

État des lieux sur la liberté de l'Internet en Afrique 2022

# L'essor de la surveillance biométrique

Septembre 2022



# Table des matières

## 1

### **Introduction 3**

1.1 Contexte de l'étude 4

1.2 Méthodologie de l'étude 6

## 2

### **Résultats : Tendances dans l'adoption de la collecte de données biométriques 7**

2.1 Cadre juridique de la collecte de données biométriques 7

2.2 Programmes de collecte de données biométriques 9

2.2.1 Registres d'état civil, y compris la délivrance de cartes d'identité nationales 9

2.2.2 Programmes d'enregistrement et d'identification biométriques des électeurs 13

2.2.3 Programmes de vidéosurveillance dirigés par le gouvernement avec reconnaissance faciale 18

2.2.4 Programmes nationaux de passeport électronique biométrique 22

2.2.5 Programmes de traitement des données biométriques utilisés dans l'enregistrement des réfugiés 26

2.2.6 Programmes d'enregistrement biométrique des cartes SIM 28

2.2.7 Collecte de données biométriques par des entreprises étrangères 31

2.3 Collecte et traitement des données biométriques des mineurs 31

2.4 Justifications du traitement des données biométriques 32

## 3

### **Discussion : tendances, risques potentiels, défis et lacunes 35**

3.1 Campagnes limitées de mobilisation et de sensibilisation du public 35

3.2 Cadres juridiques inadéquats augmentant les risques pour la vie privée 37

3.3 Exclusion de l'accès aux services essentiels 38

3.4 Amélioration de la surveillance, du profilage et du ciblage 40

3.5 Conflits d'intérêts et pouvoir des tiers 42

3.6 Capacité et formation limitées 44

## 4

### **Conclusion et Recommendations 45**

4.1 Conclusion 45

4.2 Recommendations 47



Creative Commons Attribution 4.0 Licence  
«creativecommons.org/licenses/by-nc-nd/4.0»  
Some rights reserved.

# 1.0 Introduction

Les technologies, y compris les systèmes biométriques, présentent de nouvelles opportunités et de nouveaux défis en matière de vie privée, de liberté d'expression, d'accès à l'information, d'égalité et de non-discrimination. La biométrie fait référence à la mesure et à l'analyse de caractéristiques physiques ou comportementales telles que les groupes sanguins, les empreintes digitales, l'acide désoxyribonucléique (ADN), le motif rétinien, le thermogramme facial, la géométrie de la main et la voix pour vérifier l'identité d'une personne.<sup>1</sup> Ces caractéristiques sont souvent liées à d'autres renseignements biographiques personnels dans des bases de données contenant les noms, les coordonnées, les caractéristiques démographiques, les antécédents médicaux, les opinions et la correspondance des personnes. Une fois consolidées, les bases de données peuvent être utilisées de différentes manières pour faciliter la prestation de services grâce à des applications dans des domaines tels que l'identification et la vérification numériques, l'inscription et l'identification des électeurs,<sup>2</sup> l'enregistrement de la carte SIM, la délivrance de permis de conduire, la surveillance de COVID-19, les transactions et paiements financiers, la protection sociale, les services aux réfugiés, la délivrance de passeports et de visas, le contrôle aux frontières, le contrôle de la circulation, les soins de santé reçus, la Gestion de la migration<sup>3</sup> et le contrôle d'accès aux appareils, aux systèmes et aux locaux.

Le droit à la confidentialité est reconnu dans plusieurs instruments régionaux et internationaux relatifs aux droits de l'homme et est garanti dans les constitutions nationales de nombreux États africains. L'un de ces instruments est la Déclaration de 2019 de la Commission africaine des droits de l'homme et des peuples (CADHP) sur les principes de la liberté d'expression et de l'accès à l'information en Afrique, qui prévoit dans son Principe 40 que « Toute personne a droit à la vie privée, y compris la confidentialité de ses communications et la protection de ses informations personnelles ». La déclaration appelle en outre les États membres de l'Union africaine, dans son principe 42, entre autres, à adopter des lois pour la protection des informations personnelles des individus conformément aux lois internationales sur les droits de l'homme et aux normes qui prévoient des principes de confidentialité, des recours efficaces et une surveillance adéquate. Des efforts délibérés ont été déployés par les États pour se conformer aux normes établies. Cependant, des défis subsistent comme les acteurs étatiques et non étatiques sont aux prises avec la conception et la mise en œuvre de programmes basés sur la technologie biométrique.

Ce rapport documente les tendances émergentes et actuelles en matière de collecte et de traitement des données biométriques en Afrique. Il se concentre sur le déploiement de programmes nationaux basés sur la technologie biométrique sur le continent, ainsi que sur les caractéristiques, les lacunes et les risques associés à la protection des données et de la vie privée.

<sup>1</sup> Voir, par exemple, le dictionnaire libre, « biométrie », <https://www.thefreedictionary.com/biometrics>

<sup>2</sup> Introduction de la technologie biométrique dans les élections <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>

<sup>3</sup> L'OIM et la biométrie [https://www.iom.int/sites/g/files/tmzbd486/files/our\\_work/DMM/IBM/iom\\_and\\_biometrics\\_external\\_info\\_sheet\\_november\\_2018.pdf](https://www.iom.int/sites/g/files/tmzbd486/files/our_work/DMM/IBM/iom_and_biometrics_external_info_sheet_november_2018.pdf)

## 1.1 Contexte de l'étude

Les programmes de collecte de données biométriques numériques sont de plus en plus populaires sur tout le continent.<sup>4</sup> Les gouvernements investissent dans divers programmes numériques<sup>5</sup> pour permettre la saisie d'informations biométriques de leurs citoyens à diverses fins. En effet, ces programmes ont pris de l'ampleur et ont été salués comme des catalyseurs essentiels du développement. Ils devraient également accélérer la reconnaissance et l'enregistrement de 494 millions de personnes en Afrique subsaharienne qui représentent 45% des personnes dans le monde qui n'ont aucune forme de preuve officielle d'identité légale.<sup>6</sup>

Les cartes d'identité numériques remplacent progressivement les anciennes cartes d'identité en papier. Les cartes d'identité numériques prennent la forme d'applications pour smartphones ou de cartes à puce qui utilisent des technologies telles que Bluetooth, la communication en champ proche (NFC),<sup>7</sup> l'identification par radiofréquence (RFID),<sup>8</sup> la technologie blockchain<sup>9</sup> et l'infrastructure à clé publique (PKI).<sup>10</sup> Elles ont le potentiel de fournir des solutions rapides, efficaces et sécurisées aux autorités qui les émettent et leur capacité à interagir avec d'autres systèmes et bases de données est un autre avantage. Elles sont appliquées de différentes manières pour les services gouvernementaux et les applications commerciales ou pour consommateurs dans différents secteurs.

Jusqu'en 2021, 136 pays avaient mis en œuvre des programmes d'identification numérique représentant 3,6 milliards de cartes d'identité numériques en circulation.<sup>11</sup> En outre, 82 % de tous les pays délivrant des cartes d'identité nationales ont mis en œuvre des programmes d'identification numérique qui dépendent des cartes d'identité numériques à puce ou des cartes en plastique et de la biométrie. Cette demande a créé un marché mondial de cartes d'identité numériques qui est passé de 18 milliards USD en 2018 à 44,7 milliards USD en 2022, selon Acuity Market Intelligence, avec un marché des cartes d'identité biométriques et numériques en Afrique estimé à 1,4 milliard USD.<sup>12</sup>

La pandémie de COVID-19 a accru<sup>13</sup> la nécessité de prouver l'identité et, en même temps, a renforcé l'utilisation de nouvelles technologies biométriques sans contact telles que la reconnaissance faciale et les scanographies d'iris, car les gens évitaient les dispositifs biométriques nécessitant des contacts tels que l'empreinte palmaire, les empreintes digitales et les lecteurs de clés manuelles, ce qui a accéléré la transformation numérique dans plusieurs pays. De même, l'augmentation de l'accès aux smartphones, de la couverture de la téléphonie mobile et des taux de pénétration d'Internet sur le continent sont des moteurs clés des programmes biométriques, avec 120 millions d'abonnés supplémentaires attendus en Afrique subsaharienne d'ici 2025, contre 495 millions enregistrés en décembre 2020.<sup>14</sup> Les technologies et services mobiles devraient générer 155 milliards USD de valeur économique d'ici 2025, contre 130 milliards enregistrés en 2020.

<sup>4</sup> Données biométriques : 100 pays classés en fonction de la façon dont ils les collectent et de ce qu'ils en font <https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/>

<sup>5</sup> La biométrie : ami ou ennemi de la vie privée? [https://privacyinternational.org/sites/default/files/2017-11/Biometrics\\_Friend\\_or\\_foe.pdf](https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf)

<sup>6</sup> Le défi mondial de l'identification en chiffres <https://id4d.worldbank.org/global-dataset/visualization>

<sup>7</sup> La communication en champ proche est un ensemble de protocoles de communication qui permet la communication entre deux appareils électroniques sur une distance de 4 cm ou moins. <https://developer.android.com/guide/topics/connectivity/nfc>

<sup>8</sup> L'identification par radiofréquence utilise des champs électromagnétiques pour identifier et suivre automatiquement les étiquettes attachées aux objets. Un système RFID se compose d'un minuscule transpondeur radio, d'un récepteur radio et d'un émetteur. <https://www.abr.com/what-is-rfid-how-does-rfid-work/>

<sup>9</sup> La technologie Blockchain permet aux utilisateurs de créer et de gérer des identités numériques grâce à la combinaison des identifiants décentralisés suivants, de la gestion des identités et cryptage intégré. <https://consensus.net/blockchain-use-cases/digital-identity/>

<sup>10</sup> L'infrastructure à clé publique (PKI) est l'ensemble du matériel, des logiciels, des politiques, des processus et Procédures requises pour créer, gérer, distribuer, utiliser, stocker et révoquer des certificats numériques et des clés publiques. Les PKI sont la base qui permet l'utilisation de technologies, telles que les signatures numériques et le cryptage, auprès de vastes populations d'utilisateurs. <https://bit.ly/3Cdbolx>

<sup>11</sup> Le défi mondial de l'identification en chiffres <https://id4d.worldbank.org/global-dataset/visualization>

<sup>12</sup> L'identification biométrique : un marché africain convoité <https://www.theafricareport.com/30838/biometric-identification-a-coveted-african-market/>

<sup>13</sup> Les défis de l'empreinte digitale : les identités numériques vont-elles révolutionner Service Delivery en Afrique subsaharienne? <https://africanarguments.org/2022/03/challenges-of-fingerprinting-will-digital-ids-revolutionne-service-delivery-in-sub-saharian-africa/>

<sup>14</sup> L'économie mobile Afrique subsaharienne 2021 [https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA\\_ME\\_SSA\\_2021\\_English\\_Web\\_Singles.pdf](https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/09/GSMA_ME_SSA_2021_English_Web_Singles.pdf)

Les champions de la collecte de données biométriques, tels que les gouvernements, l'Union africaine (UA), la Banque mondiale, les organisations non gouvernementales (ONG) et les acteurs du secteur privé tels que les banques, les télécommunications et le secteur de la sécurité, affirment que ces systèmes sont importants pour identifier, authentifier et vérifier avec précision l'identité des individus, notamment en facilitant les exigences du connais-ton-client (KYC);<sup>15</sup> assurer la fourniture d'une identité juridique conformément à l'Objectif de Développement Durable (ODD) No 16.9; promouvoir la sécurité nationale; renforcer la démocratie<sup>16</sup> et l'intégrité des élections;<sup>17</sup> prévenir la fraude financière et d'identité, le vol d'identité, lutter contre la corruption et contre le terrorisme.

En outre, les champions affirment que ces systèmes renforcent la confiance dans les systèmes d'identification et de paiement; améliorent les services du secteur financier; facilitent la prestation efficace de services sociaux, y compris les programmes de santé en ligne, d'aide et de protection sociale; améliorent la qualité des données en éliminant la duplication des enregistrements; contrôlent l'accès physique et numérique aux locaux et aux systèmes numériques; améliorent la sécurité des données; relient les bases de données pour améliorer les systèmes de suivi et de rétroaction; et soutiennent la croissance de l'économie numérique.

Malheureusement, ces programmes présentent également de nouveaux risques pour la réalisation et la jouissance des droits et des libertés de l'homme. Ces programmes exigent la collecte et le traitement obligatoires de données personnelles sensibles de millions de citoyens, et la protection de la confidentialité de ces données d'un point de vue technique, juridique, réglementaire et procédural est essentielle. Notamment, les programmes, tels que la délivrance de passeports électroniques par près de 50 pays africains,<sup>18</sup> ont été mis en œuvre dans un contexte de lacunes en matière de lois complètes sur la protection des données,<sup>19</sup> de protection ou de recours adéquats et d'institutions<sup>20</sup> indépendantes de contrôle. Un peu plus de la moitié des pays du continent disposent de cadres spécifiques de protection des données. Cette situation est aggravée par l'absence de mesures efficaces et solides contre les violations de la confidentialité des données, en particulier dans les pays où la surveillance par les agences de sécurité de l'État reste mal réglementée sans processus d'audit clairs ni mécanismes d'application. Il n'existe pas non plus d'approches stratégiques claires pour le déploiement de programmes de protection et de sécurité des données, ce qui a conduit à un écosystème de gestion de l'identité surpeuplé et désorganisé.<sup>21</sup>

En plus, des programmes d'identification numérique biométrique mis en œuvre de manière incomplète pourraient renforcer l'exclusion numérique et la discrimination des groupes vulnérables dans l'accès aux services gouvernementaux. En outre, les bases de données biométriques centralisées sont généralement confrontées à des risques accrus en matière de cyber sécurité et sont vulnérables aux attaques et aux pertes,<sup>22</sup> alors que la biométrie ne peut pas être facilement remplacée comme les mots de passe et les symboles. En plus, les rôles et les responsabilités des intermédiaires impliqués dans la conception, le déploiement et la mise en œuvre de ces systèmes biométriques, dont certains utilisent les pays africains comme base de collecte de données et de mise en œuvre<sup>23</sup> de leurs technologies émergentes de méga données développées en dehors du continent, suscitent des inquiétudes. Les systèmes biométriques dotés d'une capacité de reconnaissance faciale<sup>24</sup> peuvent être utilisés passivement à des fins de surveillance, éliminant ainsi l'exigence de consentement, et donc utilisés à l'insu de la personne concernée ou sans sa participation.

<sup>15</sup> Réinventer les écosystèmes identitaires en Afrique subsaharienne avec le mobile

<https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/12/Reimagining-identity-ecosystems-en-Afrique-subsaharienne-avec-mobile.pdf>

<sup>16</sup> La biométrie : ami ou ennemi de la vie privée? [https://privacyinternational.org/sites/default/files/2017-11/Biometrics\\_Friend\\_or\\_foe.pdf](https://privacyinternational.org/sites/default/files/2017-11/Biometrics_Friend_or_foe.pdf)

<sup>17</sup> Les technologies biométriques et la perspective d'une démocratie durable en Afrique <https://eisa.org/pdf/JAE20.1dowu.pdf>

<sup>18</sup> Les pays africains adoptent la biométrie et les identités numériques

<https://www.un.org/africarenewal/magazine/february-2021/african-countries-embracing-biometrics-digital-ids>

<sup>19</sup> Cartographie et analyse des lois et politiques en matière de protection de la vie privée en Afrique [https://cipesa.org/?wpfb\\_dl=454](https://cipesa.org/?wpfb_dl=454)

<sup>20</sup> Les activistes tirent la sonnette d'alarme sur les projets d'identification biométrique africains

<https://www.aljazeera.com/economy/2020/12/10/activists-sound-alarm-over-african-biometric-id-projects>

<sup>21</sup> Vers l'évaluation des écosystèmes d'identification socio-numérique en Afrique <https://www.ictworks.org/wp-content/uploads/2022/01/digital-id-african-country.pdf>

<sup>22</sup> Protection des renseignements personnels en Afrique du Sud : un cadre pour les données biométriques Sécurité de la collection

[https://www.thinkmind.org/articles/internet\\_2016\\_1\\_10\\_40022.pdf](https://www.thinkmind.org/articles/internet_2016_1_10_40022.pdf)

<sup>23</sup> Qui regarde qui? Surveillance biométrique au Kenya et en Afrique du Sud <https://enact-africa.s3.amazonaws.com/site/uploads/2020-11-11-biometrics-research-paper.pdf>

<sup>24</sup> Collecte de données biométriques et reconnaissance faciale

<https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-sécurité-en-ligne/collecte-de-données-biométriques-et-reconnaissance-faciale/>



## 1.2 Méthodologie de l'étude

Cette étude examine la mise en œuvre de certains programmes nationaux de biométrie dans 16 pays africains, dont l'Angola, le Cameroun, la République centrafricaine, la République démocratique du Congo, le Kenya, le Lesotho, le Libéria, le Mozambique, le Nigéria, le Sénégal, la Sierra Leone, la Tanzanie, le Togo, la Tunisie, l'Ouganda et la Zambie. L'étude a utilisé une approche qualitative comprenant une analyse documentaire, une analyse des politiques et des questions juridiques, ainsi que des entrevues avec des informateurs clés avec des répondants sélectionnés à dessein. Des rapports d'études antérieures, des reportages dans les médias, des travaux universitaires, des documents gouvernementaux et d'autres documents ont également été examinés. La revue de la littérature a permis aux chercheurs de mieux comprendre les développements actuels, les avantages, les lacunes, les défis, les débats et les questions sur les programmes biométriques et la protection de la vie privée et des données dans les pays cibles.

