution à 40% au final.

En termes de compétences pour l'administration, la maintenance et l'évolutivité du système, l'équipe-projet a mis en place un système innovant de détection des talents. Pour ce faire, elle a engagé un consultant qui a développé et mis en ligne un test d'évaluation des capacités dans le digital. Les Termes de Références (TdR) du recrutement ont été mis au point par le PNUD et un processus de recrutement basé sur le mérite (avec la prise en compte du genre et du handicap au passage) a été lancé et conclu avec succès.

Un programme de formation sur plusieurs mois a été organisé ensuite pour expliquer le bien fondé de tout le projet et ses externalités positives considérables sur tous les secteurs socio-

économiques du pays. Tous les usagers du système qu'ils soient du public (agents des ministères, des aéroports, de la douane, etc.) ou du privé (banques, IMF, opérateurs télécoms, organisations professionnelles, etc.) ont été formés.

En termes d'enrôlement, la stratégie retenue consistait à se concentrer sur les régions les unes après les autres, comme indiqué plus haut. Les données recueillies concernent les attributs biométriques des personnes (10 empreintes digitales avec la photographie numérique pour les besoins de la reconnaissance faciale) ainsi que les données démographiques et d'identification (des différents documents d'identité associés à une même personne) suivants : (i) type de document ; (ii) Etat de délivrance ; (iii) Date de délivrance ; (iv) Prénom ; (v) Nom ; (vi) Numéro d'identification; (vii) Nationalité ; (viii) Date de naissance ; (ix) Sexe ; (x) Date d'expiration ; (xi) Photo ; (xii) Signature ; (xiii) Autres noms ; (xiv) Lieu de naissance ; (xv) Résident permanent. Les données ainsi recueillies étaient ensuite téléchargées dans la base de données centrale. Enregistrées uniquement sur la puce de la carte d'identité, les attributs biométriques étaient utilisés pour les besoins de déduplication avant une vérification qualité des données démographiques pour corriger les dernières coquilles précédant la validation définitive de la saisie par des officiers d'enrôlement assermentés. Ces données étaient ensuite utilisées pour la confection des cartes d'identité biométrique.

Eu égard à ce qui précède, il convient de souligner la complétude des données stockées dans la base qui permettent de recueillir à la fois les données démographiques et d'état civil : l'identifiant unique utilisé permettrait d'associer potentiellement à un même individu différents documents d'identité (acte de naissance, carte d'identité, passeport, etc.). A cet effet, malgré le fait que le RNPB du Malawi ne concerne que les adultes (au-delà de 16 ans) qui sont en droit de demander une carte d'identité, il est tout à fait possible de l'étendre aux enfants afin de pouvoir les enrôler dès leur naissance avec leurs données démographiques quitte à recueillir leurs données biométriques plus tard.

Contrairement à l'Inde (ou les individus se voient uniquement attribués un numéro Aadhaar non associé à une carte quelconque) et à l'instar du Pérou, le Gouvernement malawite a opté pour une carte d'identité biométrique afin de prendre en compte en amont différentes applications qui ne peuvent attendre le développement d'applications fonctionnelles. En effet, ils sont partis d'un constat simple selon lequel l'adoption ne peut se matérialiser qu'à travers l'usage.

De plus, compte tenu des limites infrastructurelles existantes, le Malawi a opté pour une carte intégrant les données biométriques du détenteur ainsi que sa signature électronique (respectant les normes établis par l'OACI n° 9303 et la norme ISO 7816). Elle renferme également une application d'e-Santé pour faire office de carte d'assurance maladie respectant la norme ISO 21549. Elle contient également une infrastructure à clé publique (PKI) pour les besoins d'identification des bénéficiaires pour des programmes de transferts sociaux, d'inclusion financière, etc. Elle contient également une application d'e-permis de conduire. En plus du numéro d'identifiant unique, elle interagit avec les différents terminaux existants à travers : (i) code QR; (ii) code MRZ; et (iii) puce insérée dans la carte.

Pour la distribution des cartes, l'équipe-projet a mis en place, en collaboration avec les opérateurs mobiles locaux, un système SMS/USSD qui en retour du numéro d'identifiant donne le statut de la délivrance de la carte et le lieu de distribution dans la langue locale. Pour ceux qui avaient perdu leur numéro d'enregistrement, il leur restait toujours l'option d'adresser leurs requêtes à travers un centre d'appel qui les orientaient en fonction des informations fournies.

En termes de coûts de réalisation, le projet a commandé environ 10 millions de carte d'identité à raison de 1,65 Dollars EU par carte ainsi que 2.000 kits d'enrôlement biométrique. Le coût par personne est d'environ 5 Dollars EU et le nombre total des personnes engagées est de 4.500. Le Gouvernement a décidé de donner gratuitement la première carte d'identité qui a une durée de 10 ans. Pour le remplacement ou le renouvèlement, les malawites devront payés afin d'assurer la pérennité du RNPB sachant que la réflexion est en cours pour subventionner pour les populations les plus vulnérables. En plus des adultes, le projet a également enrôlé 3,6 millions d'enfants âgés de moins de 16 ans aux fins d'une future extension du système à toute la population du pays. Les enrôlements concernent également les malawites de l'étranger à travers les ambassades et consulats.

Sur les aspects techniques, il convient de noter que l'ensemble des applications et interfaces pour le recueil des données biométriques ainsi que les bases de données requises ont été développés par l'équipe IT du BNI et ont travaillé avec le Ministère en charge des TIC sur ce sujet. En raison de retard de la construction d'un centre de données (Datacenter) public, les données sont actuellement stockées dans les serveurs du Trésorerie Général du pays.

En termes de cadre institutionnel, le BNI a signé des mémorandums d'entente avec la Commission électorale du Malawi et l'Office en charge de l'Etat civil pour lier le RNPB avec le fichier électoral et le RNEC. De plus, le Gouvernement malawite a décidé de rendre obligatoire la détention de la carte nationale d'identité pour l'obtention d'une carte SIM pour les citoyens et de la carte de résident pour les personnes en situation régulière (réfugiés compris). Le numéro d'identifiant sera aussi utilisé pour le paiement des taxes et pour l'e-KYC. Il sera aussi utile dans la recherche d'éventuels employés fantômes et de passagers clandestins dans les programmes sociaux publics. A terme, des accords similaires sont prévus avec le département en charge de l'immigration, le Ministère de la Santé, des Affaires locales, de la justice, de l'agriculture, etc. Le BNI compte en son sein une équipe en charge du suivi-évaluation de l'opération et qui analyse les données collectées à travers le centre d'appel et le système de communication SMS/USSD. Ils continuent aussi à avoir des feedbacks de terrain à travers les visites régulières de sites d'enrôlement notamment.

4.7. Principales leçons pour les pays africains

Tout d'abord, il convient de souligner que le principal avantage d'un système d'authentification centralisé quelques soient les attributs utilisés réside dans ses coûts de mise en œuvre et de maintenance très accessible par rapport à un système décentralisé basé sur différents types d'attributs détenus par différents opérateurs publics et privés (modèle anglais) qui reste relativement couteux. Pour cela les pays africains peuvent pleinement tirer avantage des taux de pénétration du mobile. Toutefois, cela ne dispense pas de continuer d'avoir des systèmes alternatifs aux services qui seraient éventuellement liés à un NIP pour éviter l'exclusion d'une frange plus ou moins importante (et généralement les plus vulnérables de la population). Pour ce faire, le maintien des systèmes d'identité existants est nécessaire jusqu'à ce que la connectivité soit totale dans les pays considérés.

Par ailleurs, les défenseurs du modèle indien arguent que le pays n'avait pas d'autre choix que celle retenue pour aller vite dans la mise en place du RNP sans se soucier de la fiabilité des données collectées. C'est la raison pour laquelle les Autorités indiennes pensent maintenant à enrôler les enfants sur le même principe car ils veulent étendre le système aux projets d'aide aux enfants scolarisés. Les pays africains doivent donc tirer la leçon et éviter de tomber dans cette impasse qui laisserait complétement à l'abandon les systèmes d'état civil nationaux,

uniques bases de référence nationale, pour les nationaux d'un pays pour tous les documents administratifs souhaités. Pour ce faire, il faudra implémenter en même temps au moins le RNP et le RNEC dont la mise au point synchrone permettra d'avoir des économies d'échelle considérables couplées à la constitution d'une base de référence nationale fiable pour le SNID fondamentale.

A cet effet, le RNEC pourrait profiter de la dynamique de l'identité digitale autour du RNP En effet, le RNEC comprend les informations immuables relatifs aux citoyens d'un pays alors que les autres données changeantes pour toute la population devraient se retrouver dans RNP.
Pour ce faire : (i) soit les données disponibles (antériorités) sont suffisamment utilisables et auxquels deux types d'enregistrement peuvent se faire (reprise des antériorités & saisie de toutes les nouvelles naissances, des changements matrimoniaux, des décès, etc.) ; (ii) soit commencer de zéro et enregistrer toutes les nouvelles naissances tout le complétant à travers les opérations de recensement, d'enrôlement général pour les élections, etc. Dans tous les cas, la mise en place des deux registres (RNP et RNEC) doit être relativement concomitante pour éviter tout déphasage entre la réalisation des deux systèmes car le rattrapage risque d'être couteux et excessivement long par la suite.

D'ailleurs, il convient de signaler que cette question de la citoyenneté se pose avec une telle acuité en Inde que plusieurs options ont été envisagées pour la « reconstitution » d'un RNEC. A cet effet, il a été, par exemple, envisagé de prendre, comme point de départ les fichiers électoraux de l'année 1971. Et même dans ce cas, les Autorités indiennes se sont vite rendues à l'évidence que cela exclurait de facto plusieurs millions d'indiens qui risquent d'être considérés à tort pour beaucoup comme n'étant pas citoyens indiens. D'où la nécessité de traiter cette problématique suffisamment en amont (et dans le cadre des programmes nationaux d'identité) afin d'éviter de se retrouver devant une difficulté insoluble du fait des effets pervers en termes d'exclusion, de coûts exorbitants, de différends communautaires anciens, etc. qu'elle peut susciter. En somme, le prix à payer risque d'être très élevé par la suite.

Dans tous les cas et de mon point de vue, un RNEC reste une pièce essentielle des services publics car dans tous les cas car il demeure le registre de référence pour les activités dévolues à la nationalité, la délivrance de carte d'identité, etc. L'intérêt du RNEC réside principalement sur le fait que cela est un point d'entrée pour les enfants dans les systèmes d'identification dont les attributs pourraient être complétés ensuite avec les données démographiques et biométriques plus tard (dans l'hypothèse où les technologies existantes ne permettent pas d'avoir des données fiables lors de la naissance).

Sur un plan plus global, l'expérience indienne dans la mise en place d'un écosystème favorable au digital à travers le programme « India Stack » est aussi intéressante pour le continent vu que le système Aadhaar est une composante d'un ensemble plus vaste qui se propose de mettre en place une plateforme logicielle unifiée qui permettra aux entreprises, aux personnes et à l'administration d'interagir. Ainsi et dans le cadre ce programme, il est prévu de développer un ensemble d'API (Interface de programmation applicative) qui permettra de facilité l'interopérabilité des différents systèmes d'information utilisés en Inde pour réduire (voir annuler) l'utilisation du papier et de son corollaire de captures en tout genre.
Bien entendu, le succès d'une telle initiative disruptive demande une gouvernance établie, un cadre juridique et réglementaire favorable à l'innovation mais protecteur des libertés individuelles, et une volonté politique claire et affirmée pour limiter au maximum les résistances au changement.

A cet égard, beaucoup de pays africains peuvent convertir en avantage le fait que tout reste à faire en adoptant les bonnes approches et en s'inspirant des expériences utiles engrangées au fil des deux décennies passées par les pays étudiés plus haut, entre autres. En particulier, il y a lieu de souligner les résultats remarquables de l'Inde sur le front de l'inclusion financière grâce à l'association des numéros Aadhaar, bancaire et mobile.

Par rapport à l'expérience intéressante du Pérou, il convient de noter l'importance de la gouvernance mise en place qui devra s'appuyer sur une distinction claire entre les systèmes d'identité fondamentaux et fonctionnels, l'autonomie de l'Agence en charge de la gestion de l'identité fondamentale, les moyens techniques et humains mis à disposition et la volonté politique. De plus, il convient d'accompagner le dispositif avec un modèle économique orienté vers les coûts pour que les bénéficiaires puissent contribuer financièrement et dans la mesure de leurs moyens à la pérennité du système tout en mettant en place une compensation de l'Etat pour gérer les surcoûts liés au « last mile » (populations pauvres, habitants des zones reculées ou difficilement accessibles, nomades, etc.). A l'instar du Pérou, le Malawi n'a pas manqué de jumeler les registres d'état civil dans son système national d'identification. Cela est de nature à traiter en parallèle les problématiques de résidence et de citoyenneté qui appelle chacune des droits et devoirs spécifiques qui ne se recoupent pas forcément.

Le modèle estonien pourrait être inspirant pour des pays africain avec des taux d'alphabétisation (et de culture digitale) élevée et une base établie en termes de moyens infrastructurels et applicatifs. Par ailleurs, la séparation des données d'identification stockées sur la carte d'identité électronique et les attributs démographiques et biométriques gérées au niveau central permettent de limiter les risques de mésusage de l'identité des personnes. L'accent mis au début du processus sur le volet formation est aussi instructif dans le cadre des nécessaires mesures d'accompagnement en termes de formations, de gestion de gestion, de communication, etc. dans toute démarche de mise en place d'un SNID robuste, fiable et sécurisé.