L'analyse juridique et stratégique comprenait un examen des lois, des politiques et des pratiques relatives à la biométrie et au droit à la vie privée. L'étude a également passé en revue les progrès de certains programmes nationaux de biométrie, y compris ceux mis en œuvre par des acteurs non étatiques qui présentent des risques importants pour la vie privée, et a formulé des recommandations à l'intention de diverses parties prenantes.

Des entrevues avec des informateurs clés (ICM) ont été menées auprès de répondants choisis à dessein qui connaissaient bien les questions à l'étude. Parmi elles figuraient des défenseurs des droits des femmes, des membres du personnel d'entreprises privées, des ministères, des régulateurs des télécommunications, des médias et des associations de consommateurs. De plus, des universitaires, des avocats et des utilisateurs de médias sociaux ont été interrogés.

# Résultats: Tendances dans l'adoption de la collecte des données biométriques

*Cette section présente les résultats de la recherche. Il passe en revue les différentes lois et politiques qui affectent la collecte de données biométriques. Il examine également les différents programmes de collecte de données biométriques mis en œuvre dans les pays étudiés. Dans les différents pays, les programmes biométriques les plus répandus comprennent ceux liés à l'enregistrement des faits d'état civil, tels que la délivrance de cartes nationales d'identité, les programmes d'enregistrement et d'identification biométriques des électeurs, les programmes de vidéo surveillance dirigés par le gouvernement avec des capacités de reconnaissance faciale, les initiatives nationales de passeport électronique, l'enregistrement des réfugiés et l'enregistrement biométrique obligatoire de la carte SIM.*

## 2.1 Cadre juridique de la collecte de données biométriques

Les constitutions nationales des pays étudiés garantissent la protection de la vie privée, y compris des données personnelles. Au moins 30 pays à travers le continent ont, en plus des dispositions constitutionnelles, promulgué des lois et des politiques pour assurer la protection des données.<sup>25</sup> Cependant, plusieurs pays ont des dispositions légales qui légitiment les programmes de collecte et de traitement des données biométriques tels que l'enregistrement des cartes SIM, l'inscription des électeurs et l'identification nationale.<sup>26</sup>

Les principales lois habilitantes pour la collecte de données biométriques dans les pays étudiés sont celles relatives à l'enregistrement des faits d'état civil, à l'immigration, aux élections, aux services financiers et aux télécommunications. Ces lois, en particulier en Angola, au Cameroun, en République centrafricaine, en République démocratique du Congo, au Kenya, au Lesotho, au Libéria, au Mozambique, au Nigeria, au Sénégal, en Sierra Leone, en Tanzanie, au Togo, en Tunisie, en Ouganda et en Zambie, permettent la collecte d'empreintes digitales, de photos et de signatures avant la délivrance de documents officiels tels que les cartes d'identité et les passeports. Dans d'autres pays comme le Kenya, le Nigeria et la Zambie, les scans de l'iris sont également obligatoires.

En outre, les pays étudiés utilisent également les autorités nationales d'identification établies comme moyen de collecter des données biométriques avant la délivrance des cartes d'identité nationales. En Sierra Leone, d'autres types d'informations qui, selon la loi, devraient être recueillies comprennent celles relatives au groupe sanguin, à la couleur des yeux et à la taille. D'autre part, l'Ouganda est en train de mettre en œuvre une mise à niveau du système national d'identification afin d'inclure les données ADN, d'empreintes palmaires et de scanographie oculaire dans les détails de l'individu dans le registre national. Une loi exigeant la collecte de l'ADN et des coordonnées GPS pour l'enregistrement de l'identité au Kenya a été déclarée anti constitutionnelle. En outre, les lois sur les processus électoraux ont été largement utilisées pour collecter des données, y compris des photos et des empreintes digitales, aux fins de l'identification des électeurs, et sont dans certains cas liées à des données provenant de bases de données officielles d'enregistrement à l'État civil telles que les cartes d'identité numériques et les passeports, qui sont souvent nécessaires pour l'inscription des électeurs.

<sup>25</sup> Olumide Babalola, « Régime juridique de la protection des données et gouvernance des données en Afrique : un aperçu, 2022 », <https://www.africaportal.org/documents/22659/DG003.pdf>

<sup>26</sup> Pour une analyse détaillée des différentes lois sur la protection de la vie privée et des données, y compris sur la biométrie, veuillez consulter le rapport 2022 du CIPESA; Vie privée en péril: Une analyse de la surveillance, du cryptage et des lois de la localisation des données en Afrique [https://cipesa.org/?wpfb\\_dl=492](https://cipesa.org/?wpfb_dl=492)

Bien qu'il y ait eu une collecte massive de données biométriques en utilisant différentes lois, la protection des données est insuffisante. Dans certains pays, il n'existe pas de lois sur la protection des données. Dans d'autres, les lois sont faibles car elles ne définissent pas les objectifs de la collecte, ne précisent pas les utilisations légitimes des données, ne contrôlent pas l'accès aux données, n'intègrent pas la gestion des risques ou ne prévoient pas de mécanismes de transparence et de responsabilisation. À leur tour, ces lois tendent à faciliter l'accès aux données sans garanties suffisantes. Les lois telles que la loi n° 18-07 de 2018 sur la protection des données personnelles en Algérie,<sup>27</sup> la loi sur la protection des données du Kenya de 2019,<sup>28</sup> la loi angolaise sur la protection des données de 2011, la loi sur la protection des données de la Côte d'Ivoire de 2013 et la loi ougandaise de 2019<sup>29</sup> sur la protection des données et de la vie privée prévoient des circonstances dans lesquelles les données personnelles, y compris les informations sensibles peuvent être traitées. Ces dispositions laissent une marge de manœuvre pour faciliter l'accès et le traitement des données à caractère personnel.

Les lois prescrivent les moyens par lesquels les données personnelles peuvent être traitées, en particulier dans l'intérêt de la sécurité nationale, de l'intérêt public, de l'application de la loi et de la conduite d'enquêtes pénales. Malheureusement, la portée et les limites dans lesquelles les données peuvent être traitées ne sont pas succinctes. Ils manquent également de contrôles clairs contre d'éventuelles violations de la confidentialité des données et ont tendance à tendre vers la facilitation de l'accès par l'État et ses agences plutôt que vers la protection des droits des personnes concernées. Il est également courant dans certains des pays étudiés de constater que les lois sont largement utilisées pour faciliter l'accès aux données personnelles des individus afin de les identifier et de les cibler. Les principales catégories de personnes visées comprennent les défenseurs des droits de l'homme, les militants politiques, les dissidents et les acteurs de l'opposition au gouvernement.

L'addendum de 2018 des Nations unies aux Principes directeurs du Conseil de sécurité de 2015 (Madrid) relatifs aux combattants terroristes étrangers<sup>30</sup> ne signifie pas que la technologie biométrique crée des défis en raison de l'écart qui existe entre l'innovation technologique et l'introduction d'une législation réglementant cette technologie. Par conséquent, les États sont invités à envisager de mettre en place des évaluations efficaces de la protection de la vie privée ou de créer des organes d'examen ou d'autres types d'organes de contrôle, afin d'anticiper et d'examiner l'impact potentiel de ces nouvelles technologies ou applications. En outre, les États sont tenus de veiller à ce que toute ingérence dans la vie privée soit conforme au droit international des droits de l'homme, qui interdit les ingérences arbitraires ou illégales dans la vie privée.

L'article 10, paragraphe 4, de la Convention de l'Union africaine sur les actions de cyber sécurité et la protection des données à caractère personnel (Convention de Malabo)<sup>31</sup> appelle les États à ne traiter des données à caractère personnel impliquant des données biométriques qu'après autorisation de l'autorité de protection compétente. Comme indiqué plus en détail dans le présent rapport, plusieurs pays se sont engagés dans la collecte et le traitement de données biométriques sans garanties juridiques, techniques ou réglementaires adéquates, telles que la création d'organismes indépendants de protection des données. En tout état de cause, seul un quart des pays africains (14) ont signé la convention et moins de 25% (13) l'ont ratifiée.<sup>32</sup>

Parmi les pays en étude, seuls le Mozambique, la Sierra Leone, le Togo, la Tunisie et la Zambie ont signé la Convention, tandis que seuls le Mozambique, le Sénégal, le Togo et la Zambie ont déposé les instruments de ratification. Les autres pays faisant partie de cette étude, à savoir l'Angola, le Cameroun, la République centrafricaine, la République démocratique du Congo, le Kenya, le Lesotho, le Libéria, le Nigeria, la Tanzanie et l'Ouganda, n'ont pas encore signé ou ratifié la convention. Le Sénégal et la Tunisie, qui ont pris des mesures en vue de l'adhésion à la Convention de Malabo, sont également membres de la Convention du Conseil de l'Europe pour la protection des personnes en ce qui concerne le traitement automatisé des données personnelles (Traité n° 108).<sup>33</sup>

<sup>27</sup> Article 18[modifier]

<sup>28</sup> Partie V (articles 44 à 47)

<sup>29</sup> Chapitre 9

<sup>30</sup> Principes directeurs du Conseil de sécurité relatifs aux combattants terroristes étrangers : Principes directeurs de Madrid de 2015 + Addendum de 2018 <https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/security-council-guiding-principles-sur-les-combattants-terroristes-étrangers.pdf>

<sup>31</sup> Convention de l'UA sur la cybercriminalité et la protection des données personnelles [https://au.int/sites/default/files/treaties/29560-treaty-0048\\_-\\_african\\_union\\_convention\\_on\\_cyber\\_security\\_and\\_personal\\_data\\_protection\\_e.pdf](https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf)

<sup>32</sup> Liste d'état [https://au.int/sites/default/files/treaties/29560-sl-AFRICAN\\_UNION\\_CONVENTION\\_ON\\_CYBER\\_SECURITY\\_AND\\_PERSONAL\\_DATA\\_PROTECTION.pdf](https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf)

<sup>33</sup> Tableau des signatures et ratifications du Traité 108 <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108>



## 2.2 Programmes de collecte de données biométriques

### 2.2.1 Registres d'état civil, y compris la délivrance de cartes d'identité nationales

Bien que peu répandue, plusieurs pays ont adopté l'utilisation de la biométrie telle que la reconnaissance des empreintes digitales, faciale ou de l'iris comme forme d'authentification aux fins de la délivrance de cartes de naissance et d'identité nationales.<sup>34</sup> La Stratégie de transformation numérique de l'Union Africaine pour l'Afrique (2020-2030) reconnaît l'importance de l'identité numérique dans la promotion de la confiance, qui est essentielle pour l'économie numérique du continent et la mise en place du marché unique numérique conformément à l'Accord de libre-échange continental africain (ZLECA). Elle propose d'assurer l'inclusion, la sécurité, la confidentialité et la propriété des données dans les systèmes d'identité numérique, et de soutenir l'interopérabilité et la neutralité des systèmes d'identité numérique dans le cadre de son programme de transformation.<sup>35</sup> Une identification numérique panafricaine pourrait refléter ou être informée par le portefeuille d'identité numérique proposé, actuellement en cours de développement par l'Union européenne.<sup>36</sup> L'UE a joué un rôle déterminant dans l'élaboration des efforts de transformation numérique de l'UA<sup>37</sup> et a soutenu le déploiement de programmes d'identification numérique dans plusieurs pays d'Afrique de l'Ouest.<sup>38</sup>

En 2016, la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO) a lancé la carte de la CEDEAO en tant que carte d'identité biométrique standard pour les citoyens de ses États membres. La carte peut également être utilisée comme document de voyage pour les résidents et remplace les titres de séjour utilisés dans ses 15 États membres.<sup>39</sup> La mise en œuvre de cette initiative nécessite la création de bases de données d'identités qui serviront de référence fiable pour d'autres services tels que la délivrance de passeports, de permis de conduire, de cartes d'électeur et de cartes de sécurité sociale.<sup>40</sup>

Au-delà de la CEDEAO, divers pays ont également commencé à collecter des données biométriques, notamment pour les cartes d'identité nationales, l'inscription des électeurs et à d'autres fins. En Angola, le gouvernement délivre depuis 2009 des cartes d'identité numériques valides de 10 ans à ses citoyens. Ce système d'identification a été conçu pour protéger les données personnelles tout en stockant des quantités substantielles d'informations biométriques directement sur la carte, y compris deux empreintes digitales du pouce et des images d'iris, un certificat de naissance et des données démographiques.<sup>41</sup>

Au Cameroun, il y a eu de multiples programmes identitaires, mais aucun n'a été durable ou robuste. En 1994, le gouvernement a travaillé avec une entité privée pour enregistrer les individus et délivrer des cartes d'identité nationales (NID) et des permis de séjour. En 2005, le traitement des données biométriques a commencé. En 2008, la carte d'identité nationale a été mise à niveau pour inclure une photo couleur et une empreinte digitale électronique du titulaire de la carte, ainsi que des dispositifs de sécurité supplémentaires, et en 2013, le gouvernement a commencé à émettre des cartes d'identité nationales électroniques. Ces identifiants électroniques étaient destinés à être utilisés pour de multiples services électroniques tels que l'identification civile et les services sociaux et de santé.<sup>42</sup> En République centrafricaine, des discussions ont eu lieu en 2020 entre le gouvernement et Securiport, une entreprise privée, pour lancer l'identification biométrique et la délivrance d'identifiants électifs à tous les citoyens et réfugiés.<sup>43</sup>

<sup>34</sup> Les pays africains adoptent la biométrie et les identités numériques

<https://www.un.org/africarenewal/magazine/february-2021/african-countries-embRacing-Biometrics-Digital-IDS>

<sup>35</sup> Stratégie de transformation numérique de l'Union africaine pour l'Afrique (2020 - 2030) <https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf>

<sup>36</sup> Identité numérique européenne [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity\\_en](https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en)

<sup>37</sup> Afrique <https://digital-strategy.ec.europa.eu/en/policies/afrika>; Vers un partenariat numérique UE-Afrique

<https://ec.europa.eu/futurium/en/eu-au-digital-economy-task-force/towards-eu-africa-digital-partnership-0.html>

<sup>38</sup> Digital4Development: intégrer les technologies et services numériques dans la politique de développement de l'UE

[https://ec.europa.eu/transparency/documents-register/detail?ref=SWD\(2017\)157&lang=fr](https://ec.europa.eu/transparency/documents-register/detail?ref=SWD(2017)157&lang=fr)

<sup>39</sup> La carte CEDEAO : transformer un défi en opportunité [https://peopleid.zetes.com/sites/default/files/br\\_cedeao\\_20161110\\_uk\\_4.pdf](https://peopleid.zetes.com/sites/default/files/br_cedeao_20161110_uk_4.pdf)

<sup>40</sup> Lier le projet au registre de l'état civil <https://peopleid.zetes.com/en/link-project-civil-register>

<sup>41</sup> L'état des systèmes d'identification en Afrique : fiches pays (anglais). Laverington, D.C. : Banque mondiale Groupe. <https://bit.ly/3SzOqdE>

<sup>42</sup> Ibid Cross ref 37

<sup>43</sup> Biométrie et identification numérique en Afrique : GenKey au Niger, Securiport en RCA, nouveau partenaire revendeur pour Daon en Afrique du Sud <https://bit.ly/3dNRPqo>; La Conférence propose des documents biométriques pour les réfugiés centrafricains, <https://bit.ly/3CejJdx>

En 2019, le Kenya a lancé le Système national intégré de gestion de l'identité (NIIMS), également connu sous le nom de Huduma Namba (traduction en swahili pour « numéro matricule »).<sup>44</sup> Dans le cadre de l'enregistrement de l'identification numérique Huduma Namba en 2019, le public était tenu de présenter tous ses documents personnels tels que les cartes d'identité nationales, les certificats de naissance, les avis de naissance, les cartes de la Caisse nationale d'assurance maladie (NHIF), les cartes du Fonds national de sécurité sociale (NSSF), les certificats de numéro d'identification personnel (PIN) de l'Autorité fiscale du Kenya, le permis de conduire, les cartes d'identité des étrangers, les cartes d'identité des réfugiés, les passeports, les cartes d'invalidité et les cartes du système d'information de gestion de l'éducation nationale (NEMIS).<sup>45</sup>

Le système basé sur la technologie biométrique était un projet mystérieux, de grande envergure et de collecte de données obligatoire qui visait à créer une « source unique de vérité » de toutes les informations sur les citoyens et les ressortissants étrangers dans le pays. Il a également cherché à consolider les informations provenant d'autres bases de données telles que les cartes d'identité nationales, les passeports, les permis de conduire, la sécurité sociale et l'assurance maladie nationale. Malgré sa mise en œuvre en l'absence d'un cadre juridique complet, le projet à KES 9,6 milliards (79,7 millions USD) a été interrompu par les tribunaux<sup>46</sup> après avoir collecté les données personnelles de 37 millions de personnes dans sa première phase et traité cinq millions de cartes en juin 2021.<sup>47</sup>

Les cartes d'identité numériques biométriques nationales du Lesotho ont été introduites<sup>48</sup> en 2013 et ont couvert 85 % de la population éligible.<sup>49</sup> L'obtention de la carte d'identité nationale est intégrée aux processus d'enregistrement des naissances et des décès. L'acte de naissance est requis dans le processus de la demande de carte d'identité nationale (NID). Une photo et les empreintes digitales des 10 doigts sont prélevées électroniquement. Une fois qu'une vérification de déduplication en ligne a confirmé que la personne n'a pas déjà été inscrite, un code à barres 2D est imprimé. Il contient une empreinte digitale lisible par machine et des informations biographiques ainsi qu'une photo et d'autres informations sur le recto de la carte.

Au Libéria, le Registre national d'identification (RNI) a été créé par la loi en 2011 et autorisé à mettre en œuvre le Système national d'identification biométrique (NBIS).<sup>50</sup> Cependant, le gouvernement n'a mis en place une équipe de gestion et a alloué un financement provisoire pour le RNI qu'en octobre 2015. Le RNI espère établir ou acquérir l'infrastructure technique et les procédures de contrôle qui serviront de plate-forme pour la mise en œuvre du NBIS. Ce système, dont le projet pilote a débuté en novembre 2021,<sup>51</sup> devrait collecter, organiser, stocker, sécuriser et donner accès aux données biométriques sécurisées collectées auprès des personnes demandant des cartes biométriques nationales et d'autres documents clés, tels que les passeports, les permis de conduire et les cartes de sécurité sociale. Le Libéria dispose de plusieurs systèmes d'identité fonctionnels, notamment des numéros de passeport, des numéros d'enregistrement des fonctionnaires, des numéros de sécurité sociale, des numéros de permis de conduire, des numéros d'enregistrement des naissances et des listes électorales. Certains de ces systèmes saisissent des informations biométriques.<sup>52</sup>

<sup>44</sup> Afrique : réglementer les technologies de surveillance et les données personnelles  
<https://www.nature.com/articles/d41586-022-01949-9>

<sup>45</sup> Huduma Namba Formulaire de capture numérique <https://www.hudumanamba.go.ke/wp-content/uploads/2019/03/form-hn-23-Data-Capture-Tools-14-3-2019.pdf>; Huduma Namba Règlement 2021, <https://ict.go.ke/wp-content/uploads/2020/10/HUDUMA-NAMBA-REGULATIONS-2020.2021.pdf>

<sup>46</sup> Pourquoi l' Huduma Namba Statuer sur les questions pour l'avenir de l'identité numérique, et non Just au Kenya  
<https://privacyinternational.org/news-analysis/3350/why-huduma-namba-ruling-matters-future-digital-id-and-not-just-kenya>

<sup>47</sup> Les banques d'État sur un nouveau portail pour faciliter la collecte des Huduma cartes  
<https://nation.africa/kenya/news/state-banks-portal-to-ease-collection-of-huduma-cards-3439902>

<sup>48</sup> État de l'identité numérique au Lesotho [https://researchictafrica.net/wp/wp-content/uploads/2021/11/Lesotho\\_31.10.21.pdf](https://researchictafrica.net/wp/wp-content/uploads/2021/11/Lesotho_31.10.21.pdf)

<sup>49</sup> Diagnostic de l'économie numérique du Lesotho  
<https://openknowledge.worldbank.org/bitstream/handle/10986/33881/Lesotho-Digital-Economy-Diagnostic.pdf?sequence=1&isAllowed=y>

<sup>50</sup> Identification pour le développement (ID4D) analyse des systèmes d'identification Évaluation du Libéria  
<https://openknowledge.worldbank.org/bitstream/handle/10986/26438/113549-WP-P156810-PUBLIC-Liberia-ID4D-Web.pdf?sequence=1&isAllowed=y>

<sup>51</sup> Libéria: Registre d'identification nationale pour délivrer des cartes d'identité nationales aux Libériens le long de la frontière avec la Sierra Leone  
<https://citizenshiprightsafrika.org/liberia-national-identification-registry-to-issue-national-id-cards-to-liberians-along-sierra-leone-border/>

<sup>52</sup> Ibid. croix réf 37

Le Mozambique met en œuvre<sup>53</sup> une carte d'identité numérique avec un numéro unique d'identification du citoyen (NUIC), le Service national de l'immigration (SENAMI), pour son système d'immigration pour les documents de voyage et les permis de séjour ; et le système électronique d'enregistrement des faits d'état civil et de statistiques de l'état civil (e-SIRCEV) mis en place en 2018.<sup>54</sup> Le Mozambique dispose d'un numéro d'identification national unique, attribué lors de l'enregistrement des naissances. Ce numéro d'identification national est utilisé sur les cartes d'identité nationales (NID), les cartes de santé, les permis de conduire et les passeports. Les certificats de naissance sont une condition préalable à l'obtention des cartes d'identité nationales. La carte a une validité de cinq ans pour les personnes âgées de moins de 40 ans et de 10 ans pour les personnes âgées de 40 à 50 ans. La carte est valable à vie si le titulaire de la carte a plus de 50 ans. La carte est obligatoire et est réglementée par le décret n° 11/2008 du Conseil des ministres. Celle de Mozambique est une carte plastifiée avec une bande magnétique qui contient un numéro d'identification, une photographie, le nom complet, le sexe, la date de naissance, la nationalité, l'adresse, les données biométriques (empreintes digitales), le lieu et la date d'émission, la taille, la profession, l'état matrimonial, la date d'expiration et la signature de l'utilisateur. Le Mozambique ne dispose pas d'une législation autonome sur la protection des données personnelles.<sup>55</sup>

Au Nigéria, le numéro d'identité national (NIN) est un numéro unique aléatoire à 11 chiffres attribué à vie à une personne après inscription réussie dans la base de données des cartes d'identité (NID). La carte NID est une carte d'identité polyvalente générale à puce à microprocesseur, avec 13 applications, y compris la vérification d'identité, l'authentification et la technologie de paiement pour aider à promouvoir l'inclusion financière. La carte d'identité contient deux photographies du détenteur et une puce stockant les informations biométriques d'un individu (10 empreintes digitales et une scanographie de l'iris). La déduplication biométrique est effectuée avant la délivrance du NIN. Après une déduplication réussie, un NIN unique est émis et stocké dans la base de données NID. Les enfants âgés de moins de 16 ans sont tenus d'enregistrer leurs informations biométriques auprès du NIMC et de les mettre à jour tous les deux ans. Cependant, les données biométriques de l'enfant ne sont pas utilisées pour la déduplication. L'enfant reçoit un NIN lié à celui du parent.<sup>56</sup> Le programme national d'identification biométrique pourrait finalement coûter 2,3 milliards de dollars,<sup>57</sup> dans un pays où, en mars 2020, seuls 9 % des ressortissants disposaient d'un numéro national d'identification (NIN) et moins de 1 % d'une carte d'identité nationale.<sup>58</sup>

En 2005, le gouvernement sénégalais a annoncé le projet de cartes d'identité nationales numériques pour tous les citoyens. La même année, 174 centres d'enregistrement ont été créés à travers le pays. A ce jour, au moins 67% de la population possède une carte d'identité nationale ou une carte d'électeur qui sont utilisées à des fins civiles, de sécurité sociale et de vote. La carte d'identité sénégalaise a un code-barres avec des informations biométriques ainsi que des informations biographiques. L'identification électronique est utilisée pour plusieurs services électroniques.<sup>59</sup> En 2019, le gouvernement s'est engagé dans le processus de numérisation de son état civil et de son fichier national d'identité biométrique. Le projet a été soutenu par l'Union européenne dans le cadre du Programme d'appui au renforcement du système d'information de l'état civil et de la consolidation d'un fichier national d'identité biométrique au Sénégal<sup>60</sup>.

<sup>53</sup> Identification numérique au Mozambique [https://researchictafrica.net/wp-content/uploads/2021/11/Mozambique\\_3.11.21.pdf](https://researchictafrica.net/wp-content/uploads/2021/11/Mozambique_3.11.21.pdf)

<sup>54</sup> Ibid croix réf 50

<sup>55</sup> Ibid croix réf 37

<sup>56</sup> Ibid croix réf 37

<sup>57</sup> Biométrie et l'identité numérique à travers l'Afrique cette semaine : économies et coûts au Nigeria, divisions en Tanzanie, Ghana <https://www.biometricupdate.com/202003/biometrics-and-digital-id-across-africa-this-week-savings-and-costs-in-nigeria-divisions-in-tanzania-and-ghana>

<sup>58</sup> Biométrie et identification numérique en Afrique cette semaine : économies et coûts au Nigeria, division en Tanzanie, Ghana <https://www.biometricupdate.com/202003/biometrics-and-digital-id-a-travers-l'Afrique-cette-semaine-économies-et-coûts-dans-Nigeria-divisions-en-Tanzanie-et-Ghana>

<sup>59</sup> La Banque mondiale (2017) L'état des systèmes d'identification en Afrique, <https://tinyurl.com/wfwhjfd>

<sup>60</sup> Informatisation de l'état civil et du fichier national d'identité biométrique : Oumar Guèye En mode « fast track » : <https://bit.ly/3w1yZSQ>; État civil : l'absence de statistiques sur les naissances constatée <https://senegalservices.sn/actualite/etat-civil-le-deficit-de-statistiques-sUr-les-Naissances-Releve>

En Sierra Leone, l'article 37 de la loi nationale de 2016 sur l'enregistrement des faits d'état civil autorise l'Autorité nationale d'enregistrement des faits d'état civil (NCRA) à procéder à l'enregistrement obligatoire et continu des citoyens et des non-citoyens et à collecter des statistiques de l'état civil, à établir et à maintenir un système d'enregistrement électronique. Le système est conçu par la loi pour collecter et conserver les données biométriques des citoyens ainsi que pour générer une identification nationale sur le numéro (NIN). Les détails biométriques des individus peuvent inclure le visage, les empreintes digitales, le groupe sanguin, la couleur des yeux et la taille. Cependant, bien que la loi autorise la NCRA à collecter des données biométriques au cours du processus d'enregistrement, aucune collecte de ce type n'a lieu ou n'a jamais eu lieu en raison d'un manque de capacité institutionnelle pour déployer une telle entreprise. Depuis 2016, la NCRA recueille les données biométriques des Sierra-Léonais afin d'établir un registre civil permanent pour le pays. Le dernier exercice à grande échelle a eu lieu entre mai et juillet 2021. À partir de juin 2022, tous les ressortissants étrangers demandant un permis de séjour et de travail auprès du gouvernement doivent avoir un numéro d'identification national (NIN).<sup>61</sup>

En Tanzanie, le gouvernement a introduit un programme d'identification nationale biométrique en 2013 et a commencé à émettre des cartes en 2016.<sup>62</sup> En 2020, au moins 22,1 millions de personnes, soit 80% de la population adulte, s'étaient inscrites pour obtenir le numéro d'identification national (NIN).<sup>63</sup> En outre, l'enregistrement obligatoire de la carte SIM nécessite la collecte de données d'empreinte en plus des documents officiels tels que les cartes d'identité nationales, les certificats de naissance, les permis de conduire ou les passeports.<sup>64</sup>

Au Togo, bien que l'état civil (enregistrement des naissances, des décès et des mariages) ne soit pas encore numérisé, des rapports récents indiquent que la numérisation se fera parallèlement à la nouvelle carte d'identité nationale biométrique qui est toujours en cours.<sup>65</sup> Le pays a annoncé son programme d'identification biométrique e-ID en 2018, et des plans sont en cours pour déployer le projet visant à fournir des cartes d'identité à l'ensemble de la population, car seulement 25% de la population possède une carte d'identité.<sup>66</sup> Dans le cadre de ce programme, tous les résidents seront enregistrés et recevront un numéro d'identification unique à 10 chiffres, qui devrait servir de base à la prestation de services publics, sociaux et privés. L'e-ID sera développé par l'IIIT-Bangalore à l'aide de MOSIP (Modular Open-Source Identification Platform).<sup>67</sup>

Le pays a modifié sa loi n° 2020-009 du 10 septembre 2020<sup>68</sup> relative à l'identification biométrique des personnes afin, entre autres, d'habiliter l'Agence Nationale d'Identification (ANID) à collecter les données démographiques et biométriques des citoyens togolais en prélude à la mise en place de la base de données de base du projet de carte d'identité numérique du pays.<sup>69</sup> Une campagne de sensibilisation a été entreprise avant le lancement du projet.<sup>70</sup>

En Ouganda, le gouvernement a lancé en 2014 l'enregistrement de masse des cartes d'identité nationales biométriques qui sont délivrées et conservées par l'Autorité nationale d'identification et d'enregistrement (NIRA).<sup>71</sup> Le système a été fourni par Mühlbauer ID Services GmbH, une société allemande, pour un montant de 64 millions d'euros (63,1 millions de dollars). Outre le registre d'identification, l'Autorité est également responsable de l'enregistrement des naissances, des décès, des adoptions et des étrangers. Lors de l'inscription, les empreintes digitales et les photos des demandeurs sont saisies numériquement.

<sup>61</sup> Identification numérique nécessaire pour le passeport, la résidence, les permis de travail en Sierra Leone <https://www.biometricupdate.com/202205/digital-id-needed-for-passport-residence-work-permits-in-sierra-leone>

<sup>62</sup> Rapport sur la communauté de pratique sur le kit Digital Enquirer <https://www.africaportal.org/features/tanzania-nida-ids-civic-servICS-ou-pas/>

<sup>63</sup> Le Togo signe un protocole d'accord pour établir un système d'identité numérique MOSIP <https://www.biometricupdate.com/202011/ppps-and-social-media-influencers-for-biometrics-registration-and-national-id>

<sup>64</sup> La date limite pour l'enregistrement de la carte SIM biométrique en Tanzanie approche <https://advoc.globalvoices.org/2020/01/08/deadline-métiers à tisser-pour-l'enregistrement-de-carte-SIM-biométrique-en-Tanzanie/>

<sup>65</sup> Le Togo espère lancer une nouvelle identité biométrique en 2021 <https://citizenshiprightsafrika.org/togo-hopes-to-launch-new-biometric-id-card-in-2021/>; Togo <https://data.unicef.org/crvs/togo/>

<sup>66</sup> Faure Gnassingbé annonce un big bang à l'état civil <https://www.togofirst.com/fr/gouvernance-economique/1202-4924-faure-gnassingbe-annonce-un-big-bang-dans-letat-civil>

<sup>67</sup> Le Togo signe un protocole d'accord pour établir un système d'identité numérique MOSIP <https://www.biometricupdate.com/202112/togo-signs-mou-to-establish-mosip-digital-identity-system>

<sup>68</sup> Une nouvelle étape pourrait bientôt être franchie dans le projet d'identification biométrique du Togo <https://www.togofirst.com/en/economic-governance/1603-9611-a-new-milestone-could-soon-be-reached-in-togo-s-biometric-id-project>

<sup>69</sup> Le Togo modifie la loi sur l'identification biométrique pour faire progresser les ambitions en matière d'identification numérique <https://www.biometricupdate.com/202206/togo-amends-law-on-biometric-identification-to-advance-digital-id-ambitions>

<sup>70</sup> Le Togo se prépare au lancement de l'identification biométrique avec une campagne de sensibilisation <https://www.biometricupdate.com/202106/togo-readies-for-biometric-id-launch-with-awareness-raising-campaign>

<sup>71</sup> Autorité nationale d'identification et d'enregistrement <https://www.nira.go.ug/>

En août 2022, l'Ouganda a annoncé son intention de mettre à niveau sa carte d'identité nationale actuelle, qui a été déployée pour la première fois en 2014 pour inclure l'ADN, les empreintes digitales, l'empreinte palmaire et les informations de scanographie oculaire à partir de 2024, afin d'éliminer la criminalité.<sup>72</sup> Jusqu'à présent, la carte a été délivrée à 26 millions de personnes et son utilisation obligatoire est limitée à l'accès à une grande variété de services, bien que les personnes qui n'en ont pas soient exclues de certains services.<sup>73</sup>

En 2013, le gouvernement zambien a introduit les cartes nationales d'enregistrement (NRC), une carte d'identité nationale (NID) de faible technologie qui capture certaines informations biographiques minimales et biométriques (empreinte du pouce droit). Le système intégré d'information sur la réglementation nationale (INRIS), d'un montant de 54,8 millions de dollars, a remplacé le système papier introduit en 1965 et délivrerait des documents biométriques tels que les cartes nationales d'enregistrement, les certificats de naissance et de décès et faciliterait l'inscription des électeurs.<sup>74</sup>

Une copie de la demande est envoyée au bureau central et la demande originale est conservée au bureau de district. Le pays est en train de numériser ces données du NRC pour migrer vers un système d'identification électronique plus avancé avec authentification biométrique. Plus d'un million de points de données d'identification ont déjà été numérisés.<sup>75</sup> Le système devrait être la seule source de vérification du statut des personnes vivant en Zambie telles que les citoyens, les résidents ou les immigrants, et faciliter l'accès aux transactions et l'inscription des électeurs.<sup>76</sup> Les informations recueillies lors de l'inscription comprennent des données biométriques telles que des photographies pour la reconnaissance faciale, des empreintes digitales et des images d'iris pour les personnes dont les empreintes digitales ne sont pas lisibles ou inscrites.<sup>77</sup>

## 2.2.2 Programmes d'enregistrement et d'identification biométriques des électeurs

Au cours des dernières années, plusieurs pays africains ont adopté l'utilisation de systèmes d'enregistrement biométrique et de vérification biométrique des électeurs (BVVS) dans le but d'assurer l'égalité des électeurs et de préserver l'intégrité du processus électoral. Néanmoins, bien que la biométrie ait suscité des attentes en matière d'intégrité électorale, elle n'empêche pas automatiquement le truquage.<sup>78</sup> Le BVVS peut encore être manipulé puisqu'il n'aide qu'à vérifier les électeurs et laisse la gestion de l'ensemble du processus électoral aux organes de gestion électorale.