Quant au modèle anglais, il présente l'avantage de présenter les possibilités d'un système décentralisé avec des informations distribuées permettant de vérifier l'identité d'une personne par recoupement. Par ricochet, il pose aussi la question lié au contrôle de l'usage qui pourrait être fait des énormes quantités d'informations d'identité que les opérateurs télécoms en Afrique ont constitué en raison de l'obligation qui leur a fait au cours de ces dernières années pour identifier leurs clientèles mobiles.

Enfin le modèle malawite semble répondre aux contraintes spécifiques des pays africains (et subsahariens, en particulier). Néanmoins, il nécessite quelques ajustements qui permettraient d'améliorer sensiblement ses performances.

V. OPPORTUNITES ET DEFIS

5.1. Opportunités

5.1.1. Introduction

Les opportunités offertes par l'identité digitale à la fois pour les administrations, les entreprises et les individus semblent proprement illimitées. En effet, dans l'ère du numérique, le SNID peut générer des économies importantes pour ces trois opérateurs économiques en réduisant les coûts de transaction, en accroissant l'efficience et en créant des nouveaux services notamment aux populations les plus pauvres et vulnérables.

5.1.2. Inclusion financière

Dans un contexte de concurrence généralisée, les institutions bancaires sont dans une stratégie de concurrence qui ne laisse pas de place à l'improvisation. Une des clés de la réussite réside dans la réduction des coûts de fonctionnement sachant que le modèle bancaire traditionnel a été mis à rude épreuve par la concurrence intense des opérateurs mobiles, émetteurs de monnaies électroniques. A cet effet, l'authentification digitale permet aux banques de réduire les coûts des ouvertures des comptes bancaires. Ainsi, grâce au système Aadhaar, les banques indiennes ont fait passer ces coûts de 5 à 0,07 Dollars EU.

Compte tenu du taux de pénétration relativement élevée de la téléphonie mobile dans les pays en développement et en particulier en Afrique[3], il s'avère opportun d'envisager un couplage de l'identité digitale avec le mobile (m-ID). Ce type de technologie permettrait aux populations africaines d'accéder à des services gouvernementaux en ligne, profiter de l'e-Commerce, faciliter l'ouverture de comptes bancaires à travers le m-KYC, le paiement des taxes et autres impôts, etc. A titre d'illustration et à travers avec un couplage avec le numéro de téléphone, le système Aadhaar a abouti à l'ouverture de plus de 290 millions de nouveaux comptes bancaires.

La mise en place d'un e-KYC basé sur un SNID fiable permet également aux institutions financières (banques, IMF, etc.) d'accéder à l'historique des clients afin de pouvoir développer une large gamme de services de crédit adaptés. Or, l'accès à ce crédit permet ensuite aux populations (et en particulier aux plus pauvres) de lancer des activités génératrices de revenu qui les font, in fine, sortir de la pauvreté.

5.1.3. Accès aux services sociaux de base

Sans pièce d'identité légale, un grand nombre de personnes restent exclus de l'accès aux services sociaux de base sur le continent. Ainsi, pour inscrire un enfant à l'école, il faut d'abord produire un certificat de naissance. Or, dans certains pays, pour avoir ce certificat de naissance, les parents doivent produire un acte de mariage. Ce qui oblige donc certains parents à abandonner ce processus tant les obstacles rencontrés sont incommensurables surtout pour les enfants conçus hors mariage, en plus des pesanteurs culturels et réligieux.
Dans d'autres pays, il n'y a pas besoin de certificat de naissance à l'entrée de l'école mais plutôt au moment de passer des examens. C'est donc autant de facteurs d'exclusion qui explique souvent le peu de scolarisation des enfants (et surtout de la jeune fille) dans les populations vivant dans les contrées les plus pauvres notamment.

Par conséquent, la mise en place d'un SNID complet (intégrant idéalement un RNEC) et généralisé permettrait de venir à bout des obstacles expliquant les taux de scolarisation faible observés dans certaines contrées du continent. Il est intéressant de noter qu'il y a aussi un effort à faire également du côté du législateur pour supprimer les barrières à l'entrée du système éducatif en attendant la mise en place d'un SNID opérationnel et couvrant toute la population du pays considéré.

Quant à la couverture sanitaire, il convient de noter que beaucoup d'études faites dans divers pays (Inde, Kenya, Sierra Leone, etc.) montrent une forte corrélation entre la fourniture d'un certificat de naissance à un nouveau-né et le suivi du calendrier vaccinal.

[3] 44% de taux de pénétration pour les SIM uniques (Source : GSMA, 2017)

Plus généralement, la mise en place d'un SNID généralisé permet de soutenir l'implémentation de systèmes d'information sanitaires efficaces, outil d'aide à la décision pour concrétiser l'ODD n° 3.8 qui encourage la mise en place d'une couverture sanitaire universelle.
En complément et en termes de protection sociale, le système Aadhaar indien a permis de fournir une couverture maladie à plus de 100 millions d'indiens pauvres grâce à la fiabilisation du registre des bénéficiaires par l'entremise de l'usage de l'authentification biométrique.

5.1.4. Transferts sociaux

Compte tenu des inégalités importantes sur le continent, beaucoup de pays ont mis en place des programmes de transferts sociaux, généralement connus sous l'appellation de « filets sociaux ». Or, ces programmes sont financés généralement sur le budget national mais aussi à coup d'emprunts auprès des bailleurs internationaux. Dans d'autres pays, c'est tout le système de compensation nationale qui est au bord de la faillite en raison de la pression énorme exercée par l'indifférenciation entre populations réellement nécessiteuses et les autres.
Or, avec un SNID robuste, fiable et sécurisé, il est assez aisé de mettre en place un ciblage efficace de ces programmes afin de ne dépenser que les ressources requises par les populations qui en ont besoin. Ainsi, l'Inde a lié le numéro Aadhaar à nombre de programmes sociaux et a pu réaliser jusqu'à 15% d'économie sur le programme de fourniture de gaz pour la cuisine aux familles les plus nécessiteuses : ce qui représente 1 milliard de Dollars EU d'économie par an sur ce programme. Sur l'ensemble des programmes sociaux, les économies réalisées s'élèvent même à 11,3 milliards de Dollars EU par an.

5.1.5. Paiements digitaux gouvernementaux

Beaucoup de pays (particulièrement en Afrique) souffrent d'une administration aux effectifs pléthoriques et souvent peu efficiente. De plus, il s'avère qu'en plus de cela il faille aussi rajouter des contingents, plus ou moins fournis selon les pays, d'employés (fonctionnaires, conventionnés, etc.) fantômes. Compte tenu de la charge considérable des salaires et autres pensions dans les budgets des états, certains pays ont trouvé dans les applications du SNID un moyen efficace d'éliminer ces passagers clandestins.

A titre d'illustration, la mise à profit du SNID au Nigéria en 2017 dans les fichiers nationaux des fonctionnaires a permis de débusquer et de radier pas moins de 60.000 employés fictifs et a pu donc faire économiser à l'Etat environ 1,12 milliard de Dollars EU grâce à cette opération. Il y a lieu de souligner que la mise en place de cette application du SNID s'est faite à un cout marginal sachant que le système fondamental était déjà en place.

Dans le sens inverse, les systèmes nationaux de collecte des taxes, impôts, droits de douane, etc. pourrait aussi connaitre la même amélioration en utilisant l'identité digitale. En effet, le plus souvent, le manque de communication entre les différents systèmes d'information de l'Etat favorise les phénomènes de fraude par dissimulation. Or, avec un SNID permettant d'identifier chaque individu, le Pakistan a pu, par exemple, identifier pas moins de 3,5 millions de personnes susceptibles de payer des impôts et taxes.

5.2. Défis

Les défis liés à la mise en place, l'opérationnalisation et l'utilisation effective des SNID sont liés, entre autres, aux différents sujets suivants :

5.2.1. Gouvernance

Au moment de la conception, les gouvernements africains font face à des difficultés liées aux multiples parties prenantes qui se disputent littéralement la propriété d'un tel système entre les entités publiques en charge de l'état civil, des cartes d'identité, des passeports, etc. Et en définitive, celui qui remporte la mise est celui qui peut compter sur les appuis les plus conséquents et non nécessairement le plus adéquat et le plus qualifié.

Lors de la mise en place d'un SNID, les difficultés connues sont celles liées à la disponibilité des « compléments analogiques » relatifs à la protection des données personnelles, la cybersécurité, etc. Comme indiqué dans le chapitre consacré à la protection des données personnelles et la vie privée, l'étude conduite par le mouvement ID4Africa (Annexe II) montre le niveau élevé des préoccupations exprimées par rapport à ces sujets par la communauté africaine de l'identification des personnes.

Après la mise en place de tels systèmes, le risque majeur concerne leur utilisation par tous les secteurs interagissant directement avec des individus. Avant tout, il y a lieu de souligner que si la couverture de l'identité digitale ne se situe pas aux alentours d'un pourcentage de 75-80%, il est pratiquement impossible aux entités utilisatrices de tirer avantage d'un SNID. En effet, la couverture universelle de l'identité digitale est assez couteuse quand il s'agit d'enrôler les derniers 15-20% de la population. Et malgré un taux de complétude 75-80%, certains pays africains éprouvent d'énormes difficultés pour le passage à l'utilisation généralisée de l'identité digitale tout en garantissant les données personnelles.

5.2.2. Protection la vie privée et des données personnelles

Tout d'abord, la protection des données fait référence au droit reconnu à une personne d'accéder et de contrôler l'usage qui est fait de ses données personnelles par des tiers (entreprise, individu et administration). En raison de la multitude de traces que nous laissons dans les divers systèmes (personnel, professionnel, social, etc.) que nous utilisons de nos jours, les risques de violation potentielle de la vie privée s'en trouvent considérablement étendus.

Pour ce qui est de systèmes d'identité digitale, une des parades qui a été trouvé aux risques susmentionnés est de réduire considérablement la quantité d'informations demandées sur une personne au strict minimum. C'est la raison pour laquelle le système Aadhaar est principalement basé sur des questions donnant des réponses binaires (Oui/Non).

Cela étant dit, la protection des données personnelles passent encore par l'élaboration et la mise en vigueur de loi y afférent. Toutefois, il est tout au aussi important de s'assurer de la disponibilité des capacités technique et institutionnelle pour pouvoir l'appliquer dans toute sa plénitude. D'ailleurs, le caractère transfrontalier des flux des données personnelles posent aussi question dans la mesure où il n'y a pas encore de cadre mondial harmonisé sur la protection des données personnelles. De ce point de vue, le RGDP européen pourrait être un objectif commun vers lequel les autres régions du monde (et en particulier l'Afrique) pourraient tendre pour créer les conditions d'une harmonisation planétaire de fait, à défaut d'être actée faute de mécanisme international approprié pour le moment.

5.2.3. Risques d'exclusion

Malgré tous les avantages liés à son utilisation, la mise en place d'un SNID peut aussi induire des effets pervers qui peuvent aboutir à l'exclusion de certaines catégories de la population pour des diverses raisons qui peuvent se combiner.
Tout d'abord, il y a lieu de souligner la barrière des coûts qui est le facteur le plus important qui peut aboutir à l'exclusion des couches le plus vulnérables de la population en raison de leurs revenus modestes, de la difficulté d'accessibilité de leurs lieux d'habitation, etc. Par ailleurs, les Gouvernements des pays concernés sont tentés de mettre en place un mécanisme d'autofinancement (du moins, en ce qui concerne les frais récurrents) des SNID. C'est la raison pour laquelle il est impératif de mettre en place des dispositifs de subvention de l'accès et à l'utilisation du SNID au profit de ces populations pauvres, à l'instar du Malawi et du Pérou.

Les discriminations à l'encontre des femmes peuvent également conduire à une inégalité d'accès (et donc d'utilisation) des documents d'identité. Dans certains pays (Irak, Afghanistan, etc.), il est exigé à la femme qu'elle soit accompagnée par un proche pour avoir ces documents en raison de considérations culturelles et/ou religieuses.

Le critère de la nationalité pourrait être aussi un frein au droit à l'identité. En effet, dans certains pays l'identification ne concerne que les citoyens et plus largement les personnes en situation régulière dans le pays en question. Or, dans le même temps des mesures sont prises pour liées l'identité à l'obtention de service de base tels que l'achat d'une carte SIM alors qu'il y a des personnes qui ne peuvent produire aucun support d'identité. C'est le cas des migrants par exemple en Afrique et dans une moindre mesure les apatrides. C'est pourquoi, il y a lieu d'analyser en amont toutes les catégories de personne susceptibles d'avoir besoin d'être identifié avant de prendre des mesures qui risquent de générer l'exclusion de certaines catégories de population.

VI. PISTES DE RELEXION

6.1. Questionnements

Tout d'abord, il y a lieu de constater le manque d'études approfondies du paysage de l'identité digitale en Afrique et de recul sur des expériences conduites par les pays africains dans ce domaine. Certes, certains pays (Rwanda, Ghana, Mauritanie, Algérie, Tanzanie, etc.) ont mis en place des systèmes d'identification unique des personnes et peuvent donc aller plus dans la mise à profit de ces acquis dans des programmes élaborés d'administration électronique exhaustifs, à l'instar de l'Estonie ou de l'Inde.

Par ailleurs, le continent manque encore d'une masse critique de spécialistes de ce domaine prometteur et multidisciplinaire. Cela pose donc un sérieux problème dans l'appropriation et la prise en compte d'un sujet aussi disruptif dans les politiques de développement des pays africains.

Partant de là, le grand risque qui guette le continent est la tentation de vouloir « plaquer » des solutions toutes faites, et probablement éprouvées ailleurs, mais qui ne répondraient en rien aux besoins réels des populations africaines, bénéficiaires ultimes et centrales de tout SNID robuste, sécurisé et fiable.

6.2. Quid de l'usage des attributs détenus par les opérateurs privés?

Comme outil d'appoint pour s'assurer de la qualité de l'identité digitale, il serait éventuellement envisageable de se référer à la masse de données personnelles emmagasinées par les opérateurs privés et en particulier le GAFA (Google, Apple, Facebook et Amazon) ainsi que les réseaux sociaux et professionnels (twitter, LinkedIn, etc.) à l'échelle internationale et en particulier africaine. En effet et à titre d'illustration, l'on estime de nos jours que Facebook compte plus de 2 milliards de membre alors que le réseau professionnel LinkedIn revendique lui plus de 500 millions de membre.

Néanmoins, il y a lieu, tout de même, d'être assez circonspect par rapport à cette démarche pour les raisons suivantes :

- ✓ Les manipulations à grande échelle des données personnelles révélées à travers la retentissante affaire récente appelée « *Cambridge Analytica* » et qui a touché des dizaines de millions d'utilisateurs de Facebook rappelle la vulnérabilité du modèle sur lequel est basé la plupart des réseaux sociaux.
- ✓ D'ailleurs, il faut aussi rappeler qu'il n'y a aucun processus de vérification et d'assurance qualité dans la saisie des données personnelles dans les réseaux sociaux.
- ✓ Par conséquent, il serait inopportun de se baser uniquement sur ces données brutes à moins d'investir lourdement dans des puissants algorithmes qui, par recoupement d'information par exemple, serait capable de dissocier le vrai du faux et d'aboutir donc à des données suffisamment exploitables sans oublier le cadre strict dans lequel ces données devront être utilisés.

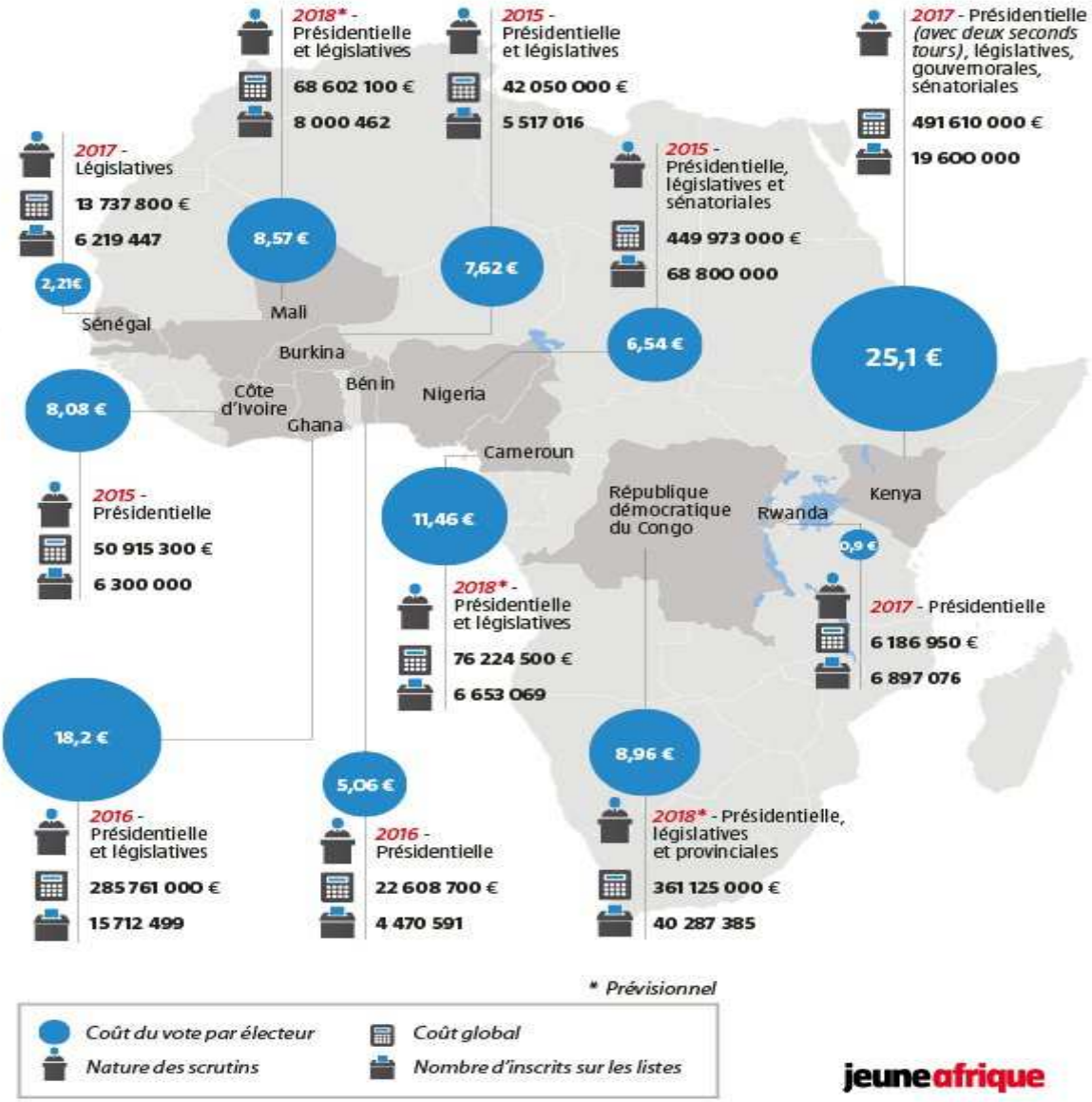
Sur la base des différents cas présentés plus haut, l'utilisation de ces données, après vérification en amont, serait plus compatible avec le modèle anglais qui se base sur des opérateurs privés certifiés qui peuvent recouper les informations glanées de différentes sources pour identifier une personne.

6.3. Enseignements tirés

Sur la base des différents modèles présentés plus haut, je pense que le Malawi a pu mettre en place un SNID intéressant mais perfectible sur certains aspects aux fins de sa mise à profit dans d'autres pays africains (subsahariens, notamment).
Tout d'abord, il convient tout d'abord de rappeler que l'organisation régulière des campagnes de recensement général de la population coûte, en règle générale, relativement cher aux pays africains. Sur la base des chiffres disponibles, ces recensements coûtent en moyenne dans les 30 millions de Dollars EU[4].

L'organisation des élections engloutit, quant à elle, des ressources encore plus importantes avec une cadence bien plus élevée, comme résumé dans le carte suivante (source : *site Internet de l'hebdomadaire Jeune Afrique*) :

[4] https://wcaro.unfpa.org/fr/news/le-sénégal-publie-les-résultats-provisoires-du-recensement-en-un-temps-record-grâce-à-l'appui



Or, avec un SNID fondamental robuste, sécurisé et fiable, l'établissement des listes électorales ne poserait aucune difficulté et ce d'autant qu'il serait dans ce cas possible d'éviter même les coûteuses opérations d'édition, d'impression et de distribution des cartes d'électeurs. En effet, il serait possible de pouvoir voter avec sa carte d'identité nationale (ou de même de résident, s'il s'agit d'une élection ou les résidents peuvent y participer). A titre d'illustration, les 21 millions de Dollars EU de contribution du Malawi dans la mise en place de son SNID sont largement plus avantageux que l'éternelle reconstitution du fichier électoral qui coûte des sommes considérables aux contribuables, à commencer par les élections de l'année prochaine.

Par ailleurs et c'est là le plus important, beaucoup de pays africains auraient évité tant de désordres et d'instabilités socio-politiques qui coûtent excessivement chers au continent. Et, il y a lieu de noter que souvent les controverses qui aboutissent aux troubles susmentionnées partent généralement des questionnements et réserves qui entourent la confection des fameuses listes électorales.
A titre d'illustration, les retombées positives de la consultation de l'équipe-projet du projet au Malawi avec les parlementaires et partis politiques du pays (opposition comprise) et leur adhésion qui s'en est suivi ont été suffisamment décisifs pour la réussite du projet. Plus

globalement, il est extrêmement important de ne pas évacuer l'importance du capital confiance qui doit être placé par toutes les organisations politiques, associatives, religieuses, communautaires, etc. d'un pays depuis l'initiation jusqu'à la finalisation et la mise en production des systèmes (fondamentaux et fonctionnels) d'identité digitale.

Par ailleurs, et afin des gages à la communauté internationale, beaucoup de gouvernements africains se sont engagés dans la voie des élections 2.0 mettant en place, à grands frais, des systèmes de vote biométriques. Or, avec le recul sur la trentaine de pays qui l'ont expérimentés, force est de constater que le compte n'y est pas en matière d'apaisement du climat pré et post-électoral.
Or, comme rappelé plus haut, la solution est, à mon sens, à regarder du côté du Malawi car tant que l'organisation des élections n'est pas relégué à un « simple » système d'identité fonctionnel qui doit même être confondu pour l'essentiel à la carte d'identité nationale, les problèmes rappelés plus haut resteront toujours d'actualité.

Par contre, le modèle indien n'est en rien la panacée sur le continent, comme se font l'écho souvent les coupures de presse[5], pour les raisons suivantes :

- ✓ Malgré l'attrait (sur papier) de l'idée d'utiliser un système uniforme sur tout le continent, à l'instar de l'Inde, il est certain qu'il s'agit là d'une voie sans issue, à mon sens. En effet, comme souvent avancé par des personnes ne connaissant pas réellement l'Afrique, cette idée fait fi de l'évidence suivante : le continent africain n'est pas un tout homogène car les réalités économiques, sociales, infrastructurelles, etc. sont différentes du nord au sud et d'est en ouest.
- ✓ Contrairement à l'Inde et au regard de l'héritage de son passé colonial, les pays africains se sont engagés, pour la plupart, dans des processus au long cours ou la construction d'une cohésion nationale qui nécessite beaucoup d'efforts et de moyens afin de réduire les sources de fragilité conduisant souvent à l'instabilité socio-politique. Ces efforts s'inscrivent, d'ailleurs, dans des cadres régionaux de plus en plus intégrés (COMESA, EAC, CEDEAO, CEMAC, etc.). L'exemple de la carte biométrique utilisée dans la circulation des personnes au sein de l'espace de la CEDEAO en est une parfaite illustration.
- ✓ Dans le même temps et à un niveau continentale, l'Afrique s'est lancé dans un ambitieux agenda de développement ou l'intégration régionale est un jalon essentiel afin de créer des marchés régionaux et continentaux sur le long terme avec en ligne de mire une libre circulation des biens, des personnes, des services et du capital.
- ✓ Sur un plan infrastructurel, la majeure partie des pays subsahariens (spécialement en Afrique centrale et de l'Ouest) ne disposent pas des même prérequis technologiques (connectivité, Datacenters, etc.) pour pouvoir compter principalement sur une authentification en ligne sur la base d'attributs biométriques centralisées. D'où l'intérêt de l'expérience malawite qui a plutôt optée pour une solution ou ces attributs sont enregistrés à la fois sur la base de données centrale et sur la carte d'identité biométrique.
- ✓ Sur le plan légal, il convient de rappeler que la légalité du numéro Aadhaar est régulièrement remise en cause car il ne s'agit là que d'une preuve de résidence, ni plus ni moins. D'où les nombreuses décisions rendues par la Cour suprême indienne pour statuer sur les liens faits par le Gouvernement entre la délivrance de certains services publics et privés. Il est donc évident que toutes ces complications juridiques ne seraient pas posés si le numéro Aadhaar était lié à un document légal reconnu (carte d'identité, acte de naissance, passeport, permis de conduire, etc.).

[5] https://www.bloomberg.com/view/articles/2018-10-14/short-sellers-missed-tencent-s-250-billion-share-plunge-party

Eu égard à ce qui précède, il est assez clair que la réussite sur une courte période de l'expérience malawite devrait inciter à plus de considération de cette solution africaine adaptée au contexte subsaharien, à l'instar du M-Pesa kenyan qui est si souvent cité en référence dans les services financiers mobiles.