En Angola, la presse locale a rapporté en 2021 que la Commission électorale nationale angolaise (CNE) avait mis en place un système électronique d'enregistrement et d'identification des personnes impliquées dans le processus électoral afin de garantir que l'ensemble du processus se déroulait de manière standardisée et crédible. Ce système comprenait la délivrance et la distribution de cartes d'identité pour les différents acteurs impliqués, tels que les délégués, les observateurs internationaux, les journalistes et la politique électorale, afin de permettre un meilleur contrôle et une meilleure organisation de l'ensemble du processus. L'inscription a été mise en œuvre à l'échelle nationale dans plus de 10 provinces pour plus de 14 millions d'électeurs.<sup>79</sup>

<sup>72</sup> L'armée ougandaise exige l'ADN d'un citoyen pour le déploiement de l'identité numérique

<https://www.visiontimes.com/2022/08/12/uganda-dna-biometric-id-social-credit.html>; Museveni veut la palme des Ougandais prints, détails ADN capturés « pour éliminer le crime »

<https://www.africanews.com/2018/02/28/museveni-wants-ugandans-palm-prints-dna-details-captured-to-eliminate-crime/>

<sup>73</sup> L'armée ougandaise exige l'ADN d'un citoyen pour le déploiement de l'identité numérique

<https://www.visiontimes.com/2022/08/12/uganda-dna-biometric-id-social-credit.html>

<sup>74</sup> L'enregistrement biométrique pour le nouveau système national d'identification de la Zambie est en cours

<https://www.biometricupdate.com/202203/biometrics-registration-for-zambias-new-national-id-system-underway>

<sup>75</sup> Ibid croix réf 37

<sup>76</sup> Identification biométrique des citoyens pour améliorer l'inscription et l'identification des électeurs en Zambie

<https://www.biometricupdate.com/202004/biometric-citizen-identification-to-enhance-voter-registration-and-identification-in-zambia>

<sup>77</sup> Identification biométrique des citoyens pour améliorer l'inscription et l'identification des électeurs en Zambie

<https://www.biometricupdate.com/202004/biometric-citizen-identification-to-enhance-voter-registration-and-identification-in-zambia>

<sup>78</sup> Les échecs productifs du vote biométrique en Afrique <https://democracyinfrance.org/the-productive-failures-of-biometric-voting-in-africa/>

<sup>79</sup> L'Angola met en œuvre une technologie des systèmes d'inscription et d'identification des personnes impliquées dans les élections processSource:

<https://peopleid.zetes.com/pt/reference/angola-implementa-plataforma-tecnologica-para-o-registo-e-identificacao-dos-intervenientes>



Au Cameroun, le Code électoral a institué la carte d'électeur biométrique permanente<sup>80</sup> pour assurer la transparence et la crédibilité des prochaines élections présidentielles. Le traitement des données biométriques d'inscription des électeurs qui a commencé en avril 2013 est devenu un processus continu entrepris pour mettre à jour régulièrement le registre des électeurs. La production des cartes d'électeurs et des listes électorales des bureaux de vote a été lancée après la phase de traitement des données. Ces dernières étapes du processus d'inscription biométrique, qui ont été entreprises entre juillet et août 2013, ont précédé l'affectation des électeurs aux bureaux de vote. La carte d'électeur personnelle biométrique porte les noms, date et lieu de naissance, filiation, photo, empreintes digitales, profession et adresse du titulaire.<sup>81</sup>

Le système biométrique mis en place pour la gestion des élections au Cameroun comprenait 10 centres biométriques régionaux situés dans les délégations régionales de l'organe de gestion des élections (ELECAM) et un centre national de biométrie électorale situé au siège de l'organe à Yaoundé. Chacune des 360 municipalités du pays disposait de deux kits d'inscription pour s'assurer que l'inscription était accessible à tous les électeurs, quel que soit leur lieu de résidence.

En République centrafricaine, pour être inscrit sur les listes électorales, il est nécessaire de présenter des documents tels que la carte nationale d'identité, le passeport, l'acte de naissance, un jugement supplétif (principalement pour ceux qui ont perdu leur acte de naissance), le livret militaire ou le livret de pension, la carte de réfugié ou tout autre document dûment délivré en lieu et place de document d'identification à l'agent d'inscription .

En RDC, il a été signalé qu'en 2016, Gemalto, le leader mondial de la sécurité numérique, avait remporté un appel d'offres international pour fournir à la Commission électorale nationale indépendante (CENI) du pays 22 000 kits mobiles d'inscription biométrique des électeurs pour soutenir une mise à jour complète du registre national des électeurs.<sup>82</sup> Il était prévu que les stations d'inscription mobiles Coesys entièrement portables de Gemalto permettaient à 18 000 centres d'inscription d'acquérir rapidement des photographies numériques, des empreintes digitales et des enregistrements de signatures de citoyens, et de délivrer instantanément des cartes d'électeur personnalisées pour les élections générales de 2019.<sup>83</sup>

Avant les développements de 2016, la Commission électorale indépendante (CEI), comme on l'appelait alors, avait opté pour l'inscription biométrique pour la constitution du premier fichier électoral en l'absence de fichier d'état civil. L'introduction de la biométrie visait à disposer d'un fichier électoral fiable garantissant l'identification unique de chaque électeur et établissant la confiance avec tous les partenaires du processus électoral.

Le Système intégré de gestion des élections au Kenya (KIEMS) comprend un registre électronique, l'inscription biométrique des électeurs (BVR), des dispositifs électroniques d'identification des électeurs (EVID) et un système de transmission des résultats (RTS). L'organisme électoral, la Commission indépendante de délimitation des circonscriptions électorales (IEBC), a piloté l'inscription électronique des électeurs en 2009 dans 18 circonscriptions.<sup>84</sup> Cela a ensuite été étendu à l'ensemble des 290 circonscriptions lors de l'élection générale de 2013. La méthode d'inscription biométrique des électeurs (BVR) permet de saisir l'image faciale, les empreintes digitales et les renseignements biographiques de l'électeur, comme son nom, son sexe, son numéro de carte d'identité ou de passeport et son numéro de téléphone. Lors de l'inscription des électeurs pour l'élection de 2013, l'IEBC a déployé 15 000 trousseaux BVR fournies par OT Morpho Canada Inc. dans 24 614 centres d'inscription et a recueilli les détails de 14,4 millions d'électeurs.<sup>85</sup>

<sup>80</sup> Voir l'article 84 de la Loi n° 2012/001 du 19 avril 2012 portant Code électoral, <https://bit.ly/3ikeDOF>

<sup>81</sup> [https://recef.org/wp-content/uploads/Rapport\\_Biometrie.pdf](https://recef.org/wp-content/uploads/Rapport_Biometrie.pdf)

<sup>82</sup> La République démocratique du Congo choisit l'enrôlement biométrique mobile de Gemalto pour soutenir des élections équitables <https://bit.ly/3xU6vve>

<sup>83</sup> Ibid.

<sup>84</sup> Inscription biométrique des électeurs [https://www.iebc.or.ke/election/technology/?Biometric\\_Voter\\_Registration\\_System\\_\(BVR\)](https://www.iebc.or.ke/election/technology/?Biometric_Voter_Registration_System_(BVR))

<sup>85</sup> L'enregistrement biométrique des électeurs au Kenya : nouvelle solution, nouveaux problèmes <https://issafrica.org/iss-today/kenyas-biometric-voter-registration-new-solution-new-problems>

En 2017, IEBC a investi 36,4 millions USD pour moderniser le KIEMS avec l'achat de 45 000 tablettes tout-en-un d'un coût de 786 USD chacune auprès d'Idemia, une société française.<sup>86</sup> Au total, 19,6 millions d'électeurs ont été inscrits pour l'élection de 2017 et 14 523 candidats ont participé à l'élection, ce qui a coûté au pays 338,4 millions de dollars.<sup>87</sup> Cependant, il y a eu des échecs massifs et des irrégularités au cours de l'élection, ce qui a conduit à l'annulation du résultat de l'élection présidentielle. Pour les élections de 2022, le nombre d'électeurs inscrits a augmenté de 12,8 % pour atteindre 22,1 millions d'électeurs.<sup>88</sup> L'IEBC a déployé 55 100 kits KIEMS, dont certains ont été fournis par Smartmatic International Holding B. V. dans 46 229 bureaux de vote auxquels 14,3 millions de Kenyans ont participé.<sup>89</sup> L'organe électoral a été confronté à des problèmes liés à l'intégrité du registre électronique, y compris la duplication des électeurs, le contrôle d'accès et le recoupement entre le BVR et celui du Bureau national d'enregistrement pour retirer les personnes décédées et inscrire de nouveaux électeurs, problèmes qui ont été mis en évidence dans un audit mené par KPMG avant l'élection.<sup>90</sup>

Au Lesotho, l'enregistrement biométrique des électeurs a été introduit pour la première fois lors des élections de 2002, après que la Commission électorale indépendante (CEI) ait attribué à une société informatique appelée Arivia.Kom un contrat de 15,5 millions de lotis du Lesotho (940 000,00 USD) pour la fourniture d'une solution informatique mise en paquet pour les élections, y compris la mise en place des sites, la fourniture de logiciels et l'inscription des électeurs qui constituaient la capture de données biologiques, les empreintes digitales, les photographies et les signatures dans la base de données. Le système produit ensuite une carte d'électeur que le propriétaire utilisera pendant le processus de vote.<sup>91</sup>

L'adoption du nouveau système a été positive et la CEI a indiqué que 830 000 électeurs étaient inscrits au cours de la période initiale, alors que l'objectif était de 900 000 personnes. Pour toutes les autres élections suivantes, à moins que ce ne soit la première fois qu'une personne s'inscrit comme électeur, il n'y a pas eu de demande de réinscription. Ce n'est que pour les prochaines élections de 2022 qui doivent avoir lieu le 7 octobre 2022 que le processus d'inscription a changé. Pour ces élections, seule la carte d'identité nationale ou le passeport électronique portant le numéro d'identification est nécessaire l'enregistrement, et chaque futur électeur doit mettre à jour les informations d'inscription de ses électeurs avec ses informations d'identification.

Au Libéria, la Commission électorale nationale (NEC) du pays a annoncé son intention de passer de la reconnaissance optique des marques pour la sécurité des électeurs à la biométrie des empreintes digitales alors qu'elle se prépare pour les élections générales de 2023.<sup>92</sup> Selon la présidente du NEC, Davidetta Browne Lansanah, des tablettes portables avec des scanners d'empreintes digitales seront utilisées pour capturer les empreintes du pouce pour un registre électoral biométrique. L'exercice de transition devrait commencer le 15 décembre 2022 et se terminer le 17 mars 2023.<sup>93</sup>

Au Nigeria, le gouvernement a adopté en 2011 le programme de collecte de données biométriques pour l'inscription de ses électeurs pour une carte d'électeur permanente (PVC) en tant que système automatisé d'identification de l'empreinte digitale. À l'époque, le registre généré était considéré comme le meilleur jamais produit par la CENI et a été utilisé pour les élections générales de 2011 et 2015.<sup>94</sup> En préparation des prochaines élections générales de 2023, la Commission électorale nationale indépendante (CENI) a lancé un portail où les citoyens éligibles peuvent s'inscrire pour leur nouveau PVC et les électeurs inscrits peuvent vérifier leurs coordonnées. Après l'inscription en ligne sur le portail, les électeurs admissibles doivent encore prendre rendez-vous pour que leurs données biométriques, qui comprennent les images faciales et les empreintes digitales, soient saisies au bureau de l'INEC ou dans les centres désignés.

<sup>86</sup> Dans les failles du biomètre électoral du Kenya.ics

[https://www.lemonde.fr/en/le-monde-africa/article/2022/05/27/inside-the-flaws-of-kenya-s-electoral-biometrics\\_5984834\\_124.html](https://www.lemonde.fr/en/le-monde-africa/article/2022/05/27/inside-the-flaws-of-kenya-s-electoral-biometrics_5984834_124.html)

<sup>87</sup> Citizen TV, président de l'IEBC Chebukati Selon les besoins de la Commission, la Commission Ksh 40,9 B pour les élections » (Citizen TV, août 2021),

<https://www.youtube.com/watch?v=j0ldLOBZ60A>

<sup>88</sup> Elections 2022 pour présenter le plus grand nombre d'électeurs inscrits et de bureaux de vote dans l'histoire du Kenya

<https://www.standardmedia.co.ke/national/article/2001448421/election-2022-to-feature-highest-number-of-registered-voters-polling-stations-in-kenyas-history>

<sup>89</sup> Déclaration des résultats de l'élection du président de la République du Kenya au Centre national de décompte <https://www.iebc.or.ke/uploads/resources/QLTILx0Vr.pdf>

<sup>90</sup> Rapport préliminaire de la mission d'observation en Technologie KICTANet <https://www.kictanet.or.ke/?mdocs-file=46145>

<sup>91</sup> ITWeb, <https://www.itweb.co.za/content/nWJadvb8Ze5MbJO1>.

<sup>92</sup> Le Libéria prévoit un registre biométrique des électeurs avec inscription à compter de décembre

<https://www.biometricupdate.com/202209/liberia-plans-biometric-voter-registry-with-enrollment-beginning-in-december>

<sup>93</sup> Ibid. cRoss réf. 87

<sup>94</sup> Introduire la technologie biométrique dans les Élections <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>

Cependant, l'absence d'harmonisation de la collecte de données crée beaucoup de gaspillage. Par exemple, en 2015, 120 milliards NGN (627 millions USD) auraient été dépensés pour les élections, dont environ 200 millions USD pour l'enregistrement biométrique des électeurs et la délivrance de cartes. Comme le gouvernement fédéral cherche à harmoniser les données biométriques collectées par les différentes agences du pays avant 2023, la base de données de l'INEC n'est pas liée au numéro d'identification national (NIN).

Au Sénégal, par décret n° 2016-1536 du 29 septembre 2016, portant application de la loi n° 2016-09 du 14 mars 2016 instituant une carte d'identité biométrique de la CEDEAO, le gouvernement a institué la carte d'électeur biométrique. Ce décret a abrogé les dispositions de la loi de septembre 2005 instituant la carte nationale d'identité sénégalaise numérisée et confère à la carte d'identité biométrique de la CEDEAO une valeur de carte nationale d'identité et de carte électorale – la carte d'identité de la CEDEAO contient une puce électronique multi-applications et peut être utilisée à d'autres fins.

La carte d'électeur biométrique ainsi incluse dans la carte d'identité biométrique de la CEDEAO a un numéro unique à 17 chiffres codé selon le sexe, la région et la date de naissance. Pour les électeurs (personnes déjà inscrites sur les listes électorales), il précise le numéro de l'électeur, la région, le département, la circonscription, la commune, le bureau de vote et le numéro d'identification national (NIN). Les citoyens sénégalais âgés de cinq à 15 ans peuvent demander une carte d'identité de la CEDEAO et ceux âgés de 15 ans et plus doivent obtenir une carte d'identité de la CEDEAO. Sa validité est de 10 ans.<sup>95</sup>

En Sierra Leone, le gouvernement a lancé son premier enregistrement biométrique des électeurs et a réussi à saisir les données biométriques de 2,7 millions d'électeurs en 2012. Il a été estimé que le coût de l'inscription des électeurs était de 75 333 livres égyptiennes (10 dollars) par électeur, et une carte à puce que le pays envisage d'introduire pourrait coûter 120 579 livres égyptiennes (16 dollars). Les différentes cartes du pays ne sont pasinteropérables, il n'existe aucun mécanisme permettant de relier les identités entre les différents registres d'identité, et les données qu'elles contiennent sont souvent incohérentes et ont été décrites comme peu fiables.<sup>96</sup> Avant les élections présidentielles et générales de 2018, le gouvernement a adopté un exercice d'inscription biométrique des électeurs. Le processus, qui a été mis en œuvre conjointement par la Commission électorale nationale (NEC) et l'Autorité nationale de l'état civil (NCRA), n'a toutefois pas inclus l'identification biométrique des électeurs le jour du scrutin.

Avant les élections de 2023, le gouvernement a tenté d'introduire des amendements à la Loi sur les élections publiques qui exigeraient que les citoyens aient un numéro d'identification national (NIN), exigeant essentiellement l'enregistrement biométrique auprès de la NCRA pour avoir le droit de voter. Cependant, cette décision a été largement condamnée par les militants qui ont travaillé pour s'assurer que les dispositions controversées soient retirées de la législation finale.

En 2015, le gouvernement tanzanien a introduit un système d'enregistrement biométrique<sup>97</sup> des électeurs avec une société privée néerlandaise, GenKey, travaillant en tant que sous-traitant pour Lithotech Exports, basée en Afrique du Sud, engagée pour mettre en œuvre le système par lequel 24 millions d'électeurs éligibles ont été enregistrés. En 2021, la présidente Samia Suluhu Hassan a indiqué que le gouvernement envisageait la possibilité d'introduire le vote biométrique lors des élections de 2025 afin de réduire le nombre d'irrégularités communes aux élections dans le pays.<sup>98</sup> En outre, cela améliorerait la participation des électeurs, car l'expérience montre que de nombreux électeurs occupés ont de la difficulté à assister au vote en personne.

<sup>95</sup> Décret n° 2016-1536 du 29 septembre 2016 portant application de la loi n° 2016-09 du 14 mars 2016 instituant une carte d'identité biométrique de la CEDEAO <http://www.jo.gouv.sn/spip.php?article10986>; carte d'identité biométrique de la CEDEAO : l'Assemblée nationale fait la loi <https://senegalservices.sn/actualite/carte-didentite-biometrique-cedeao-lAssemblee-nationale-vote-la-loi>

<sup>96</sup> Ibid croix réf 37

<sup>97</sup> Lancement de l'inscription biométrique des électeurs en Tanzanie <https://www.aa.com.tr/en/politics/biometric-voter-registration-kicks-off-in-Tanzania/72446>

<sup>98</sup> Le président tanzanien invoque la nécessité d'un vote biométrique pour freiner les irrégularités électorales <https://www.biometricupdate.com/202108/tanzanian-president-invokes-need-for-biometric-voting-to-curb-election-irreProfessions>

Au Togo, la Commission électorale nationale indépendante (CENI) a commencé l'enregistrement biométrique des électeurs en 2014 avant l'élection présidentielle de 2015. Le pays a utilisé les kits d'inscription mobile pour intégrer les nouveaux électeurs éligibles dans le système. Au cours de la campagne d'inscription des électeurs, la CENI a utilisé sa base de données existante de trois millions d'enregistrements pour vérifier les dossiers des citoyens, ainsi que pour supprimer tous les dossiers des personnes décédées et invalides, y compris ceux qui avaient été perdus ou dupliqués. La CENI vérifie à la fois les données démographiques et les données biométriques, en utilisant la reconnaissance d'empreintes digitales pour ces dernières. Une fois cette vérification en deux étapes terminée, les citoyens reçoivent une carte d'électeur imprimée.