Néanmoins, il convient aussi d'esquisser les améliorations à apporter à ce modèle :

- ✓ Tout d'abord, il faudrait étendre le système à tous les malawites depuis leur naissance afin de couvrir également les enfants âgés de 0 à 16 ans pour les besoins des programmes nationaux s'adressant à ce public spécifique. Un effort a été fait en ce sens avec l'enrôlement de 3,6 millions d'enfants de moins 16 avec pour la plupart le recueil des attributs biométriques. Mais, il faut continuer sur cette lancée pour avoir également l'enrôlement de tous les enfants tout en alimentant le RNP avec les nouvelles naissances.
- ✓ Partant de là, il serait opportun de revoir le numéro d'identifiant afin que celui-ci soit plutôt numérique (NIP) avec suffisamment de digit pour couvrir un grand nombre de personne (l'Inde s'est limité à 12 digits par exemple pour son numéro Aaadhaar avec plus d'un milliard d'habitants). C'est la seule manière d'associer à une personne identifiée avec ce numéro à plusieurs documents d'identité nationale ou sectorielle.
- ✓ A travers le mémorandum signé entre le BNI et l'Office en charge de l'état civil le lien est désormais fait entre les deux documents d'identité légale de base, à savoir le certificat de naissance (jusqu'à 16 ans) et la carte d'identité (après 16 ans).
- ✓ Sur la base des acquis du modèle péruvien, il serait indiqué que le mémorandum précité aille plus loin que les aspects technologiques (intégration des deux registres) en incluant un partenariat entre les deux entités de telle sorte que l'Office en charge de l'état-civil puisse profiter du savoir-faire et des moyens dont dispose le BNI. Pour ce faire, il serait possible soit d'utiliser les kits d'enregistrement biométrique déjà acquis pour le projet de SNEI ou acquérir de nouveaux kits plus adaptés à l'enrôlement des enfants (nouveau-nés) vu que les attributs biométriques pourraient être recueillis plus tard, au moment de la demande de la carte d'identité nationale.
- ✓ Afin d'élargir les champs des personnes couvertes à tous les résidents (ou de passage) du pays (étrangers en situation régulière, réfugiés et même touristes à terme, etc.), il est impératif d'adopter rapidement un NIP national qui serait de nature à éviter les risques d'exclusion liés au SNEI. En effet, vu qu'il y a déjà un mémorandum d'entente déjà signé entre le BNI et l'Autorité de Régulation des Communications pour que les opérateurs mobiles puissent obligatoirement exiger une pièce d'identité pour l'obtention d'une carte SIM. Or, si un étranger en situation régulière peut encore présenter une pièce d'identité de son pays d'origine, il serait autrement plus difficile pour un réfugié de le faire s'il n'a pas un document officiel du Malawi le reconnaissant comme tel.

6.4. Ecosystème favorable au SNID

En résumé, voici donc les principales caractéristiques d'un SNID robuste, sécurisée et fiable :

- ✓ Il est absolument nécessaire d'avoir une claire séparation entre les composantes fondamentale et fonctionnelle pour éviter un schéma de concentration absolue au sein d'une même entité avec tout ce que cela génère comme préoccupations en matière de respect des libertés fondamentales, de confusion dans les missions dévolues à chacune des parties prenantes nationales, etc.
- ✓ La composante fondamentale du SNID devra comprendre au moins le RNP et le RNEC avec, le cas échéant, le RNB. Pour le reste, l'ensemble des autres composantes du SNID forment (passeport, permis de conduire, fichier électoral, système d'assurance sociale et de santé, DMP, etc.).

- ✓ Associés au NIP, les deux documents d'identification de base pour les citoyens devront être : (i) la carte nationale d'identité (à moins d'une disposition légale contraire, comme c'est le cas au Royaume-Uni) pour les personnes majeures ; et (ii) l'acte de naissance pour les enfants (avec un âge inférieur à la majorité).
- ✓ Le complément biométrique constitue un appoint d'identification/authentification intéressant dans les contextes nationaux avec un analphabétisme élevé. Néanmoins, le traitement de ces données sensibles nécessite la mise en place d'un cadre juridique et légale garantissant l'inviolabilité de ces attributs et le contrôle des utilisateurs sur ces derniers.
- ✓ Le NIP devra être attribué depuis la naissance pour les citoyens d'un pays et au moment de l'enrôlement pour le reste de la population résidente ou citoyenne d'un pays et vivant à l'étranger. Ce numéro doit être , d'une manière ou d'une autre, associé à toutes les pièces d'identité légales et reconnues (acte de naissance, carte d'identité, passeport, permis de conduire, titre de séjour des étrangers, réfugiés compris, etc.). Conformément à l'ODD n° 16.9, il faudra absolument éviter de recourir à un support d'identification créé ex nihilo uniquement (et donc en dehors de toute base légale établie) pour les besoins du NIP, à l'instar du modèle indien.
- ✓ Compte tenu des taux de pénétration de la téléphonie mobile sur le continent, il convient d'explorer des solutions d'identité digitale embarquées sur les cartes SIM des téléphones portables pour pouvoir faire le lien, entre autres, avec des facilités de paiement via les services financiers mobiles.
- ✓ En termes de gouvernance, il s'avère fondamental de mettre en place, si ce n'est pas le cas, un Office National d'Identification (ONI) doté d'une autonomie administrative et financière pour la gestion du SNID fondamental (RNP et RNB, si applicable). Les missions de l'ONI pourraient, en théorie et au besoin, être étendues au RNEC. Toutefois, un cadre de collaboration clair entre l'ONI et l'Office national en charge de l'état civil peut suffire avec des incitations claires aux fins de cette coopération, à la lumière des retours d'expérience du modèle péruvien.
- ✓ Concernant la conception technique du SNID, il serait souhaitable d'éviter de réinventer la roue vu qu'il y a beaucoup de solutions open source disponibles et qui ont l'avantage d'atténuer les risques de trappe des solutions propriétaires largement décriés par les pays africains. De plus, il serait même possible d'envisager des développements locaux d'applications sur la base de l'expérience malawite qui n'a pas généré des défaillances techniques notables depuis sa mise en production.
- ✓ En termes d'acquisitions d'équipements (terminaux d'enrôlement, authentification, etc.) et de documents sécurisés pour certains supports d'identité (carte électronique, acte de naissance, passeport, etc.), il convient de mettre en place des solutions de long terme qui permet aux pays africains de ne pas dépendre éternellement de l'aide extérieur. Cela pourra être traité à travers les innovantes startups africaines qui ont là la possibilité de créer des emplois qualifiés et de longue durée (vu la demande qui ira crescendo au cours des prochaines années et décennies) et de la richesse sur le continent. Par ailleurs, il serait intéressant d'explorer les possibilités de PPP dans ce secteur avec un clair plan de transfert de compétences à la clé, toujours pour adresser le lancinant problème des solutions propriétaires et des coûts exorbitants et surtout considérables qui y sont associés.
- ✓ Afin de développer la création de valeur autour de l'identité digitale, il serait opportun d'envisager un cadre favorable au développement d'API qui permettrait aux opérateurs privés de pouvoir développer leurs activités avec une connaissance précise de leurs utilisateurs, et cela dans un cadre suffisamment encadré.

Pour compléter les prérequis institutionnels de l'écosystème, la mise en place au niveau national d'une Instance Nationale de Protection de Données Personnelles (INPDP), véritable autorité autonome indépendante garante du respect de la vie privée et de la protection des données personnelles, s'avère essentielle pour que celle-ci puisse être associé à toutes les étapes de la concertation nationale devant aboutir à la mise du SNID.

De plus, et eu égard aux enjeux de cybersécurité évidents, il est tout aussi primordiale pour chaque pays, et si ce n'est déjà le cas, de recourir à un Centre d'Alerte et de Réaction aux Attaques Informatiques (CSIRT) couplé avec un Centre Opérationnel de Sécurité (COS). En termes de certification électronique et à la lumière du Malawi, il faudrait également mettre en place, si ce n'est déjà fait, une infrastructure à clé publique pour les besoins de la signature électronique à insérer dans la carte d'identité biométrique.

Afin d'assurer une cohérence globale avec la stratégie nationale digitale de chaque pays, il convient d'inscrire la réalisation de l'ensemble des volets susmentionnés dans le cadre de la plateforme d'interopérabilité nationale qui facilite la communication des différents systèmes d'informations gouvernemental.

Sur la base des résultats de l'expérience du Malawi, il est absolument recommandé d'accompagner la mise en place du SNID avec des applications concrètes et qui touchent directement la vie des populations du pays considéré. Ainsi, et sur le continent, la problématique de l'inclusion financière se pose avec beaucoup d'acuité vu la faible proportion des habitants bancarisés, surtout en Afrique subsaharienne.

Concernant le RNEC, l'expérience du Malawi est aussi intéressante car elle donne une solution pratique par rapport à l'enregistrement des antériorités qui peut se révéler extraordinairement fastidieux en raison de l'état de délabrement avancé des registres papier d'état civil dans nombre de pays africains. Dans ce cas, l'enregistrement de l'ensemble de la population dans le cadre de la campagne d'enrôlement général aux fins de la constitution du SNID peut être un bon compromis pour prendre en compte également les enfants (du moins par rapport aux données démographiques) pour ceux qui sont âgés de moins de 12 ans (âge limite pour l'exploitation des empreintes digitales à l'état actuel des solutions fiables disponibles sur le marché). Pour le reste, le RNEC pourra ensuite être la source de l'enrôlement en temps réel des nouveau-nés dont les données biométriques seront collectées, le cas échéant, en temps opportun en fonction des technologies disponibles et accessibles pour les pays concernés.

6.5. Différents modèles de système d'identité digitale

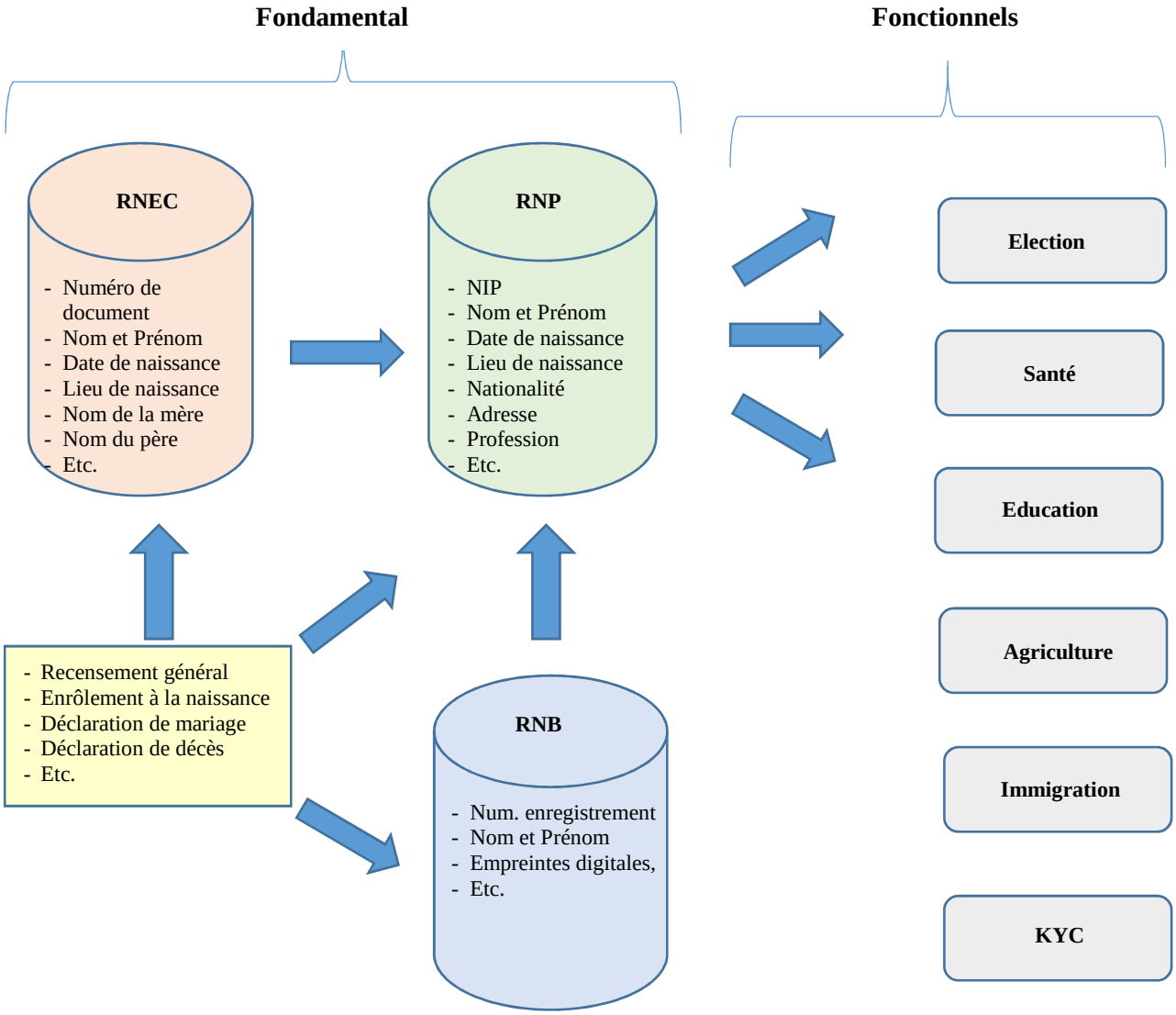
6.5.1. Introduction

Eu égard à ce qui précède, il convient de souligner que les pays africains pourraient être classés principalement en deux catégories en fonction de leur degré de préparation pour l'identité digitale.

6.5.2. Pays en développement digital

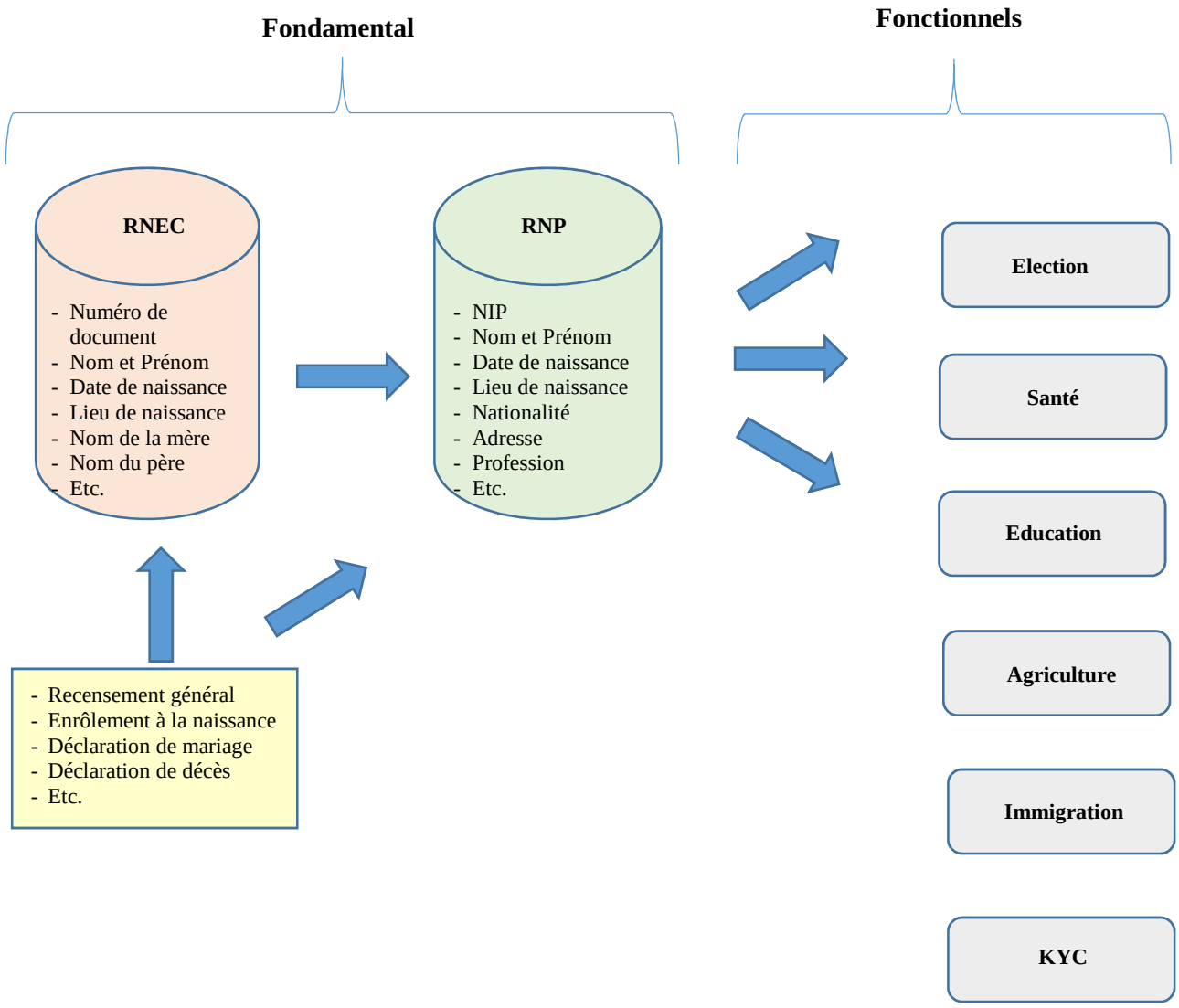
Dans ce cas-là et à la lumière des différentes, il y a plusieurs facteurs à prendre en compte dont notamment le niveau d'alphabétisme et la culture digitale, la qualité de la connectivité nationale et les facilités liées au développement de l'administration électronique (Datacenter, cloud, systèmes d'information gouvernementaux, etc.).

A cet effet, il semblerait qu'il y ait un consensus sur la valeur ajoutée de la biométrie pour les besoins de l'authentification de l'identité des personnes.
Ainsi, une proposition de modèle de SNID adapté à ce cas de figure pourrait être :



6.5.3. Pays digitalement avancés

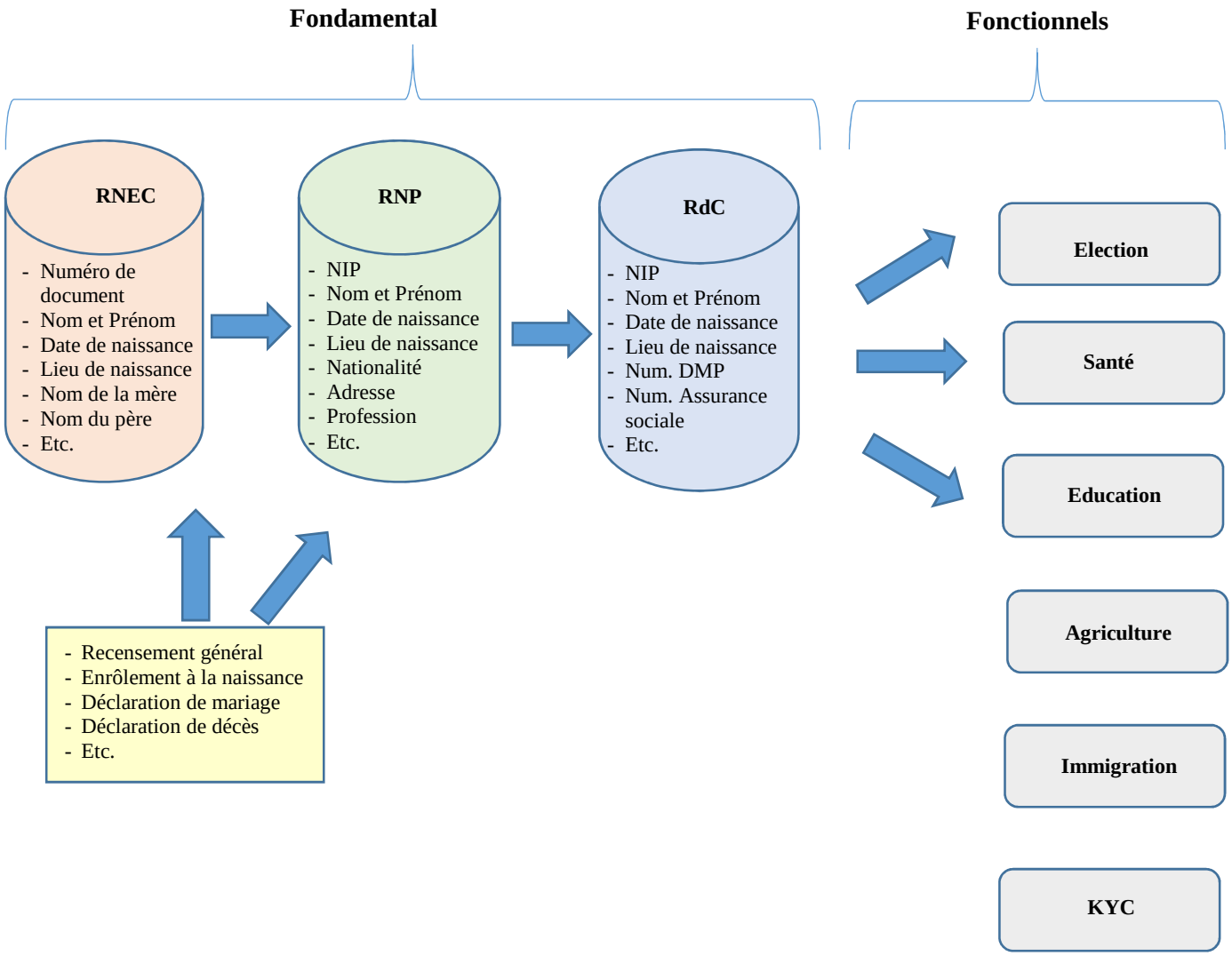
Concernant la présente catégorie de pays, il convient de noter qu'en raison de bases solides en termes d'infrastructures digitales et des résistances éventuelles à l'usage de la biométrie (en conformité avec les lois éventuelles en matière de protection des données personnelles), voici un premier modèle qui est basé sur l'utilisation directe du NIP dans les SNID fonctionnels.



Dans ce cas, l'identification est basée plutôt sur le contenu du support d'identité digitale (cartes d'identité ou de résident électronique) qui permet d'identifier le requérant d'un service au moyen de codes secret connus uniquement par lui-même et stocké sur ce support, à l'instar du modèle estonien.

L'inconvénient de ce modèle est qu'il nécessite une refonte des SNID fonctionnels pour prendre en compte le NIP dans l'authentification des personnes. En fait, cela convient plutôt à des SNID qui doivent être greffés sur des systèmes d'information existant qui ne sont pas très évolués.

Partant de là, certains pays pourraient plutôt opter pour une solution conforme au modèle X-ROAD estonien qui consisterait à mettre en place une interface entre les composantes fondamentale et fonctionnelles du SNID.
Voici donc un schéma qui résume cette alternative :



Comme indiqué plus haut, le Registre de Correspondance (RdC) est constitué d'une table permettant de faire le lien entre le NIP et les différents numéros d'identification utilisés dans les différents systèmes d'identité fonctionnels. Cette table tampon permet d'éviter l'accès direct aux informations contenues dans le RNP. En effet, le rôle majeur du SNID fondamental est de confirmer l'identité d'une personne à qui les différentes entités concernées sont censés lui fournir un service après confirmation de son identité. Afin d'éviter les risques de non authentification erronée, il est souhaitable d'opter pour une mise à jour automatique dudit registre.

Par ailleurs et dans les trois modèles, il est essentiel de mettre en place un outil de suivi de toutes les actions faites dans le SNID fondamental (consultation, traitement, etc.) afin que les utilisateurs puissent garder le contrôle sur l'usage qui est fait de leurs données personnelles.

6.6. Modèles de financement et rôles du secteur privé

Compte tenu de l'importance du SNID dans le développement socio-économique des pays africains, il s'avère utile de passer en revue les différents modes de financement existant :

1. Financements propres : ce type de financement est possible pour peu que les capacités techniques et les arrangements institutionnels soient déjà en place. Autrement cela risque de coûter cher au pays concerné sans que les objectifs poursuivis ne soient atteints. Néanmoins, il serait opportun tout de même d'avoir recours à l'assistance technique des bailleurs internationaux, par exemple, pour atténuer le risque d'asymétrie informationnelle entre les pouvoirs publics et les opérateurs privés dans le domaine de l'identité digitale dans le cas des pays en développement digital.
2. Financements auprès des bailleurs/banques commerciales : beaucoup de pays africains qui ont mis en place des SNID ont eu recours à des bailleurs internationaux et/ou aux banques commerciales, à l'instar du Malawi.
3. PPP : 2 modes possibles :
   (i) BOT (Build, Operate and Transfer) : ce type d'arrangement consiste à un partenariat entre un Etat et un partenaire privé avec un financement public (propre ou à travers le support d'un financier externe) couvrant en partie les coûts d'investissement/opération sachant que la partie restante provient du partenaire externe. Il est également envisageable de laisser l'entièreté des coûts d'investissement et même d'opération au partenaire privé. Par ailleurs, il est possible d'inclure également dans le schéma une banque commerciale (idéalement couplé avec un opérateur mobile) qui gère les flux financiers relatifs aux paiements des requérants pour l'accès aux services proposés (demande d'une carte d'identité, passeport, etc.). Cela permet de s'affranchir des risques de crédit surtout du côté gouvernemental en cas d'absence d'Office National d'Identification (ONI) en particulier. Il convient de souligner qu'en raison de ce montage la partie publique est en droit d'attendre un SLA suffisamment élevé pour s'assurer d'une qualité de service optimale.
   (ii) Contrat de service : ce type d'arrangement est, pour ainsi dire, une version plus « légère » que le BOT standard. En effet, dans ce cas de figure, l'on peut envisager un montage ou la partie publique assume à part entière les coûts d'investissement en laissant les coûts d'opérations au partenaire privé. Bien entendu, les gains financiers réalisés par les opérateurs privés sont moindres dans ce cas. A cet effet, le défi d'un tel montage est quand même de maintenir un niveau de qualité de service acceptable dans le cadre du contrat de service à négocier.

Concernant le PPP, il reste assez controversé parmi les pays africains en raison du fait que l'identité digitale a souvent une connotation de souveraineté nationale. Par ailleurs, il y a lieu de noter qu'en raison de l'obsolescence rapide des technologies, ces PPP ne dépassent rarement les 5 ans et ce d'autant qu'il y a une inquiétude tenace du côté des pays concernés de se retrouver prisonnier des solutions proposées par un fournisseur spécifique.

Par conséquent, il serait souhaitable qu'il y ait un réel effort des pays bénéficiaires par rapport à l'amélioration de l'offre de formations sur ces questions afin de susciter un secteur privé africain dynamique qui puisse s'investir et innover dans ce domaine très porteur car créateur d'emplois et de richesse (Cf. Malawi).