Le système d'enregistrement biométrique et d'identification des électeurs du Togo est fourni par Zetes Group, basé en Belgique, qui a été acquis en 2017 par Panasonic pour créer le registre électoral national.<sup>99</sup> Le système permet l'enregistrement, la centralisation dans une base de données unique, la vérification des données biométriques par le système automatisé d'identification dactyloscopique (AFIS), la reconnaissance faciale, la gestion des litiges et la publication des listes électorales.<sup>100</sup> Le système utilise à la fois les empreintes digitales et la biométrie faciale et a été utilisé pour la première fois pour l'inscription biométrique des électeurs en 2007, puis pour les exercices ultérieurs en 2010 et 2013.<sup>101</sup> Grâce à ce processus, les données de trois millions de Togolais ont été collectées et traitées.

En Ouganda, un registre biométrique des électeurs a été introduit pour la première fois en 2001 avec la mise en œuvre du projet de systèmes photographiques d'enregistrement et d'identification des électeurs (PVRIS), devenant ainsi l'un des premiers à adopter la biométrie en Afrique.<sup>102</sup> Les électeurs ont été inscrits à l'aide d'un appareil photo numérique pour prendre une photo de l'électeur, et les données biographiques ont été capturées à l'aide d'un formulaire d'inscription sur papier. En 2016, la Commission électorale a adopté le système de vérification biométrique des électeurs (BVVS) avec les empreintes digitales et les images de tous les électeurs inscrits. Les dossiers de ces électeurs (qui, lors des élections de 2016, concernaient plus de 15,27 millions de personnes) provenaient du système d'information sur la sécurité nationale, géré par l'Autorité nationale d'identification et d'enregistrement (NIRA) et servant de base à la délivrance des cartes d'identité nationales. Le BVVS utilise les empreintes digitales pour faire correspondre les détails de l'électeur afin de confirmer que le candidat est inscrit sur les listes électorales d'un bureau de vote donné. Les données dans les BVV comprennent le nom, le lieu et la date de naissance, l'emplacement du bureau de vote et les empreintes digitales de l'électeur. Le BVVS a également été utilisé lors des élections de 2021, privant ainsi de leurs droits les citoyens qui ne possédaient pas de carte d'identité nationale.

En 2020, le gouvernement zambien, avec le soutien du Programme des Nations unies pour le développement (PNUD), a choisi Smartmatic International pour mettre en œuvre l'inscription biométrique des électeurs afin d'améliorer le registre électoral du pays.<sup>103</sup> Le projet d'inscription des électeurs en Zambie s'inscrit dans le cadre de l'engagement continu du PNUD à améliorer la performance des gouvernements démocratiques. Le système utilise la technologie de numérisation des empreintes digitales et du visage pour capturer des données biométriques ainsi que des copies écologiques des cartes d'identité. Le système a été mis en œuvre dans tout le pays et a capturé les données des sept millions de personnes qui ont voté aux élections générales d'août 2021.

<sup>99</sup> Qui sommes-nous ? <https://peopleid.zetes.com/en/about-us>

<sup>100</sup> ZETES en charge de l'enregistrement des électeurs pour les récentes élections municipales au Togo <https://peopleid.zetes.com/en/Togo-Local-Elections-2019>; Enregistrement biométrique au Togo <https://peopleid.zetes.com/en/reference/biometric-voter-registration-togo>

<sup>101</sup> Enregistrement biométrique des électeurs au Togo <https://peopleid.zetes.com/en/reference/biometric-voter-registration-togo>

<sup>102</sup> Introduction de la technologie biométrique dans les élections <https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf>

<sup>103</sup> Zambie : le registre électoral du pays passe à la biométrie <https://www.smartmatic.com/us/case-studies/article/zambia-countrys-voter-register-goes-over-to-biometrics/>

### 2.2.3 Programmes de vidéosurveillance dirigés par le gouvernement avec reconnaissance faciale

La reconnaissance faciale basée sur le mobile par les compagnies de téléphonie mobile telles que FaceID d'Apple et les différents systèmes basés sur Android a accéléré l'adoption et l'acceptation des systèmes d'authentification par empreintes digitales et par visage.<sup>104</sup> L'émergence du phénomène COVID-19 couplée au développement rapide de l'intelligence artificielle ces dernières années a également stimulé le déploiement de la technologie de reconnaissance faciale. La reconnaissance faciale a été utilisée pour la recherche des contacts COVID-19 en Corée du Sud, en Chine, en Russie, en Inde, en Pologne et aux États-Unis.<sup>105</sup>

Plusieurs pays ont déployé une surveillance par caméra de télévision en circuit fermé (CCTV) dans les grandes villes et les rues. Certains de ces projets ont été mis en œuvre dans le cadre de la Safe City de Huawei.<sup>106</sup> Les systèmes du produit comprennent la mise en place de centres de commande, de caméras de vidéosurveillance, de vidéosurveillance intelligente, de technologie de reconnaissance faciale et de plaques d'immatriculation, de surveillance des foules, de détection de la connaissance de la situation, de surveillance ou de détection du bruit, de détection d'objets abandonnés et de surveillance des médias sociaux.<sup>107</sup> En 2019, les systèmes de vidéosurveillance appartenant à des états avaient été mis en œuvre dans plusieurs pays du continent, notamment en Algérie, en Angola, au Botswana, au Cameroun, en Égypte, en Éthiopie, au Ghana, en Côte d'Ivoire, au Kenya, à Madagascar, à l'île Maurice, au Maroc, au Nigeria, en Afrique du Sud, en Tunisie, en Ouganda, en Zambie et au Zimbabwe.<sup>108</sup> Cependant, les préoccupations concernant ces technologies comprennent les biais algorithmiques, le piratage, les violations de la vie privée, les problèmes de sécurité et la conformité légale, en particulier en ce qui concerne le consentement et la façon dont les données sont obtenues.<sup>109</sup>

<sup>104</sup> C'est une nouvelle décennie pour la biométrie. Terminons 2019 et jetons un coup d'œil à ce qui nous attend en 2020

<https://www.acuitymi.com/post/it-s-a-new-decade-for-biometrics-let-s-wrap-up-2019-et-regardez-quoi-dans-le-magasin-pour-2020>

<sup>105</sup> Éloignez la reconnaissance faciale de la riposte au COVID-19

<https://www.cato.org/blog/keep-facial-recognition-away-covid-19-response>

<sup>106</sup> Huawei dévoile l'expérience Safe City Solution Centre au Mobile World Congress 2016

<https://www.huawei.com/us/news/2016/2/unveils-safe-city-solution-experience-center>

<sup>107</sup> La ville sûre de Huawei est-elle sûre pour les villes africaines ?

<https://techcabal.com/2021/08/04/is-huaweis-safe-city-safe-for-africans/>; Regarder les « villes sûres » de Huawei

[https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191030\\_HillmanMcCalpin\\_HuaweiSafeCity\\_layout\\_v4.pdf](https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/191030_HillmanMcCalpin_HuaweiSafeCity_layout_v4.pdf)

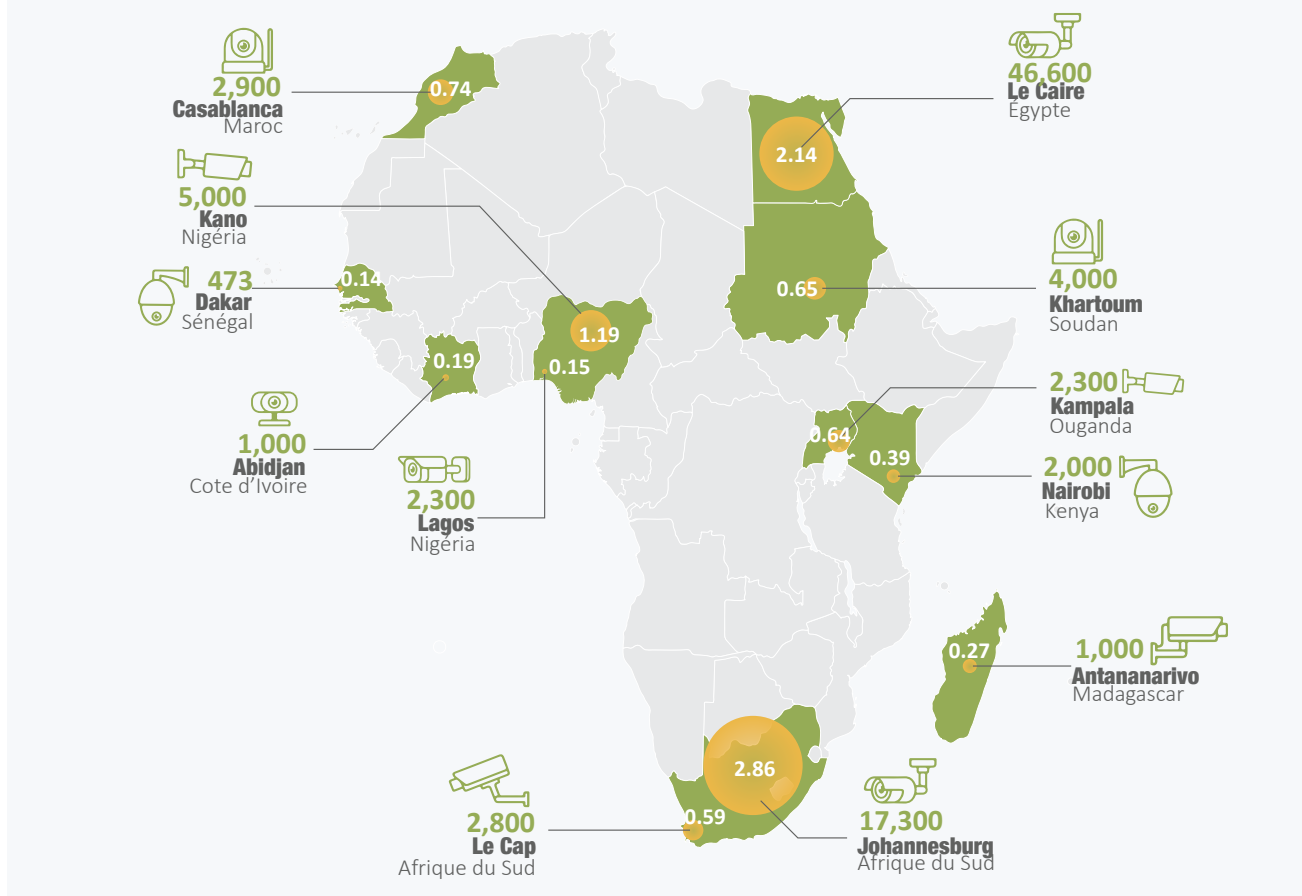
<sup>108</sup> Le programme de technologie de surveillance de Huawei « Safe Cities » est désormais actif dans 12 pays d'Afrique

<https://chinaglobalsouth.com/2019/11/13/huaweis-surveillance-technology-program-safe-cities-now-active-en-12-pays-africains/>

<sup>109</sup> L'avenir de la technologie de reconnaissance faciale en Afrique <https://issafrika.org/iss-today/future-of-facial-recognition-technology-iAfrrique-du-Nord>



la figure 1: Estimation du nombre et de la densité des caméras de vidéosurveillance dans certaines villes d'Afrique<sup>110</sup>



Comme le montre le tableau ci-dessus, certaines des villes africaines ayant la plus forte densité de vidéosurveillance sont: Johannesburg, Afrique du Sud avec 17 300 caméras (2,86 pour 1 000 habitants); Le Caire, Égypte avec 46 600 caméras (2,14 pour 1 000 habitants); et Kano, au Nigéria, avec 5 000 caméras (1,19 pour 1 000 habitants).

En Angola, le Centre intégré pour la sécurité publique (CISP) lancé en décembre 2019 et exploité par les forces de sécurité de l'État utilise des caméras de vidéosurveillance pour surveiller les citoyens de Luanda, la capitale du pays.<sup>111</sup> On estime à 955 le nombre de caméras installées par Huawei dans la ville et équipées d'une capacité de reconnaissance faciale.<sup>112</sup> Les agences de sécurité de l'État sont autorisées par la loi angolaise à installer des caméras de vidéosurveillance sans autorisation préalable, et les forces de l'ordre peuvent déployer des technologies de surveillance, y compris des logiciels espions et l'interception des communications selon les besoins.<sup>113</sup>

En 2014, le Cameroun a piloté 70 caméras de vidéosurveillance dans six grandes villes, puis les a portées à 1 500<sup>114</sup> pour la vidéosurveillance dans le cadre du projet de ville intelligente du pays utilisant le système Safe Cities de Huawei.<sup>115</sup> En 2019, le gouvernement a lancé le Centre national de commande de vidéosurveillance et des propositions sont à l'étude pour ajouter 7 000 caméras à l'écosystème.<sup>116</sup>

<sup>110</sup> Statistiques sur les caméras de surveillance : quelles villes ont le plus de caméras de vidéosurveillance ?

<https://www.comparetech.com/vpn-privacy/the-worlds-most-surveilled-cities/>

<sup>111</sup> Tout pour mon Cuba <https://tudoparaminhacuba.wordpress.com/2019/12/30/pr-abre-centro-integrado-de-seguranca-publica/>

<sup>112</sup> Statistiques sur les caméras de surveillance : quelles villes ont le plus de caméras de vidéosurveillance ?

<https://www.comparetech.com/vpn-privacy/the-worlds-most-surveilled-cities/>

<sup>113</sup> Liberté du Net 2020 : Angola [https://freedomhouse.org/country/angola/freedom-net/2020#footnote6\\_pib2ugn](https://freedomhouse.org/country/angola/freedom-net/2020#footnote6_pib2ugn)

<sup>114</sup> Sécurité : 22,95 milliards de FCFA pour l'expansion du projet de vidéosurveillance de l'intelligence urbaine

<https://cameroon-report.com/securite/security-fcfa-22-95-billion-for-expansion-of-urban-intelligence-video-surveillance-project/>

<sup>115</sup> Le Cameroun dévoile la vidéosurveillance construite par Huawei centre

<https://itweb.africa/content/rW1xL759r3B7Rk6m>

<sup>116</sup> Atteinte à la sécurité ou à la vie privée: Huawei installe plus de caméras de vidéosurveillance au Cameroun

<https://techpoint.africa/2019/08/29/huawei-cctv-cameroon>

En attendant, les ministères camerounais de l'Administration territoriale et des Postes et Télécommunications envisagent l'installation de la reconnaissance faciale à travers le service e-police offert par le Réseau national de télécommunications d'urgence (RNTU). Ce réseau a été lancé le 5 janvier 2017, pour un coût estimé à plus de 77 milliards de francs CFA (120,7 millions USD) et offre des services destinés à assurer la sécurité des personnes et de leurs biens dans les 10 villes du pays. Ces services comprennent les appels standards et d'urgence, la police électronique, la vidéosurveillance et les conférences. La gendarmerie et la police utilisent déjà des caméras de vidéosurveillance pour leurs enquêtes. Le service e-police s'appuie sur des terminaux installés dans 50 commissariats de gendarmerie répartis sur l'ensemble du territoire. Il permet le stockage des informations des citoyens dans les bases de données de la police, ainsi qu'un suivi des individus en fonction de leurs empreintes digitales ou de leur reconnaissance faciale.<sup>117</sup>

Le Kenya a été l'un des premiers pays à déployer le système African Safe Cities de Huawei, qui a connecté 1 800 caméras de haute définition et 200 infrastructures de surveillance du trafic haute définition dans la capitale, Nairobi, en 2014.<sup>118</sup> Le projet Public Safety Communication and Surveillance System (IPSCSS)<sup>119</sup> visait à contribuer à la prévention de la criminalité et à accélérer l'intervention et le rétablissement. Cependant, les données du Service national de police indiquent que le système n'a pas permis de réduire beaucoup les taux de criminalité dans la ville, où la criminalité a augmenté entre 2017 et 2018.<sup>120</sup> En outre, les aéroports du Kenya utilisent la technologie faciale et d'empreintes digitales installée en 2019. Le projet de stabilisation communautaire globale de la côte et des points frontaliers clés, financé par le Japon,<sup>121</sup> a soutenu l'installation de la technologie de reconnaissance faciale<sup>122</sup> NeoFace Watch de NEC.<sup>123</sup> La même technologie a été déployée sur les routes principales et autoroutes dans le cadre d'une mise à niveau du réseau de vidéosurveillance du Système intégré de commandement et de contrôle (ICCS) du pays.<sup>124</sup>

Au Lesotho, où il n'existe actuellement aucun programme de vidéosurveillance dirigé par le gouvernement avec reconnaissance faciale, il existe quelques systèmes de vidéosurveillance, qui sont gérés par différents ministères, tels que l'armée qui effectue la vidéosurveillance de certains endroits. Le Libéria n'a pas de programme officiel de vidéosurveillance du gouvernement. Cependant, les entreprises individuelles et privées sont libres d'acquérir des caméras de vidéosurveillance avec reconnaissance faciale et de les utiliser à volonté.

En 2016, le gouvernement du Mozambique a commencé à installer une surveillance CCTV dans les villes de Maputo et Matola, prétendument pour des raisons de sécurité. Le projet aurait été attribué sans appel d'offres public.<sup>125</sup> Le projet impliquerait l'installation de 450 caméras de surveillance à Maputo et Matola dans le cadre du projet du Commandement national d'interception de l'information, qui comprenait également un prétendu plan d'« écoute téléphonique » pour espionner le public.<sup>126</sup>

<sup>117</sup> Technologie : la reconnaissance faciale bientôt effective au Cameroun <https://www.237online.com/technologie-la-reconnaissance-faciale-bientot-effective-au-cameroun/>

<sup>118</sup> La diffusion des technologies de surveillance en Afrique suscite des inquiétudes en matière de sécurité <https://africacenter.org/spotlight/surveillance-technology-in-africa-security-concerns/>

<sup>119</sup> La surveillance est-elle une panacée aux menaces sécuritaires du Kenya <https://giswatch.org/en/country-report/communications-surveillance/kenya#sdfootnote11sym>

<sup>120</sup> L'impact de la disposition technologique chinoise sur les libertés civiles en Afrique <https://www.africaportal.org/documents/20819/Policy-Insights-99-gagliardone.pdf>

<sup>121</sup> Technologie frontalière de reconnaissance faciale NEC pour le Kenya en tant que biométrie aéroportuaire. Les déploiements se poursuivent <https://www.biometricupdate.com/201910/nec-facial-recognition-border-tech-for-kenya-as-airport-biometrie-deploiements-continuer>

<sup>122</sup> Nec [www.nec.com](http://www.nec.com)

<sup>123</sup> NeoFace Montre <https://www.nec.com/en/global/solutions/biometrics/face/neofacewatch.html>

<sup>124</sup> La police kenyane lance la reconnaissance faciale sur un réseau de vidéosurveillance urbain <https://www.biometricupdate.com/201809/kenyan-police-launch-facial-recognition-on-urban-cctv-network>

<sup>125</sup> Club pour le Mozambique, « Les citoyens seront surveillés 24 heures sur 24 – Global Voices, <https://clubofmozambique.com/news/mozambique-citizens-to-be-monitored-24-hours-a-day-global-voices/>

<sup>126</sup> Mozambique : les citoyens seront surveillés 24 heures sur 24 – Global Voices <https://clubofmozambique.com/news/mozambique-citizens-to-be-monitored-24-hours-a-day-global-voices/>

Au Nigeria, le gouvernement fédéral a attribué un contrat de 470 millions USD pour l'installation de 2 000 caméras de vidéosurveillance à Abuja et Lagos à une entreprise chinoise, ZTE Communications, en 2010.<sup>127</sup> Deux ministères, à savoir le ministère des Finances et le ministère des Affaires policières, ainsi que la Nigerian Communications Satellite Limited (NIGCOMSAT), ont signé un accord tripartite pour la gestion des caméras de vidéosurveillance. L'accord fait du ministère fédéral des Finances l'emprunteur du fonds, le ministère des affaires de police a été désigné comme bénéficiaire et la Nigerian Communication Satellite Limited a été répertoriée comme l'opératrice. Le projet devait être livré d'ici juillet 2011.<sup>128</sup> Cependant, le projet a été abandonné par le gouvernement après que la vidéosurveillance ait été installée. Ainsi, beaucoup de caméras de vidéosurveillance installées à Abuja ne fonctionnent pas.<sup>129</sup>

Dans sa quête pour mettre en œuvre l'initiative Smart City, l'État de Lagos a commencé l'installation de 2 000 caméras de vidéosurveillance. Le commissaire à la science et à la technologie, Hakeem Popoola Fahm, a fait cette révélation lors de la conférence de presse ministérielle de 2021 pour commémorer la deuxième année au pouvoir de l'administration du gouverneur Babajide Sanwo-Olu. Le gouvernement de Lagos avait précédemment installé 100 caméras de vidéosurveillance dans la métropole d'Ikeja.<sup>130</sup> Pendant ce temps, le service d'inspection des véhicules de l'État de Lagos utilise la reconnaissance des plaques d'immatriculation des images de vidéosurveillance pour surveiller les contrevenants au code de la route et imposer des sanctions aux propriétaires de véhicules fautifs, la contravention de l'amende étant envoyée à l'adresse et au numéro de téléphone du propriétaire du véhicule incriminé. Certains agents des forces de l'ordre de l'État de Lagos porteraient maintenant des caméras corporelles.<sup>131</sup>

Dans le but de lutter contre l'insécurité dans l'État d'Ondo à la suite de l'attaque de juin 2022 contre une église dans laquelle jusqu'à 40 personnes ont été tuées, le gouverneur de l'État a signé un décret pour l'utilisation obligatoire d'appareils de vidéosurveillance dans les institutions publiques et privées. Il a déclaré que le décret serait appliqué dans les lieux de culte, les institutions financières, les établissements d'enseignement et les centres d'événements ainsi que dans d'autres lieux régulièrement utilisés par le public. Le décret stipule également que les dispositifs CCTV installés, en plus de capturer toutes les activités des institutions publiques et privées, doivent également disposer de matériel de stockage de données et que les données qui y sont stockées doivent être mises à la disposition des agences de sécurité chaque fois que cela est nécessaire.<sup>132</sup>

En juin 2021, le secrétaire général de la Haute Autorité des aéroports du Sénégal (HAAS), le colonel Ababacar Sédikh Diouf, a annoncé le projet d'installation d'un système de vidéosurveillance avec reconnaissance faciale. Ce système renforcerait la sécurité des aéroports et des pays et serait relié à la base de données d'Interpol et à la liste des terroristes recherchés. À ce jour, rien n'indique que ce système ait été mis en place à l'aéroport de Dakar.<sup>133</sup>

En Sierra Leone, les médias ont rapporté en 2017 que la police sierra-léonaise (SLP) investissait 4,5 milliards de livres égyptiennes (294 213 dollars) dans des caméras de vidéosurveillance dans le cadre de son projet Safe City. Lors de l'audience budgétaire du 2018 le 21 août 2017, le SLP a annoncé qu'il installerait également le système national de communication radio numérique, avec une ligne d'appel sans frais 112 et la mise en place de la salle de contrôle qui permettrait à la force de répondre à la criminalité, à d'autres menaces à la sécurité et au désordre public.<sup>134</sup>

<sup>127</sup> Le projet de caméra de vidéosurveillance d'Abuja de 470 millions de dollars est en ruines  
<https://guardian.ng/sunday-magazine/cityfile/abuja-470m-cctv-camera-project-lies-in-ruins/>

<sup>128</sup> <https://www.tekedia.com/the-nigerias-cctv-bill/>

<sup>129</sup> <https://www.premiumtimesng.com/news/163975-high-level-corruption-rocks-470million-cctv-project-secure-abuja.html>

<sup>130</sup> <https://www.sunnewsonline.com/lagos-begins-installation-of-2000-cctv-cameras/>

<sup>131</sup> Droit de la surveillance en Afrique : examen de six pays  
[https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts\\_Surveillance\\_Law\\_in\\_Africa.pdf?sequence=1&isAllowed=](https://opendocs.ids.ac.uk/opendocs/bitstream/handle/20.500.12413/16893/Roberts_Surveillance_Law_in_Africa.pdf?sequence=1&isAllowed=)

<sup>132</sup> Akeredolu ordonne l'installation obligatoire de caméras de surveillance dans les lieux publics  
<https://punchng.com/akeredolu-orders-compulsory-installation-of-cctv-in-public-places/>

<sup>133</sup> Sénégal : Blaise Diagne L'aéroport international lance la reconnaissance faciale  
[https://www.aeronautique.ma/Senegal-L-Aeroport-international-Blaise-Diagne-se-met-a-la-reconnaissance-faciale\\_a4843.html](https://www.aeronautique.ma/Senegal-L-Aeroport-international-Blaise-Diagne-se-met-a-la-reconnaissance-faciale_a4843.html)

<sup>134</sup> La police installera des caméras de vidéosurveillance à Freetown <https://zainabijoaque.wordpress.com/2018/03/16/police-to-install-cctv-cameras-across-freetown/>

En Tanzanie, le gouvernement s'est lancé dans une frénésie d'installations de vidéosurveillance dans les prisons,<sup>135</sup> le parc national de Mukumi,<sup>136</sup> ainsi qu'autour du mur de Mimerani<sup>137</sup> de 25 kilomètres au nord du pays dans le but de contrôler le vol dans les prisons, de freiner le braconnage ainsi que le vol de minéraux pour contrôler le vol de minéraux tanzanites, respectivement. En 2018, le pays a mis en place le système de contrôle biométrique aux frontières avec reconnaissance faciale aux aéroports internationaux du Kilimandjaro et Julius Nyerere à l'aide de la technologie fournie par Vision-Box.<sup>138</sup>

En octobre 2018, le président ougandais Museveni a mis en service un centre de surveillance CCTV doté d'une capacité de reconnaissance faciale fournie par le géant chinois des télécommunications Huawei Technologies. Le système de 126 millions de dollars comprenait l'installation de 2 300 caméras couvrant la métropole de Kampala.<sup>139</sup> Le système national de vidéosurveillance comprenait initialement 83 centres de surveillance, dotés de 522 opérateurs et 50 commandants. Les autorités ont indiqué qu'il était prévu de l'intégrer à d'autres organismes ougandais tels que l'Autorité fiscale ougandaise et le Département de l'immigration.<sup>140</sup>

En janvier 2020, la deuxième phase a été lancée pour couvrir 2 319 municipalités et grandes villes. En 2022, les forces de police ougandaises ont indiqué qu'elles avaient besoin de 20 000 caméras supplémentaires pour couvrir le pays et un projet d'installation de 5 000 caméras supplémentaires pour couvrir les bidonvilles de Kampala était en cours à hauteur de 50 millions de dollars.<sup>141</sup> Les dirigeants de l'opposition dans le pays se sont opposés par le passé au projet de vidéosurveillance comme un stratagème pour traquer et persécuter les dirigeants de l'opposition plutôt que de suivre la criminalité.<sup>142</sup>

De son côté, le gouvernement zambien aurait déployé en 2020 des solutions de projet de caméras de surveillance sur les routes, soi-disant pour aider à réduire la criminalité et permettre à la police de surveiller les points chauds dans les zones sujettes à la criminalité. Sous le nom de code Advanced Road Safety Management System and the Intelligent Mobility Solutions (IMS) – Safe City Project, l'initiative a été mise en œuvre par une société chinoise, Zhongxing Telecommunication Equipment (ZTE) Corporation.<sup>143</sup>

## 2.2.4 Programmes nationaux de passeport électronique biométrique

En juillet 2016, l'Union africaine (UA) a dévoilé le premier passeport électronique du continent, lors d'un sommet de l'UA à Kigali, au Rwanda, dans le but de le distribuer à tous les citoyens africains d'ici 2020 afin de faciliter les déplacements sur le continent.<sup>144</sup> Bien que cela ne se soit pas produit, plusieurs pays et blocs économiques ont adopté le concept et introduit des passeports électroniques à leurs citoyens, qui ont des puces électroniques pour stocker les informations biométriques du titulaire du passeport.

<sup>135</sup> Tanzanie : Le gouvernement installe des détecteurs et des caméras de vidéosurveillance dans les prisons <https://allafrica.com/stories/202005270227.html>

<sup>136</sup> Installer des caméras CCTV en Tanzanie dans le sanctuaire sud pour freiner le braconnage <https://www.savetheelephants.org/about-elephants-2-3-2/elephant-news-post/?detail=tanzania-to-install-cctv-cameras-in-southern-sanctuary-to-curb-poaching>

<sup>137</sup> La Tanzanie installe des caméras de vidéosurveillance pour contrôler le vol de minerais <https://www.newtimes.co.rw/article/164162/News/tanzania-installs-cctv-cameras-to-control-theft-of-minerals#:~:text=Surveillance%20cameras%2C%20scanners%20as%20well,been%20commissioned%20by%20the%20government.>

<sup>138</sup> Les autorités tanzaniennes adoptent la technologie Vision-Box pour le contrôle biométrique dans les aéroports <https://findbiometrics.com/tanzanian-authorities-adopt-vision-box-tech-501292/>

<sup>139</sup> Ouganda »Les flics à court d'argent dépensent 126 millions de dollars en vidéosurveillance de Huawei <https://www.reuters.com/article/us-uganda-crime/ugandas-cash-strapped-cops-send-126-million-on-cctv-from-huawei-idUSKCN1V50RF>

<sup>140</sup> L'Ouganda utilise la technologie de reconnaissance faciale de Huawei pour réprimer la dissidence après les manifestations antigouvernementales <https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters/>

<sup>141</sup> La police ougandaise demande 5 000 caméras de vidéosurveillance pour surveiller les bidonvilles <https://www.independent.co.ug/police-ask-for-5000-cctv-cameras-to-monitor-slums/>

<sup>142</sup> L'Ouganda investit 126 millions de dollars dans la vidéosurveillance avec la biométrie faciale de Huawei <https://www.biometricupdate.com/201908/uganda-invests-126m-in-cctv-with-facial-biometrics-from-huawei>

<sup>143</sup> ZM: Projets de caméras de surveillance déployés pour surveiller les personnes <http://www.ifg.cc/aktuelles/nachrichten/regionen/568-zm-sambia-zambia/58826-zm-surveillance-camera-projets-déployés-pour-sur-les-personnes.html>

<sup>144</sup> États-Unis d'Afrique? L'Union africaine lance un passeport panafricain <https://www.cnn.com/2016/07/05/africa/african-union-passport>

La mise en œuvre des passeports électroniques nécessite le déploiement de systèmes numériques avancés de gestion des frontières, y compris une infrastructure de collecte et de traitement des données biométriques, des systèmes de contrôle d'accès, des bases de données d'identification biométrique, des répertoires à clé publique, et de protocoles de partage d'informations pour desservir les points frontaliers d'un pays. La plupart de ces systèmes devraient être interopérables et développés conformément aux normes et aux pratiques recommandées de l'Organisation de l'aviation civile internationale (OACI).<sup>145</sup> Selon OACI, plus de 140 États et entités non étatiques telles que les Nations unies utilisent actuellement des passeports électroniques, avec plus de 1 milliard de passeports électroniques en circulation.<sup>146</sup>

En avril 2017, le Conseil des ministres de la Communauté d'Afrique de l'Est (CAE) a demandé aux États partenaires (Burundi, République démocratique du Congo, Kenya, Rwanda, Soudan du Sud, Tanzanie et Ouganda) de commencer à délivrer le nouveau passeport électronique de la CAE d'ici le 31 janvier 2018<sup>147</sup> et d'éliminer progressivement les anciens passeports d'ici novembre 2022.<sup>148</sup>

En République démocratique du Congo (RDC), les médias ont rapporté en 2016 qu'un nouveau modèle de passeport biométrique contenant une puce électronique avait été officiellement dévoilé le 10 novembre 2015.<sup>149</sup> Le passeport, conforme aux normes de l'OACI, et le système de délivrance ont été élaborés par Semlex, une société belge.<sup>150</sup> Les informations collectées comprennent des photographies, des empreintes digitales et d'autres informations personnelles ainsi que des frais d'enregistrement de 185 USD, partagés entre le gouvernement (65 USD) et Semlex (125 USD).<sup>151</sup> En juin 2022, il a été signalé qu'il y avait une controverse autour du contrat Semlex, y compris des accusations de corruption et de blanchiment d'argent en RDC<sup>152</sup> et ses projets dans d'autres pays africains tels que la Côte d'Ivoire et le Kenya.<sup>153</sup>

Le gouvernement kenyan a été le premier de la CAE à déployer le passeport électronique en septembre 2017 après son annonce en décembre 2016 pour remplacer le passeport de première génération.<sup>154</sup> Le coût initial du projet était de 1,5 milliard de KES (12,4 millions USD) et devrait tripler au bout de la troisième année. L'Autorité nationale pakistanaise de la base de données et d'enregistrement (NADRA) a remporté l'appel d'offres pour le système de passeport électronique et a délivré 775 000 passeports en mai 2019. Les passeports sont conformes aux normes de l'OACI, disposent d'un lien avec l'infrastructure à clé publique (PKI), d'une puce RFID et sont intégrés à des caractéristiques biométriques telles que l'image faciale et les empreintes digitales.<sup>155</sup> Le passeport électronique coûte entre 37,7 et 62,6 USD selon le nombre de pages et 99,9 USD à remplacer en cas de perte.<sup>156</sup> Les délais de retrait progressif de l'ancien passeport ont été prolongés à plusieurs reprises depuis 2018 jusqu'au plus récent, le 30 novembre 2022, pour tous les États partenaires de la CAE.<sup>157</sup>

<sup>145</sup> Guide de voyage OACI sur le contrôle et la gestion des frontières

<https://www.icao.int/Security/FAL/TRIP/Documents/ICAO%20TRIP%20Guide%20BCM%20Part%201-Guidance.pdf>

<sup>146</sup> Principes de base du passeport électronique <https://www.icao.int/Security/FAL/PKD/Pages/ePassport-Basics.aspx>

<sup>147</sup> La CAE commencera à délivrer le passeport électronique EA janvier 2018

<https://www.eac.int/press-releases/148-immigration-and-labour/754-eac-to-start-émission-ea-ePassport-janvier-2018>

<sup>148</sup> Le Kenya fixe une date limite pour Migration vers le passeport électronique du CAE <https://cioafrica.co/kenya-sets-deadline-for-migration-to-eac-e-passport/>

<sup>149</sup> Le Potentiel 13 nov. 2015; Radio Okapi 10 novembre 2015; Congo virtuel 10 Nov. 2015

<sup>150</sup> République démocratique du Congo: Passeports biométriques avec puces électroniques délivrés depuis novembre 2015, y compris la procédure de demande et les exigences, ainsi que la période de validité (2015-juillet 2016) <https://www.refworld.org/docid/57a18bdf4.html>

<sup>151</sup> Passeport République démocratique du Congo [https://en.wikipedia.org/wiki/Democratic\\_Republic\\_of\\_the\\_Congo\\_passport](https://en.wikipedia.org/wiki/Democratic_Republic_of_the_Congo_passport)

<sup>152</sup> Le contrat de passeport biométrique lucratif et troublé du Congo est-il toujours ouvert ?