6.7. Perspectives

A la lumière de ce qui précède, il y a lieu de de souligner la nécessité, pour les pays africains, de la mise au point d'un guide pratique tiré des enseignements d'autres pays similaires (pays du Sud) pour s'en inspirer et expérimenter éventuellement des outils éprouvés et d'accès libre pour éviter les trappes des solutions propriétaires souvent onéreuses.
En effet, les pays bénéficiaires ont définitivement besoin d'un outil de référence qui leur permet de percevoir les réelles opportunités liées à l'identité digitale tout en leur donnant les clés pour se prémunir contre les risques qui y sont associés.
En complément, il serait aussi intéressant de lancer l'idée d'un index multidimensionnel qui permet de jauger le degré de préparation sur l'identité digitale de chacun des pays africains afin de créer une certaine émulation entre eux dans l'optique de la généralisation de l'identité digitale, en soutien à l'ODD n° 16.9.

Par ailleurs, le volet formation s'avère aussi primordial. Pour ce faire, il serait essentiel que le continent puisse développer des écoles spécialisées dans le digital et en particulier dans les thématiques liées à l'administration électronique (identité digitale, compris), la quatrième révolution industrielle (intelligente artificielle, blockchain, robotique, impression 3D, etc.), etc. pour tirer avantage de l'innovation digitale foisonnante sur le continent.

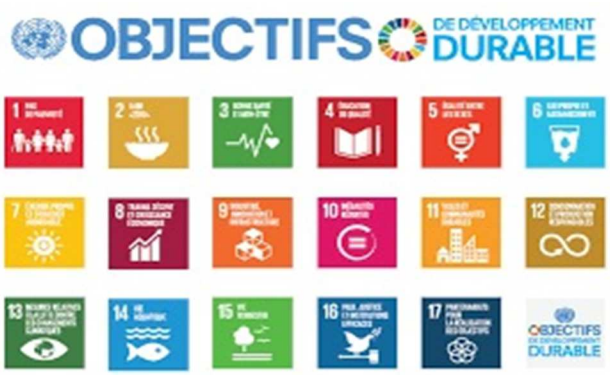
L'identité digitale est définitivement un secteur stratégique et prometteur pour le secteur privé africain, à travers ses startups en particulier, pour développer des solutions locales pour des problèmes locaux.

A l'instar du réseau africain sur la protection des données personnelles, il est aussi important de lancer une plateforme d'échange et de collaboration africaine similaire sur les problématiques de la cybersécurité qui coute de plus en plus chères aux économies africaines. La question de la protection des données personnelles est aussi un élément central au développement d'une identité digitale qui ne soit pas utilisé pour porter atteinte aux libertés individuelles. L'ensemble des acteurs publics et privés africains ont un rôle à jour dans cette œuvre commune.

A cet effet, il convient de rappeler que l'Union Africaine a adopté en 2014 la convention africaine sur la cybersécurité et la protection des données à caractère personnel. Jusqu'à date, rares sont les pays qui ont adopté cette convention dans leur législation nationale pour des raisons diverses. Il est donc temps de reprendre le texte initial en analysant les causes qui expliquent le peu d'engouement manifesté par les Gouvernement africains à l'égard de cette convention afin de proposer éventuellement deux textes séparés sur la cyber sécurité et la protection des données personnelles.

ANNEXE I: PRESENTATION DES ODD – FOCUS SUR L'OBJECTIF 16

Schéma synthétique des ODD :



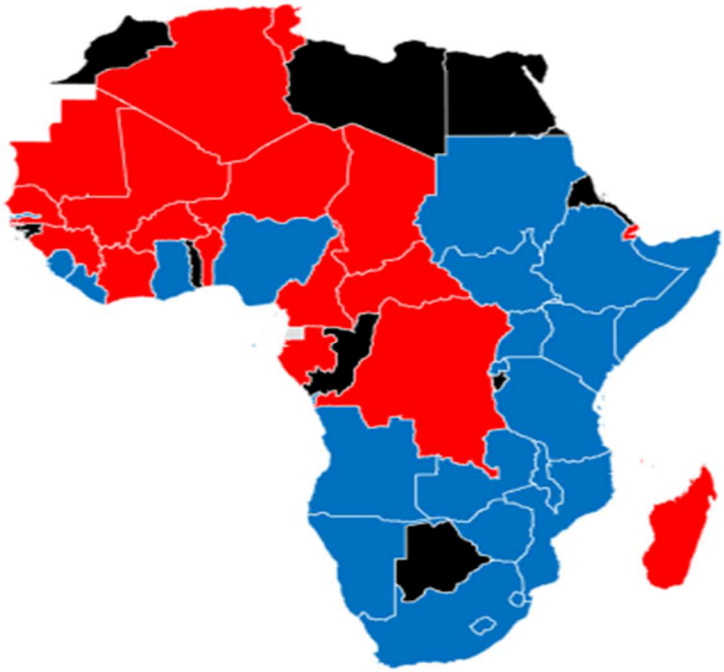
ODD n° 16 :

- 16.1 : Réduire nettement, partout dans le monde, toutes les formes de violence et les taux de mortalité qui y sont associés.
- 16.2 : Mettre un terme à la maltraitance, à l'exploitation et à la traite, et à toutes les formes de violence et de torture dont sont victimes les enfants.
- 16.3 Promouvoir l'état de droit aux niveaux national et international et donner à tous accès à la justice dans des conditions d'égalité.
- 16.4 : D'ici à 2030, réduire nettement les flux financiers illicites et le trafic d'armes, renforcer les activités de récupération et de restitution des biens volés et lutter contre toutes les formes de criminalité organisée.
- 16.5 : Réduire nettement la corruption et la pratique des pots-de-vin sous toutes leurs formes.
- 16.6 : Mettre en place des institutions efficaces, responsables et transparentes à tous les niveaux.
- 16.7 : Faire en sorte que le dynamisme, l'ouverture, la participation et la représentation à tous les niveaux caractérisent la prise de décisions.
- 16.8 Élargir et renforcer la participation des pays en développement aux institutions chargées de la gouvernance au niveau mondial.
- **16.9 : D'ici à 2030, garantir à tous une identité juridique, notamment grâce à l'enregistrement des naissances.**
- **16.10 : Garantir l'accès public à l'information et protéger les libertés fondamentales, conformément à la législation nationale et aux accords internationaux.**
- 16.a : Appuyer, notamment dans le cadre de la coopération internationale, les institutions nationales chargées de renforcer, à tous les niveaux, les moyens de prévenir la violence et de lutter contre le terrorisme et la criminalité, en particulier dans les pays en développement.
- 16.b : Promouvoir et appliquer des lois et politiques non discriminatoires pour le développement durable.

ANNEXE II: RESULTATS DE L'ENQUETE D'ID4AFRICA

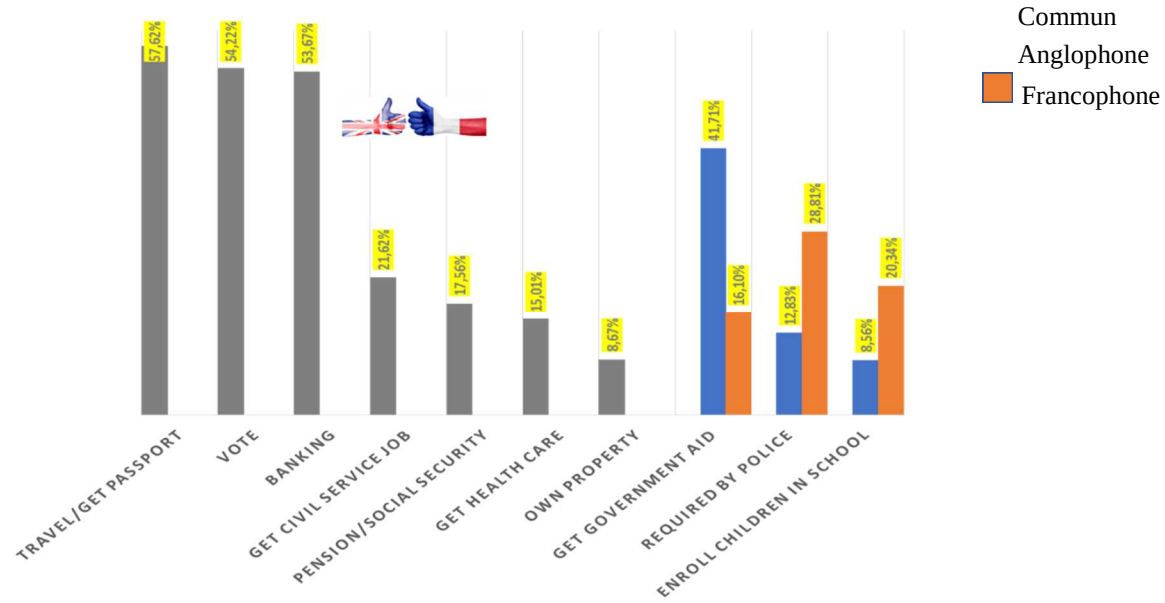
Le mouvement ID4Africa, plateforme d'échanges sur l'identité digitale au profit des pays africains, a conduit une large étude qui a vu la participation de 41 pays sur l'entièreté du continent à travers la plateforme SurveyMonkey[6]. Les résultats de ces études ont été présentés lors de la 4ème réunion annuelle d'ID4Africa organisée à Abuja (Nigéria) du 24 au 26 avril 2018.

Ci-après les pays (anglophones en bleu et francophones en rouge) qui ont répondu et ceux qui n'ont pas donné suite à l'étude (en noir) :



Résultats de l'étude :

Applications (fonctionnelles) de l'identité sur le continent :

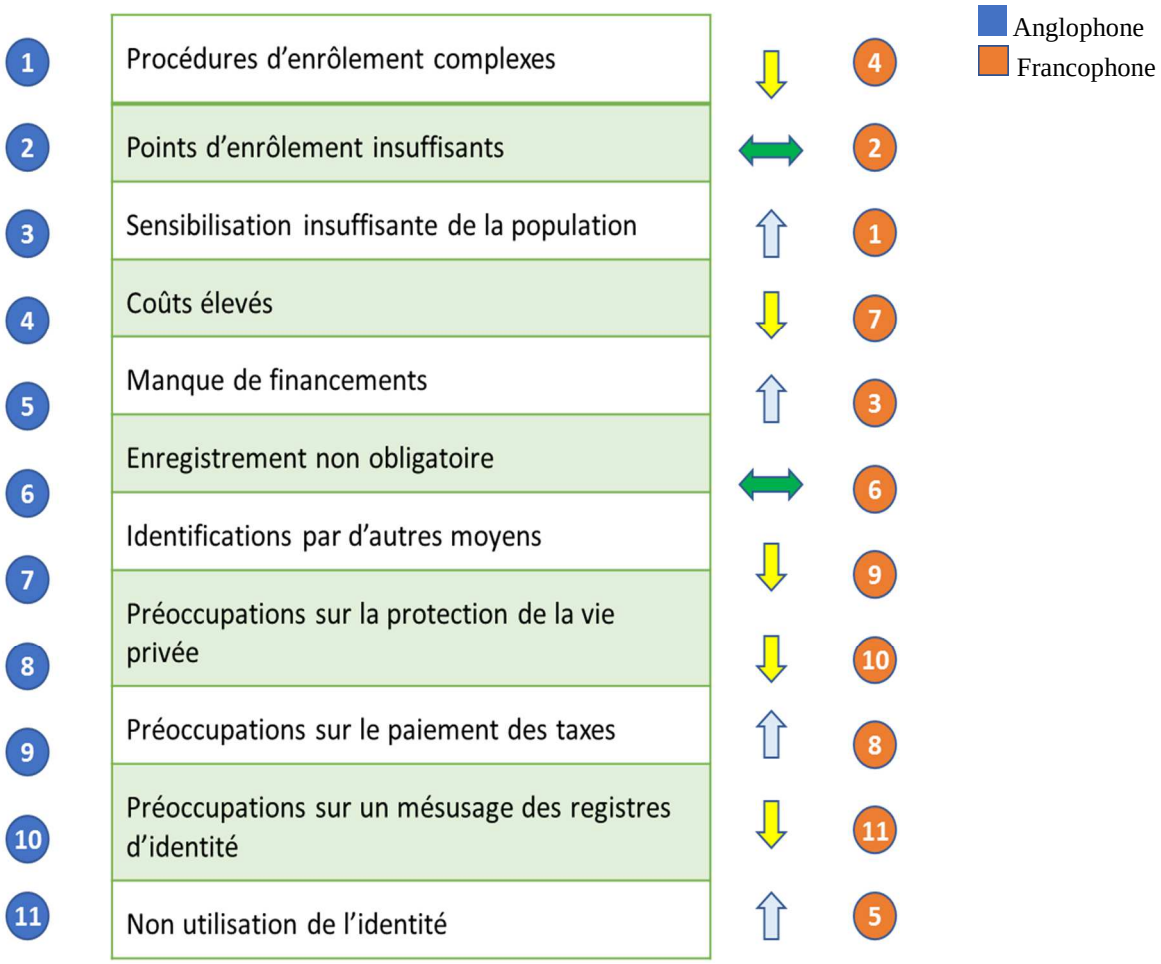


[6] 350 réponses ont été reçues dont 300 complètes.
Les réponses qui étaient complètes à hauteur de 80% ont été considérées.

Observations : Tout d'abord, il convient de souligner que les trois usages les plus plébiscités sont les suivants : (i) documents de voyage (passeports, en particulier) ; (ii) processus électoral (fichier, en particulier) ; et (iii) services bancaires. De plus, il convient aussi de remarquer la nette différence entre les pays francophones et anglophones sur le recours aux ressources publiques ainsi que l'exigence d'une preuve d'identité par la police et pour les besoins de l'inscription des enfants à l'école.

A cet effet, ces résultats sont donc encourageants dans la promotion de l'usage l'identité (digitale) dans des domaines aussi essentiels que la fiabilisation des processus électoraux, sources de beaucoup de tensions socio-politiques sur le continent (et en particulier en Afrique subsaharienne), l'inclusion financière à travers la multitude de services financiers digitaux proposés à travers le continent par les opérateurs télécoms notamment. La première place occupée par les documents de voyage est symptomatique du fait que le chemin vers l'intégration africaine (qui passe par un usage restreint des passeports uniquement pour les voyages hors du continent) est encore long. Une exception à cela tout de même car la CEDEAO a réussi à instaurer un cadre harmonisé permettant aux citoyens des pays concernés de circuler librement munis d'une pièce d'identité uniquement.

Raisons de la couverture limitée des systèmes d'identité nationale :

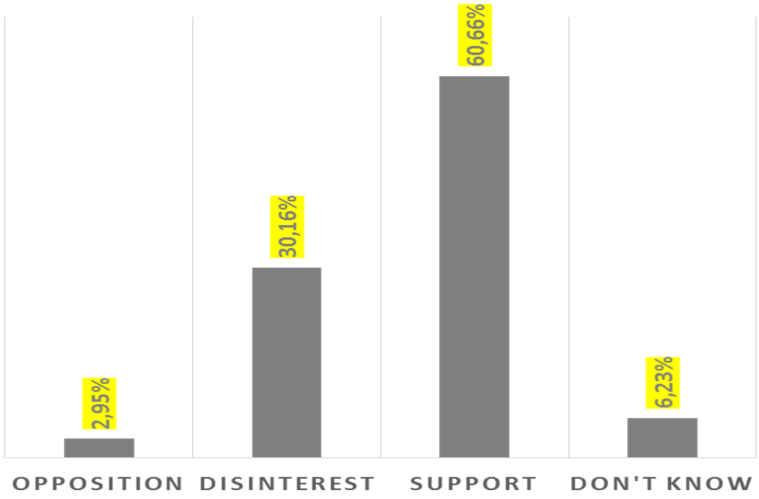


Observations : Pour les pays anglophones, voici les cinq principales raisons expliquant la couverture et donc l'utilisation limité des systèmes d'identité nationaux : (i) procédures d'enrôlement complexes ; (ii) points d'enrôlement insuffisants ; (iii) sensibilisation insuffisante

de la population ; (iv) coûts élevés ; et (v) manque de financements. Pour les francophones, il s'agit de : (i) sensibilitation insuffisante de la population ; (ii) points d'enrôlement insuffisants ; (iii) manque de financements ; (iv) procédures d'enrôlement complexe ; et (v) non utilisation de l'identité dans la vie quotidienne.

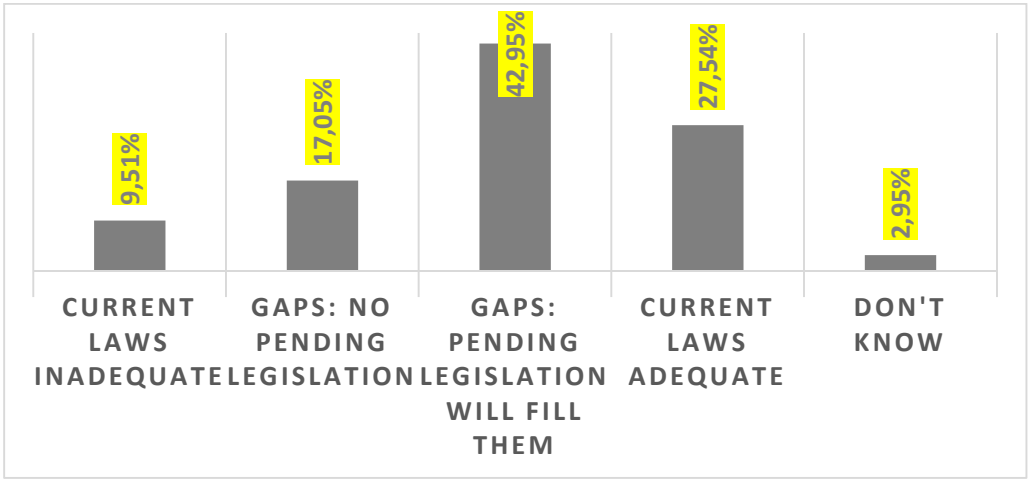
Eu égard à ce qui précède, il convient donc de souligner que les pays africains sont, d'une manière générale, d'accord sur l'importance des infrastructures digitales, la gouvernance du paysage de l'identité digitale et des financements requis.

Attitude des populations locales par rapport aux systèmes d'identité :



Observations : A la lumière du graphique précédent, l'on peut noter le fort intérêt des populations locales dans les systèmes d'identité. Par ailleurs, ces données confortent aussi la nécessité de prévoir un volet d'accompagnement dans les projets d'identité digitale afin de couvrir les besoins en formations (à la fois pour les aspects techniques, fonctionnelles et d'utilisation finale) et en campagnes de communication utilisant des moyens accessibles pour les populations de l'arrière-pays dans le contexte africain.

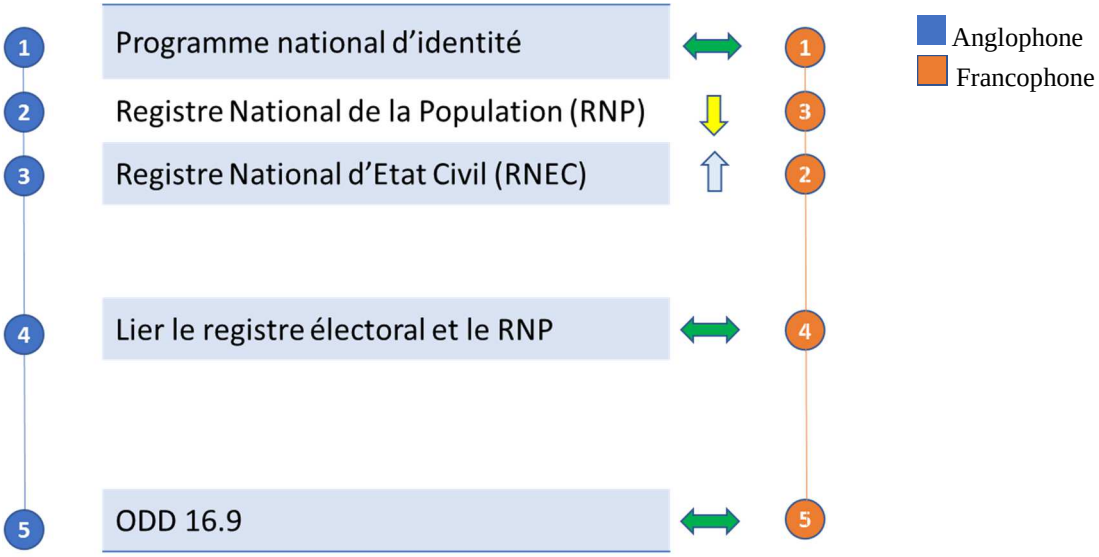
Cadre juridique :



Observations : Les résultats ci-haut dénotent un gap réel en termes de cadre juridique applicable à l'identité digitale et plus largement dans les domaines connexes (protection des données personnelles, cybersécurité, etc.). L'étude a permis aussi dans le cadre des réponses qualitatives reçues d'aboutir aux conclusions suivantes :

(i) Nécessité d'une harmonisation des cadres juridiques nationaux et régionaux ;
(ii) Rendre obligatoire l'utilisation du NIP au niveau national à travers la loi ;
(iii) Sensibilisation du législateur pour une prise de conscience nationale sur les avantages et les inconvénients de l'identité digitale ; et
(iv) Nécessité de protéger l'indépendance des organes de gestion de l'identité digitale à travers la loi.

Niveaux d'engagement politique dans les systèmes d'identité nationaux :



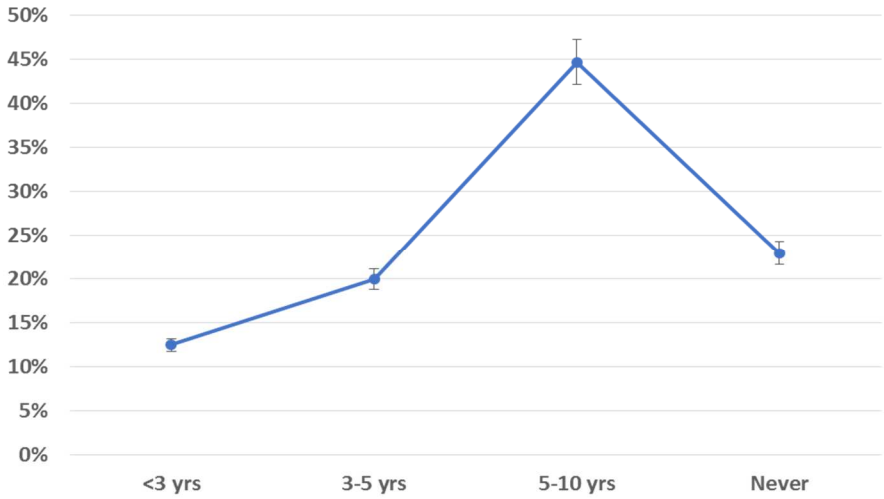
Observations : Il est intéressant de constater que, fondamentalement, les pays ayant répondu associent fortement le RNP et le RNEC dans le cadre de leurs programmes nationaux d'identité. Néanmoins, il convient aussi de remarquer qu'il y a quelques préoccupations exprimées dans le lien direct entre les RNP et les registres électoraux car il y a, en filigrane, la problématique des commissions nationales électorales nationales qui occupent encore des positions prééminentes. Par contre, la peu d'intérêt manifesté sur l'ODD 16.9 reste préoccupant d'autant qu'il s'agit d'un engagement planétaire pour garantir à tous une identité juridique, notamment grâce à l'enregistrement des naissances, d'ici 2030. Au passage, il convient de rappeler que, pratiquement, la moitié des personnes concernées par cet objectif sont africaines.

Systèmes d'identité & Démocratie :

Question posée aux pays participants : Est-ce une bonne idée d'utiliser la biométrie pour fiabiliser les processus électoraux ?
Réponses obtenues : OUI franc et massif -> 97% pour les pays anglophones et 98% pour les pays francophones.

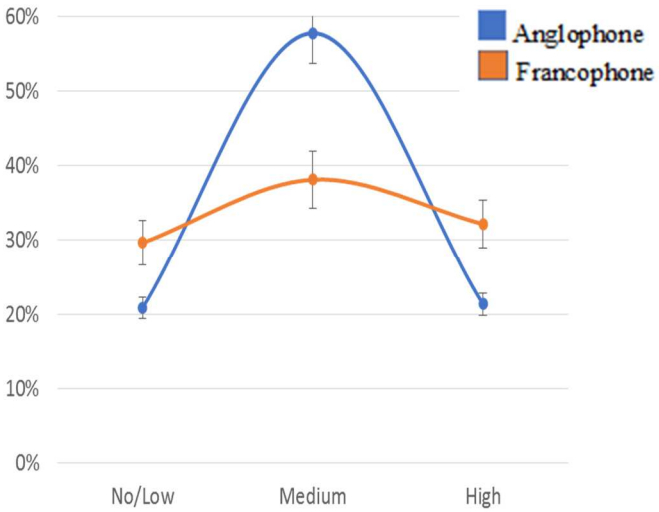
Observations : Il n'y a donc aucun doute sur la perception positive de la biométrie dans l'organisation des élections. Néanmoins, il convient, de mon point de vue, d'aller plus loin car la question centrale reste celle-ci relative de la mise en place d'une base de données biométrique unique qui servirait à l'authentification de tous les systèmes fonctionnels (santé, éducation, protection sociale, élection, etc.). Il convient de signaler que cela coûte des sommes considérables à beaucoup de pays africains qui pourraient éviter cela grâce à la mutualisation précitée.

La question sous-jacente suivante a également été demandée aux pays participants : sous quels délais pensez que votre pays mettra en place un système national de vote électronique ?
Résultants :

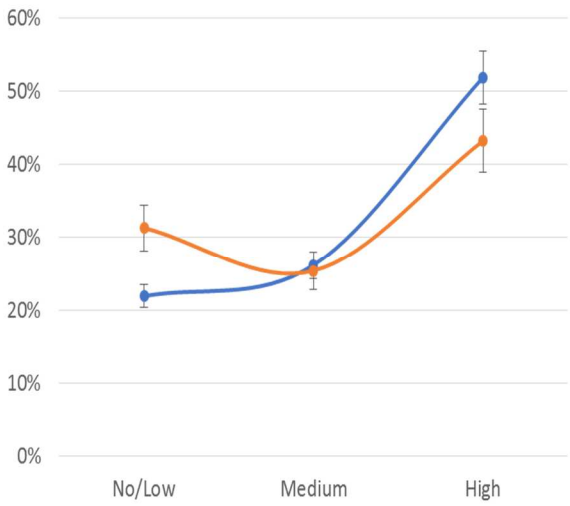


Eu égard à ce qui précède, il faudra donc à la fois travailler avec les pays africains dans la mise en place des données biométriques mutualisées tout en les assistant dans la mise en place d'organe de contrôle (type Instance de protection des données personnelles) et de cadre juridique adéquat pour éviter la manipulation de ces données extrêmement sensibles.