<https://www.biometricupdate.com/202207/congos-troubled-lucrative-biometric-passport-contract-still-open>

<sup>153</sup> Les enquêtes permettent de déterminer l'étendue – et les limites – de l' Semlex réseaux politiques en Afrique

<https://www.biometricupdate.com/202010/investigations-identify-the-extent-and-limitations-of-semlex-political-networks-in-africa>

<sup>154</sup> Le Kenya fait cavalier seul sur le passeport électronique alors que ses voisins tergiversent

<https://www.theeastafrican.co.ke/news/Kenya-goes-it-alone-on-e-passport-as-neighbours-dither-/2558-4082904-tnadadz/index.html>

<sup>155</sup> Système de passeport électronique Kenya <https://www.nadra.gov.pk/international-projects/e-passport-for-kenya/>

<sup>156</sup> Transition des passeports électroniques de l'ancienne génération aux passeports électroniques de nouvelle génération au Kenya

<https://cmadvocates.com/transition-from-the-old-generation-passports-to-the-new-generation-e-passports-in-kenya/>

<sup>157</sup> Migration chaotique vers le nouveau passeport électronique kenyan

<https://www.theelephant.info/features/2022/01/07/shambolic-migration-to-new-kenyan-e-passport/>



La Tanzanie est devenue le deuxième pays de la CAE à adopter le passeport électronique dans le cadre d'un projet qui a débuté en septembre 2017 et a été lancé en février 2018.<sup>158</sup> Le projet a été financé par le gouvernement irlandais, la société HID fournissant les services pour un coût de 57,82 millions de dollars.<sup>159</sup> Le programme national de passeport électronique est mis en œuvre par le ministère de l'Immigration et l'enregistrement commence par une demande en ligne où les demandeurs sont tenus de fournir leur numéro NIDA. Le processus d'enregistrement utilise les données biométriques de la personne collectées par le NIDA et le département de l'immigration, ainsi que des documents tels que des certificats de naissance, des cartes d'identité nationales, des affidavits de naissance ou des certificats de naturalisation.<sup>160</sup> Les renseignements biométriques recueillis comprennent les empreintes digitales, la photographie et les signatures du demandeur. Le passeport électronique, qui coûte 67,5 USD, a remplacé l'ancien passeport qui a été progressivement supprimé en janvier 2020.<sup>161</sup>

L'Ouganda a lancé le passeport électronique en 2018 et, en mai 2022, est devenu le premier État partenaire de la CAE à passer entièrement au passeport électronique de la CAE à la suite d'une directive de la CAE exhortant tous les États à éliminer progressivement les anciens passeports lisibles à la machine (MRP).<sup>162</sup> Le passeport électronique ougandais est conforme aux normes de l'OACI et comprend une puce RFID, des informations biographiques et des informations biographiques sécurisées telles que les empreintes digitales et les images faciales. Le passeport électronique est lié au titulaire par son numéro d'identification national (NIN). Les documents requis lors de la demande comprennent les cartes d'identité nationales, les certificats de naissance, les lettres de consentement et, le cas échéant, les documents à l'appui de la profession d'un candidat.<sup>163</sup>

La demande de passeport électronique en Ouganda est effectuée au coût de 67,81 USD. Notamment, le portail en ligne contient une politique de confidentialité explicite qui exige le consentement du demandeur avant de poursuivre. Il prévoit que les informations divulguées seront utilisées aux fins spécifiques du service offert et sont conservées pendant une période limitée pour atteindre l'objectif pour lequel elles ont été collectées.<sup>164</sup> En outre, il indique que l'agence s'engage à prendre des précautions pour protéger les renseignements d'un demandeur contre « toute perte ou utilisation, accès et divulgation illégaux » et que les renseignements sont protégés par des normes en ce qui concerne leur sensibilité.

Au Cameroun, la délivrance du passeport biométrique est effectuée par le Centre National de Production des Passeports rattaché à la Délégation Générale de la Sécurité Nationale (DGSN). Les candidats doivent saisir leurs données personnelles dans un formulaire de candidature en ligne et une fois ces données validées et les paiements effectués, le fichier de données d'identité complété est généré pour téléchargement. La deuxième phase consiste en un enregistrement physique où la signature, les empreintes digitales et la photo sont recueillis après vérification des informations fournies en ligne.<sup>165</sup>

La République centrafricaine délivre des passeports biométriques depuis 2012, conformément aux exigences de l'Union économique et monétaire des États de l'Afrique centrale (CEMAC).<sup>166</sup> Au Lesotho, le ministère de l'Intérieur, par l'intermédiaire de ses bureaux des passeports, a introduit les passeports électroniques en 2013. Pour demander le passeport électronique, tel que décrit dans la loi de 2018 sur les passeports et les voyages du Lesotho, il faut

<sup>158</sup> Passeport biométrique pour un contrôle plus strict de l'immigration et des frontières en Tanzanie

<https://www.m2sys.com/blog/e-governance/biometric-passport-for-tighter-immigration-and-border-control-in-tanzania/>

<sup>159</sup> La Tanzanie lance le passeport électronique en tant que Magufuli appelle à un contrôle plus strict des immigrants illégaux

<https://www.thecitizen.co.tz/tanzania/news/national/tanzania-launches-e-passport-as-magufuli-calls-for-tighter-control-of-illegal-immigrants-2621606#:~:text=President%20John%20Magufuli%20has%20on,key%20role%20in%20revenue%20collection>

<sup>160</sup> Passeports et Travel Documents Informations <https://www.immigration.go.tz/index.php/immigration-services/passports-and-travel-documents>

<sup>161</sup> La Tanzanie présente les passeports électroniques

<https://www.africanews.com/2018/02/01/tanzania-introduces-electronic-passports/>

<sup>162</sup> L'Ouganda est en tête de l'Afrique de l'Est pour passer pleinement au passeport électronique

<https://www.theeastafrican.co.ke/tea/news/east-africa/uganda-leads-east-africa-in-switching-to-e-passport-3825742>

<sup>163</sup> Passeport ordinaire <https://www.immigration.go.ug/passports/ordinary-passport>

<sup>164</sup> Démenti <https://www.passports.go.ug/>

<sup>165</sup> Un passeport biométrique en 48 heures au Cameroun <https://www.crtv.cm/2021/06/un-passeport-biometrique-en-48h-au-cameroun/>;

Police camerounaise <https://www.dgsn.cm/>; Bienvenue au passeport électronique du Cameroun pré-inscription portail <https://portal.passcam.cm/>

<sup>166</sup> Ibid croix réf 11

remplir le formulaire de demande disponible dans les bureaux des passeports et soumettre une copie des documents d'identité. Si le demandeur a moins de 16 ans, son certificat de naissance et le consentement écrit du parent ou du tuteur sont requis. Pendant le rendez-vous, une photo de format passeport et 10 empreintes digitales pour un jeune de 16 ans et plus sont prises. Les empreintes digitales des mineurs ne sont pas relevées.

Le Bureau des passeports du Libéria, qui relève du Ministère des affaires étrangères, est habilité à délivrer des passeports. Le ministère fournit aux demandeurs des services de demande de passeport en ligne et en personne. Dans le cadre du processus de demande, les informations biométriques des citoyens, y compris les photographies et les empreintes digitales, sont prises. Selon le ministère, le nouveau livret de passeport électronique libérien est doté d'une technologie de pointe, qui n'a plus de code à barres 2D, mais plutôt une puce de microprocesseur d'identification par radiofréquence (RFID) implantée dans le livret sans possibilité de détection par le toucher. Le nouveau passeport électronique biométrique libérien est conforme aux normes de l'OACI

Au Nigeria, le passeport électronique du Nigeria Immigration Service (NIS) a été entièrement harmonisé et intégré au NIMC à la suite de la mise en place obligatoire du lien entre le NIN et le passeport électronique. Le NIS a introduit le passeport électronique le 17 mai 2007. L'utilisation du passeport électronique est devenue un outil majeur dans la lutte contre la criminalité transfrontalière car il contient des données biométriques telles que les empreintes digitales et les images faciales ainsi que les signatures numériques des titulaires.

En 2019, NIS a mis en place une nouvelle exigence pour les ressortissants étrangers séjournant au Nigeria pendant plus de 90 jours de se rendre au bureau du NIS pour obtenir leurs données biométriques capturées, ainsi que de soumettre d'autres informations personnelles à enregistrer avant le 31 décembre de la même année. Les immigrants qui sont entrés dans le pays après le 31 décembre 2019 et qui ont cherché à rester au Nigéria pendant plus de 90 jours étaient tenus de s'inscrire dans le cadre du système.

L'État sénégalais a introduit le passeport biométrique à puce en octobre 2016 sous la direction de la police des étrangers et des documents de voyage (DPETV) du ministère de l'Intérieur qui collecte, stocke et imprime les passeports. Toutefois, la mise en œuvre et la maintenance du système d'émission sont effectuées par IRIS Corporation Berhad, une société malaisienne.

En Sierra Leone, les demandeurs de passeport sont tenus de se présenter au bureau de l'immigration où leurs données biométriques (empreintes digitales) sont capturées. Ils sont également tenus de soumettre ou de faire prendre leur photo de format passeport.<sup>167</sup>

Au Togo, les données biographiques recueillies sur un formulaire physique sont inscrites en bas et le demandeur donne ensuite accès à ses données biométriques telles que les empreintes digitales de tous les doigts, ainsi que leur photo et leur signature.

<sup>167</sup> Preuves documentaires pour les passeports ordinaires <https://slid.gov.sl/ordinary-passport/>

<sup>168</sup> Exigences relatives à la demande d'un passeport zambien ou d'un document d'identité de voyage [http://zambiahighcommission.ca/wp/wp-content/uploads/app\\_passport\\_guide.pdf](http://zambiahighcommission.ca/wp/wp-content/uploads/app_passport_guide.pdf)

<sup>169</sup> Demande de passeport <https://www.zambiaembassy.org/page/passport-application>

## 2.2.5 Programmes de traitement des données biométriques utilisés dans l'enregistrement des réfugiés

Pour améliorer leur prestation de services, plusieurs organisations humanitaires travaillant avec des communautés de réfugiés et de migrants, telles que le Haut-Commissariat des Nations Unies pour les réfugiés (HCR), ont adopté les technologies numériques telles que la biométrie, la cartographie spatiale et les plateformes médiatiques sociales dans les programmes humanitaires.<sup>170</sup> Cette technologie est devenue encore plus pertinente lorsque l'objectif de développement durable 16.9 des Nations Unies a donné à chaque personne le droit à une identité légale, y compris l'enregistrement des naissances, d'ici 2030.<sup>171</sup> Les données biométriques saisies lors de l'enregistrement des réfugiés par le HCR dans le cadre de ses 78 opérations dans le monde comprennent les empreintes digitales, les traits du visage et les scans de l'iris pour toutes les personnes de plus de cinq ans, en plus d'autres informations contenues dans les documents d'identité.<sup>172</sup>

Au Cameroun, la collecte d'identification biologique des réfugiés a lieu depuis 2016 sous la direction du HCR. Il concerne l'ensemble des 1,7 million<sup>173</sup> de réfugiés sous mandat du HCR au Cameroun et permet à l'agence « de disposer de données actualisées susceptibles de faciliter l'accès des réfugiés à l'aide humanitaire et d'assurer leur protection », selon le porte-parole du HCR. Les réfugiés sont tenus d'enregistrer leurs empreintes digitales, leurs photographies et leurs scans de l'iris.

Il s'agit d'une opération continue qui vise à mettre à jour les données d'identité de base, à inscrire les réfugiés âgés de plus de quatre ans, à procéder à une identification approfondie des personnes ayant des besoins spéciaux et à collecter des données sur les intentions de retour et à renouveler tous les documents (cartes d'attribution et attestation de réfugié).<sup>174</sup> En 2022, les autorités ont lancé un projet biométrique de lot visant à délivrer 6 000 cartes d'identité biométriques aux réfugiés centrafricains basés dans la région orientale du pays, qui seront étendus pour couvrir les 300 000 réfugiés restants dans le pays.<sup>175</sup> Le projet est mis en œuvre en partenariat avec le HCR et financé par la Banque mondiale avec le soutien technique d'Impact Palmarès R&D.

En RDC, le HCR est la principale agence travaillant dans le secteur des réfugiés en collaboration avec la Commission nationale de la RDC pour les réfugiés. L'agence des Nations Unies est censée avoir un département de gestion des données qui collabore avec l'Unité de protection sur la collecte de données biométriques.<sup>176</sup> Le pays compte 498 959 réfugiés, 5,6 millions de personnes déplacées à l'intérieur de leur propre pays (PDI) et 1,6 million de personnes déplacées de retour.<sup>177</sup>

Selon le HCR, le Kenya comptait une population totale de 504 932 personnes, dont des réfugiés (81%), des demandeurs d'asile (14%) et des apatrides (3%) en 2022, dont une majorité est originaire de Somalie (259 040), du Soudan du Sud (118 655) et de la République démocratique du Congo (48 968).<sup>178</sup> Les personnes qui demandent le statut de réfugié ou d'asile sont tenues de s'enregistrer auprès du Secrétariat des affaires des réfugiés du gouvernement du Kenya.<sup>179</sup> L'enregistrement se fait à Kakuma et Nairobi et utilise un système unifié de gestion des données qui est combiné à un système biométrique. Après l'enregistrement, une carte d'identité de réfugié, un certificat de réfugié ou une carte d'étranger est délivré.<sup>180</sup>

<sup>170</sup> ANALYSE : L'humanitaire numérique en Afrique : espoir ou battage médiatique ? <https://www.premiumtimesng.com/news/headlines/551771-analysis-digital-humanitarianism-in-africa-hope-or-hype.html>

<sup>171</sup> Ibid.

<sup>172</sup> Biométrie, HCR [https://help.unhcr.org/jordan/wp-content/uploads/sites/46/2022/04/Biometrics-EN\\_Final\\_April2022.pdf](https://help.unhcr.org/jordan/wp-content/uploads/sites/46/2022/04/Biometrics-EN_Final_April2022.pdf)

<sup>173</sup> Cameroun <https://reporting.unhcr.org/cameroon>

<sup>174</sup> Cameroun : Identification biométrique des réfugiés de Douala lancée par le HCR

<https://www.digitalbusiness.africa/cameroon-identification-biometrique-des-refugies-de-douala-lancee-par-lunhcr/>; Cameroun : Extrême-Nord Minawao résultats biométriques - avril 2018 <https://reliefweb.int/report/cameroon/cameroon-extr-me-nord-r-sultats-biom-trie-minawao-avril-2018>

<sup>175</sup> Le Cameroun lance un projet pilote de délivrance de cartes d'identité biométriques 6k aux réfugiés centrafricains

<https://www.biometricupdate.com/202207/cameroon-begins-pilot-to-issue-6k-biometric-id-cards-to-car-refugees>

<sup>176</sup> Enregistrement et profilage <https://reporting.unhcr.org/node/12365>; RD Congo

<https://reporting.unhcr.org/sites/default/files/UNHCR%20DRC%20Fact%20Sheet%20-%20July%202020.pdf>

<sup>177</sup> RDC <https://reporting.unhcr.org/drc>

<sup>178</sup> Kenya <https://reporting.unhcr.org/kenya>

<sup>179</sup> Inscription et documentation <https://www.unhcr.org/ke/registration>

<sup>180</sup> Reconnaissance des réfugiés de Nairobi <https://www.nrc.no/globalassets/pdf/reports/refugees-in-nairobi/recognising-nairobis-refugees.pdf>

Lors de l'enregistrement, les données biographiques et d'autres informations importantes relatives au demandeur, à sa famille et à ses proches vivant au Kenya et à l'étranger sont collectées.<sup>181</sup> De plus, des photos d'identité, des empreintes digitales et des scans de l'iris du demandeur et des membres de sa famille présents sont pris. Les demandeurs sont également tenus de présenter des documents tels que des passeports, des cartes d'identité nationales, des permis de conduire, des cartes d'identité militaires, des certificats de mariage ou de divorce, des livrets de famille, des certificats d'éducation, des dossiers médicaux et une preuve d'enregistrement antérieur en tant que réfugiés ou demandeurs d'asile dans d'autres pays. Une fois enregistrés, les demandeurs reçoivent une preuve d'enregistrement, un laissez-passer de demandeur d'asile, un laissez-passer de mouvement et, enfin, une carte d'identité de réfugié est délivrée à ceux qui remplissent les conditions requises.