Protection des données personnelles et de la vie privée :



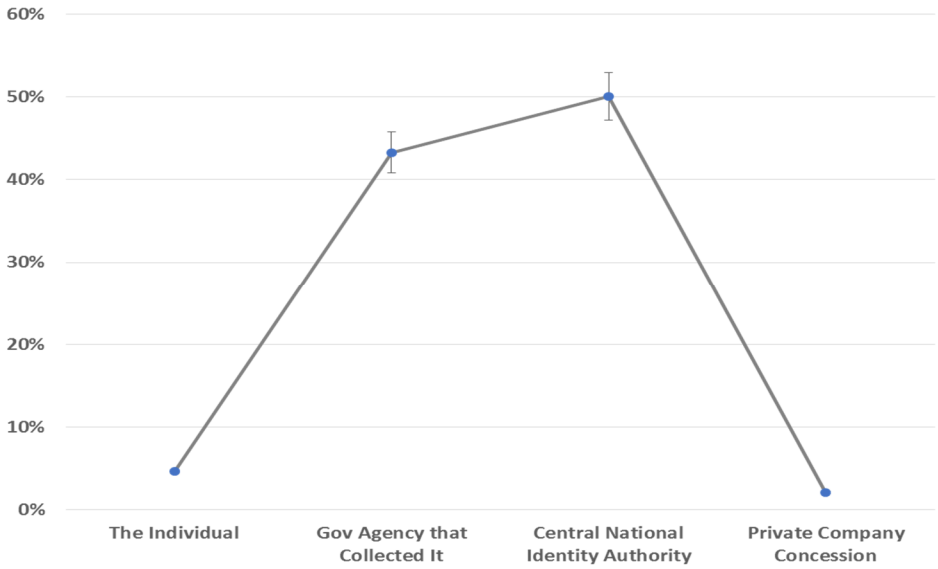
Protection des données personnelles



Protection de la vie privée

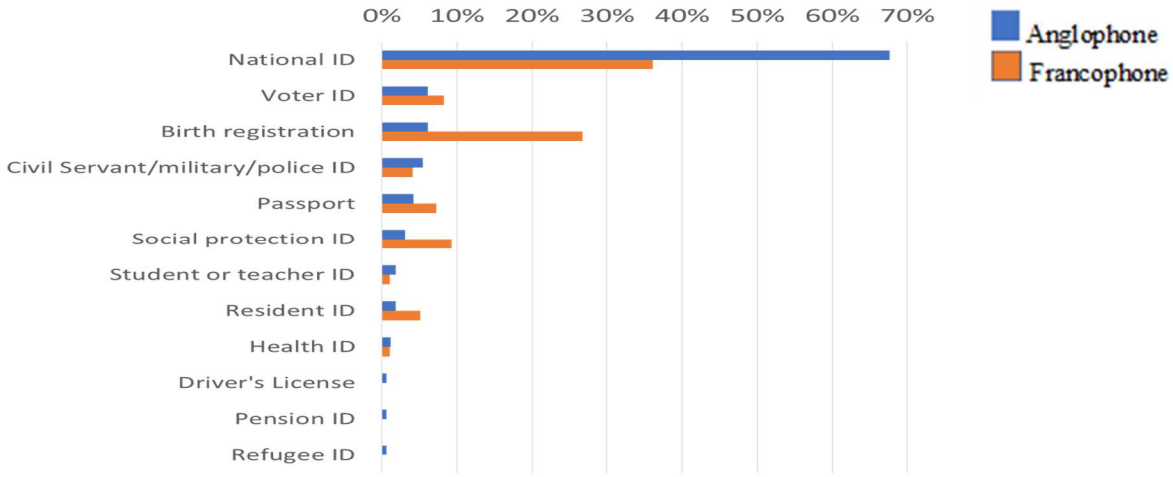
Question posée : quelle est votre niveau de préoccupation par rapport aux deux sujets ci-haut ?
Observations : D'une manière générale, l'on observe beaucoup plus de préoccupations sur la protection de la vie privée (concept plus ancien) que la protection des données personnelles. D'où la grande attente de ces pays vis-à-vis des bailleurs de fonds internationaux (bilatéraux et multilatéraux) ainsi que les agences internationales spécialisées pour les accompagner dans la mise en place de cadres nationaux de protection de la vie privée et de la protection des données personnelles.

Ancrage institutionnelle des systèmes d'identité :



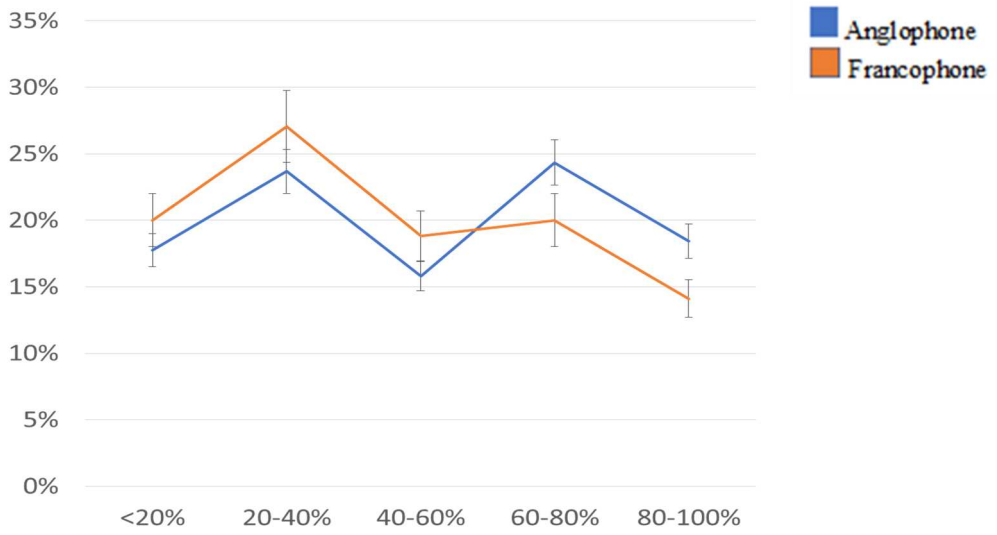
Observations : Les résultats ci-haut traduisent, d'une manière générale, les trois points suivants : (i) l'absence d'un consensus national observés dans les pays en matière d'ancrage institutionnel de la plateforme d'identité fondamentale (par opposition aux systèmes fonctionnels qui peuvent dépendre des entités qui en déjà la charge) ; (ii) la problématique de la centralisation versus décentralisation ; et enfin (iii) la place du secteur privé dans le montage des systèmes d'identité nationaux. Il convient de noter, à ce titre, la réticence des représentants des gouvernements consultés par rapport à des collaborations avec le secteur privé pour des raisons de souveraineté national.

Systèmes d'identité existants :



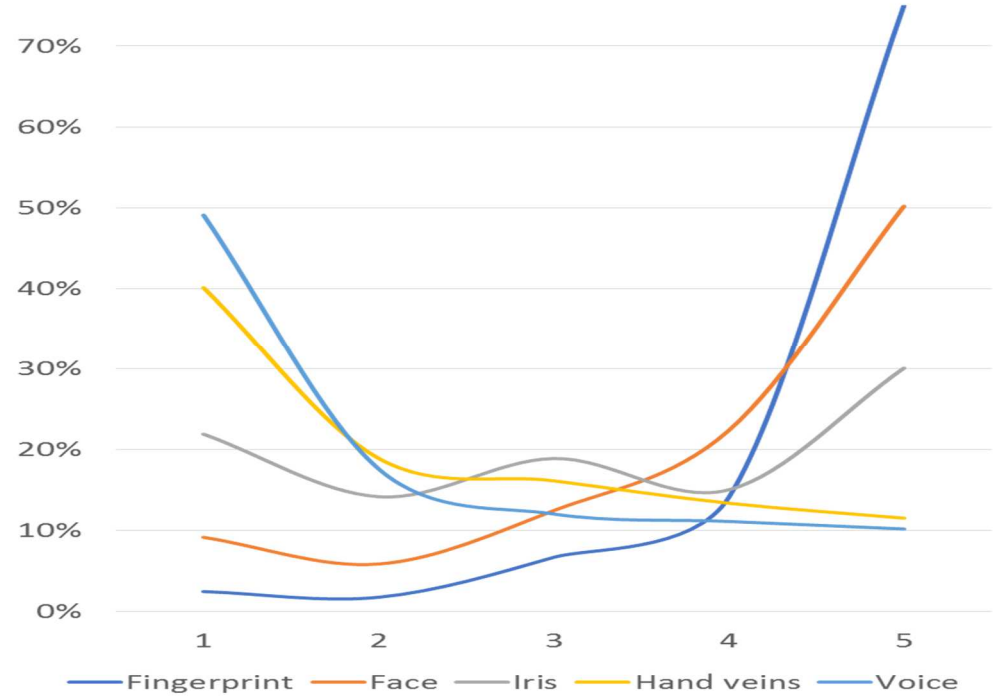
Observations : Il convient de noter une nette différence entre les pays anglophones et francophones sur le recours aux systèmes d'identité fondamentaux et fonctionnels. En effet, il semblerait que les pays anglophones privilégient plutôt les systèmes d'identité fondamentaux plutôt que les systèmes fonctionnels contrairement aux pays francophones.

Couverture des systèmes d'identité nationaux :



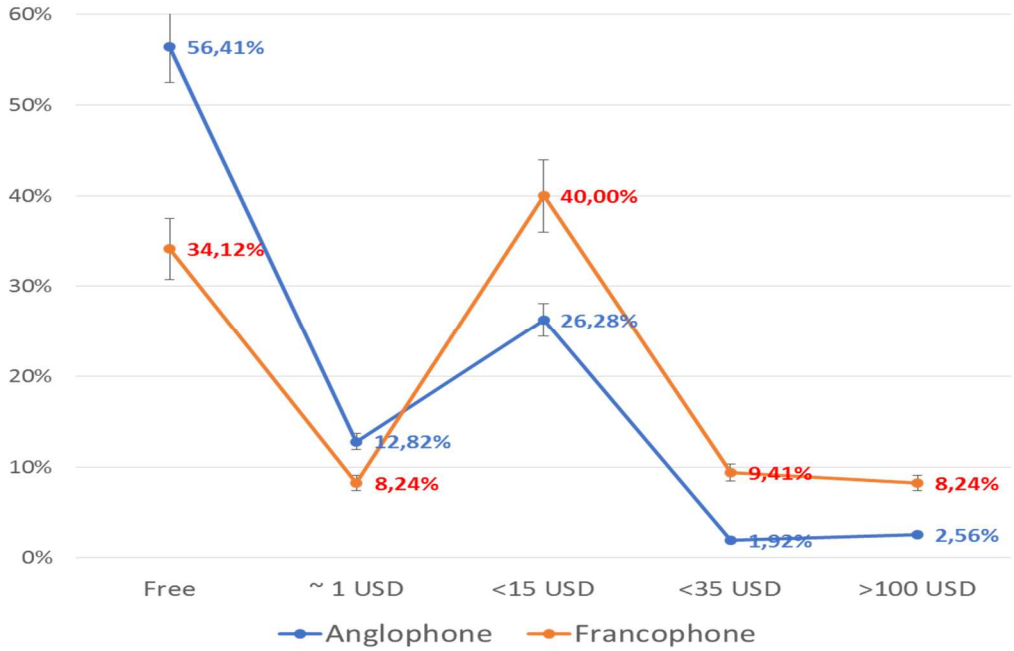
Observations : Les résultats ci-haut nous renseignent qu'il y a très peu de pays africains (moins de 20% sur ceux interrogés) qui disposent d'un système d'identité couvrant tout le pays. D'où l'immensité de la tâche qui attend l'ensemble des acteurs mondiaux engagés sur ce secteur avec en ligne de mire 2030 pour concrétiser l'ODD 16.9.

Appétence pour les différentes technologies biométriques existantes :



Observations : il convient de signaler qu'il n'y a pas de différences notables entre pays anglophones et francophones. Les deux technologies qui sont plus appréciés sont les empreintes digitales et la reconnaissance faciale. Cette problématique est d'autant plus importante qu'elle est une clé pour la mise en place de systèmes d'identité digitaux efficients dans un contexte africain marqué par un gap infrastructurel et énergétique conséquent, surtout dans les régions centrale et de l'Ouest.

Coûts des documents d'identité pour les utilisateurs finaux :



Observations : Il est intéressant de noter que les pays anglophones sont plus disposés à des coûts faibles, voire nuls, pour l'accès aux documents d'identité contrairement aux pays francophones. Cette question est éminemment importante car le talon d'Achille de systèmes d'identité sophistiqués (et donc couteux) reste les coûts d'accès qui peuvent être rédhibitoires pour les franges les plus pauvres des populations des pays considérés. D'où la prise en compte du facteur d'exclusion sur les coûts qui peut se révéler problématique sur le chemin de la généralisation recherchée des systèmes d'identité nationaux.