Pour l'enregistrement des réfugiés, le Lesotho utilise le système du HCR connu sous le nom de Population Registration and Identity Management Ecosystem (PRIMES). Le système a été introduit au Lesotho en 2018 et comprend l'enregistrement des réfugiés, la gestion des cas ainsi que le système de gestion de l'identité biométrique (BIMS), le module qui collecte et gère les données biométriques des réfugiés. Ce système est basé sur les nuages (cloud) et géré par le HCR.<sup>182</sup>

Les 2,7 millions de réfugiés<sup>183</sup> au Nigéria sont tenus de s'enregistrer pour obtenir un numéro d'identification national afin de leur faciliter la délivrance de documents et de services appropriés. En 2021, les banques et les institutions financières nigérianes ont commencé à reconnaître les cartes d'identité de réfugiés délivrées par la Commission nationale pour les réfugiés, les migrants et les personnes déplacées à l'intérieur de leur propre pays (NCFRMI) et le HCR, ainsi que les documents de voyage conventionnels (CTD) fournis par la Commission et le service nigérian de l'immigration (NIS) pour faciliter leur identification, leurs opérations bancaires et leur inclusion financière. Les personnes déplacées à l'intérieur de leur propre pays (PDI) sont également tenues de s'inscrire auprès d'un NIN pour une bonne intégration sociale.

En 2017, le gouvernement tanzanien, par l'intermédiaire du Ministère de l'intérieur, du Département de l'immigration et de l'Organisation internationale pour les migrations (OIM), aurait lancé un système d'enregistrement biométrique des migrants irréguliers dans la région de Tanga.<sup>184</sup> Selon les rapports, l'enregistrement électronique des migrants en situation irrégulière et installés en Tanzanie fait suite à un projet pilote réussi dans la région de Kigoma dans lequel plus de 22 800 migrants ont été enregistrés et ont reçu une carte d'identité plastifiée personnalisée avec photo, qui leur permet de rester en Tanzanie jusqu'à deux ans, tandis que leur statut d'immigration est déterminé par les autorités tanzaniennes.<sup>185</sup> Le pays compte 247 033 réfugiés.<sup>186</sup>

En 2018, le gouvernement ougandais, avec le soutien du HCR, a lancé un programme à grande échelle visant à vérifier l'identité de 1,5 million de réfugiés présents dans le pays, à l'aide de données biométriques.<sup>187</sup> Le gouvernement utiliserait l'Ecosystème d'enregistrement biométrique de la population et de gestion de l'identité (PRIMES) du HCR, qui est utilisé pour enregistrer des millions de réfugiés dans le monde.<sup>188</sup>

<sup>181</sup> Comment puis-je enregistrer ma demande d'asile? <https://help.unhcr.org/kenya/applying-for-asylum-in-kenya/how-do-i-register-my-application-for-asylum/>

<sup>182</sup> De proGres à PRIMES <https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-03-16-PRIMES-Flyer.pdf>

<sup>183</sup> Nigéria <https://reporting.unhcr.org/nigeria>

<sup>184</sup> La Tanzanie lance un système d'enregistrement biométrique pour Migrants <https://www.iom.int/news/tanzania-launches-biometric-registration-system-migrants>

<sup>185</sup> Ibid.

<sup>186</sup> Tanzanie <https://reporting.unhcr.org/tanzania>

<sup>187</sup> L'Ouganda lance une grande opération de vérification des réfugiés

<https://www.unhcr.org/en-us/news/latest/2018/3/5a9959444/uganda-launches-major-refugee-verification-operation.html>

<sup>188</sup> Ibid.

## 2.2.6 Programmes d'enregistrement biométrique des cartes SIM

Au cours des dernières années, plusieurs pays africains ont cherché à lier l'enregistrement de la carte SIM à la biométrie des utilisateurs telle qu'elle est saisie dans les programmes nationaux d'identification, soulevant des préoccupations concernant la vie privée et la protection des données ainsi que l'exclusion de catégories de personnes qui n'ont peut-être pas de carte d'identité nationale. En fait, l'enregistrement obligatoire de la carte SIM a stimulé la demande et l'adoption d'informations d'identification numériques, deux éléments essentiels pour accéder aux services numériques.<sup>189</sup>

Au Cameroun, l'enregistrement de la carte SIM biométrique adossée à la carte nationale d'identité biométrique est en vigueur depuis 2016. L'article 6 du décret n° 2015/3759 relatif à l'identification des abonnés impose aux abonnés de cartes SIM de fournir leur carte d'identité nationale originale, leur adresse exacte, y compris une carte de localisation, et le numéro international d'identification de l'équipement mobile (IMEI) de leur appareil. Cela est conforme à l'article 55 de la loi sur les communications électroniques.

En 2019, le Conseil camerounais de régulation des télécommunications (ART) a sanctionné les opérateurs mobiles Orange, MTN et Nextel d'amendes d'un montant total de 3,5 milliards de francs CFA (5,9 millions de dollars) pour non-respect des règles d'enregistrement des cartes SIM. Le régulateur des télécommunications a accusé les opérateurs de continuer à vendre des cartes SIM non enregistrées et d'autres défaillances dans la gestion correcte des procédures d'enregistrement SIM stipulées par la loi.

Les réglementations d'Information et de Communication du Kenya de 2015<sup>190</sup> (Registration of SIM Cards) exigent que tous les abonnés à la carte SIM fournissent leurs informations biographiques telles que les noms, les dates de naissance, le sexe, l'adresse physique, l'adresse postale, les autres numéros possédés, des copies des cartes d'identité nationales, des cartes d'identité militaires, des passeports ou des certificats de naissance à l'opérateur de télécommunications.

En avril 2022, Safaricom, la plus grande entreprise de télécommunications du Kenya, a été poursuivie pour avoir exigé des photos de ses abonnés, en violation du règlement de 2015 sur l'information et la communication (enregistrement des cartes SIM) au Kenya et de l'article 31 de la loi de 2019 sur la protection des données.<sup>191</sup> La société a déclaré que la collecte des photos des abonnés visait à renforcer la sécurité et à réduire la fraude d'identité dans l'utilisation de ses services.<sup>192</sup> Le régulateur a ensuite précisé aux propriétaires des 64,9 millions de cartes SIM du pays<sup>193</sup> que la soumission de photos n'était pas obligatoire.<sup>194</sup>

Début 2022, l'autorité de réglementation des télécommunications du Kenya, l'Autorité des communications, a imposé au 15 avril la date limite pour l'enregistrement obligatoire de la carte SIM, après quoi toutes les cartes SIM non enregistrées seraient désactivées. Cependant, la date limite pour mettre à jour les registres des abonnés sur les détails a ensuite été reportée au 15 octobre 2022, après le tollé public concernant les courts délais pour se conformer à la directive.<sup>195</sup>

<sup>189</sup> Sur la voie du succès de l'identification numérique en Afrique : tirer parti des tendances mondiales <https://institute.global/policy/road-digital-id-success-africa-leveraging-global-trends>

<sup>190</sup> Règlement de 2015 sur l'information et la communication (enregistrement des cartes SIM) du Kenya, <https://www.ca.go.ke/wp-content/uploads/2018/02/Registration-of-SIM-%E2%80%93Cards-Regulations-2015-1.pdf>

<sup>191</sup> LSK veut que Safaricom soit contraint de supprimer Abonnés Photos <https://www.the-star.co.ke/news/2022-04-19-lsk-wants-safaricom-compelled-to-delete-subscribers-photos/>

<sup>192</sup> Enregistrement de la carte SIM: Pourquoi Safaricom prend vos photos <https://www.youtube.com/watch?v=B0zN1ooUKVA>

<sup>193</sup> Rapport sur les statistiques sectorielles du troisième trimestre pour l'exercice 2021/2022 (1er janvier - 31 mars 2022) <https://www.ca.go.ke/wp-content/uploads/2022/06/Sector-Statistics-Report-Q3-2021-2022.pdf>

<sup>194</sup> Vous n'êtes pas obligé de soumettre votre photo lors de l'enregistrement de la carte SIM – Chiloba <https://www.co.ke/news/you-are-not-required-to-submit-your-photo-during-sim-card-registration-chiloba-122677/>

<sup>195</sup> L'Autorité prolonge l'exercice de validation de l'enregistrement de la carte SIM Par Six mois <https://www.ca.go.ke/authority-extends-sim-card-registration-validation-exercise-by-six-months/>



L'Autorité des communications du Lesotho (LCA) a publié le Règlement sur les communications (module d'identité d'abonné et enregistrement des appareils mobiles) en mai 2021. Il est obligatoire d'enregistrer toutes les cartes SIM et tous les appareils mobiles utilisant des services de télécommunication au Lesotho. L'enregistrement est effectué par les entreprises de télécommunications, puis la base de données est périodiquement transférée à la LCA, qui est le gardien de la base de données centrale conformément aux paragraphes 5(1)-(2) du Règlement.

En vertu du paragraphe 21(1) du Règlement, les diplomates sont exemptés de la prise de leurs empreintes digitales ou de leurs renseignements biométriques. Seuls les documents d'identité professionnelle et diplomatique sont nécessaires pour enregistrer leurs cartes SIM. Au Lesotho, le processus d'enregistrement de la carte SIM a commencé le 24 juin 2022.<sup>196</sup> Bien que le Règlement ne mentionne pas les photos comme exigence pour le processus d'inscription, lors de l'inscription, des photos faciales sont prises.

Le gouvernement du Libéria, par l'intermédiaire de l'Autorité des télécommunications du Libéria, a imposé l'enregistrement obligatoire des utilisateurs de cartes SIM prépayées qui doivent présenter une pièce d'identité, un passeport et une photo valides ou enregistrer leurs données biométriques avant l'activation de la carte SIM. Les utilisateurs existants qui ne sont pas en mesure d'enregistrer leurs cartes SIM dans certains délais sont bloqués ou déconnectés de divers réseaux GSM.

Suite aux émeutes de la faim qui ont eu lieu à Maputo en 2010 et que nous avons principalement coordonnées par SMS, le gouvernement a décidé d'introduire l'enregistrement des cartes SIM. Initialement, les opérateurs de téléphonie mobile disposaient d'un délai de trois mois pour achever le processus d'enregistrement, qui a ensuite été prolongé jusqu'en 2011. En 2012, seulement environ la moitié des cartes SIM utilisées avaient été enregistrées. En 2015, le gouvernement a fixé une nouvelle date limite et finalement en 2016, un million de lignes ont été désactivées pour non-enregistrement. Les abonnés doivent présenter un passeport ou une carte d'identité nationale pour enregistrer une carte SIM.<sup>197</sup>

En décembre 2020, le gouvernement fédéral nigérian a ordonné à tous les citoyens et personnes résidant légalement au Nigéria de lier leur numéro d'identification national (NIN) à leur carte SIM, avec une menace de déconnexion des cartes SIM non liées. En 2011, la Commission nigériane de la communication (NCC) a budgétisé 6,1 milliards de nairas (141,6 millions USD) pour procéder à l'enregistrement biométrique des cartes SIM dans les six zones géopolitiques du pays en plus de Lagos. Le régulateur exige des opérateurs de télécommunications qu'ils enregistrent les cartes SIM de leurs abonnés dans le but de réduire l'insécurité et la criminalité. La CCN a officiellement annoncé que l'enregistrement des anciennes cartes SIM avait pris fin le 30 juin 2013.

En date du 4 avril 2022, la CCN a annoncé que plus de 125 millions de propriétaires de cartes SIM avaient soumis leur NIN pour qu'ils soient liés, vérifiés et authentifiés. La CCN a déclaré que les appels des abonnés qui n'avaient pas respecté la directive sur le couplage NIN-SIM seraient interdits. La partie 2 du règlement de 2011 de la Commission nigériane des communications (enregistrement des abonnés au service téléphonique) établit l'obligation de maintenir et d'exploiter une base de données centrale domiciliée au sein de la NCC pour le traitement central et le stockage des informations des abonnés. En outre, l'article 8 du Règlement donne accès aux informations sur les abonnés dans la base de données centrale par les organismes de sécurité. Toutefois, il exige qu'une demande écrite préalable précisant l'objet de la demande soit adressée au NCC par « un fonctionnaire de l'organisme de sécurité demandeur qui n'a pas le grade inférieur à celui de commissaire adjoint de police ou un grade correspondant dans tout autre organisme de sécurité ».

<sup>196</sup> L'inscription SIM reprend en juin <https://www.gov.ls/sim-registration-resumes-in-june/>

<sup>197</sup> Mozambique <https://prepaid-data-sim-card.fandom.com/wiki/Mozambique>

En août 2007, le Sénégal a pris le décret 2007-937 du 7 août 2007 qui impose aux opérateurs de réseaux publics de télécommunications d'enregistrer tous les acheteurs et utilisateurs de cartes SIM. En 2013, sous prétexte de lutter contre la criminalité liée à l'utilisation de la téléphonie mobile, l'Autorité sénégalaise de régulation des télécommunications et des postes (ARTP) a relancé l'exercice d'enregistrement de la carte SIM. Les informations requises pour l'inscription comprennent un nom de famille, un prénom et un numéro CNI (ID). Les données d'enregistrement de la carte SIM sont liées à la base de données nationale d'identité.<sup>198</sup>

L'article 3 du Règlement de 2020 sur la gestion de l'identification et de l'enregistrement des abonnés des télécommunications de la Sierra Leone exige que les fournisseurs de services de communication agréés obtiennent, enregistrent et stockent les informations des abonnés.<sup>199</sup> Les données d'enregistrement requises du client comprennent une photo de format passeport, représentant clairement l'image faciale du client et/ou des informations biométriques ou une copie d'un document d'identification valide. Le règlement définit les renseignements biométriques comme étant les « empreintes digitales et l'image faciale » d'un abonné. Les autres données d'enregistrement requises conformément aux spécifications d'enregistrement fournies par l'organisme de réglementation comprennent les noms, la date de naissance et le sexe des abonnés.

En Tanzanie, l'enregistrement de la carte SIM est effectué biométriquement par les entreprises de télécommunications qui exigent que les individus aient une carte d'identité émise par le NIDA ou NIN. Conformément au règlement de 2020 sur les communications électroniques et postales (enregistrement des cartes SIM), toutes les cartes SIM doivent être enregistrées biométriquement ou être déconnectées. Les entreprises de télécommunications sont liées à la base de données NIDA et peuvent accéder aux données des individus dans une mesure non divulguée au public. Pour l'enregistrement de la carte SIM, les entreprises de télécommunications collectent les empreintes digitales et les signatures numériques des individus, tout en accédant à leurs autres informations personnelles via la base de données de NIDA. La Tanzanie a d'abord rendu obligatoire l'enregistrement de la carte SIM par le biais de la Loi de 2010 sur les communications électroniques et postales (EPOCA), dont l'article 93 dispose que « toute personne qui possède ou a l'intention d'utiliser une carte SIM détachable ou une carte SIM intégrée sera tenue d'enregistrer une carte SIM ou un téléphone mobile avec carte SIM intégrée ».

L'enregistrement des cartes SIM a été rendu obligatoire en Ouganda en 2012 à la suite d'une campagne menée par le régulateur des communications, arguant que l'exercice était nécessaire pour lutter contre la criminalité en permettant le suivi des criminels et l'identification des propriétaires de cartes SIM.<sup>200</sup> Les abonnés sont tenus de présenter leur carte d'identité nationale pour enregistrer leurs cartes SIM. En outre, les opérateurs de télécommunications ont accès à une interface de programmation d'application (API) fournie par l'Autorité nationale d'enregistrement d'identité (NIRA) pour vérifier et valider les enregistrements de carte SIM sur les informations. La carte d'identité est vérifiée par un processus d'authentification en deux étapes au moyen d'un lecteur de carte biométrique électronique et la soumission d'informations biographiques à la NIRA et d'une photographie claire.

L'opérateur doit vérifier les détails de la carte d'identité nationale à l'aide d'un lecteur de carte biométrique électronique, faire correspondre les données biométriques en direct du demandeur avec les données biométriques sur la carte et obtenir une vérification en temps réel avec la base de données NIRA via l'API.

<sup>198</sup> Décret 2007-937 du 7 août 2007 [http://www.osiris.sn//IMG/pdf/document\\_Decret\\_relatif\\_a\\_lidentification\\_des\\_abonnes\\_153.pdf](http://www.osiris.sn//IMG/pdf/document_Decret_relatif_a_lidentification_des_abonnes_153.pdf)

<sup>199</sup> Règlement de 2020 sur la gestion de l'identification et de l'enregistrement des abonnés aux télécommunications

<https://www.natcom.gov.sl/wp-content/uploads/2021/02/The-Telecommunications-Subscribers-Identification-and-Registration-Management-Regulations-2020.pdf>

<sup>200</sup> Cartographie et analyse des lois sur la protection de la vie privée en Afrique, [https://cipesa.org/?wpfb\\_dl=479](https://cipesa.org/?wpfb_dl=479)

## 2.2.7 Collecte de données biométriques par des entreprises étrangères

De nombreuses missions étrangères basées dans les pays examinés recueillent également des données personnelles sur les personnes qui cherchent à se rendre dans leur pays. Les principaux types d'informations collectées par voie électronique par les États-Unis,<sup>201</sup> le Canada,<sup>202</sup> l'Union européenne<sup>203</sup> et le Royaume-Uni<sup>204</sup> comprennent les données biographiques (nom, date de naissance, nationalité, lieu de naissance et autres détails personnels sur la page de données biographiques du passeport du demandeur), les empreintes digitales, les empreintes palmaires, l'écriture manuscrite ou les signatures, et les images faciales.

## 2.3 Collecte et traitement des données biométriques des mineurs

Les principaux domaines dans lesquels les données sur les mineurs ont été collectées concernaient l'enregistrement des faits d'état civil, notamment la délivrance des certificats de naissance, des cartes d'identité nationales, des passeports électroniques, de l'immigration, des services de santé et de l'enregistrement des cartes SIM. Dans les juridictions de la CEMAC, les personnes âgées de plus de 16 ans peuvent se voir délivrer un permis de conduire de catégorie A ou A1.<sup>205</sup> La carte d'identité nationale numérique de la Zambie sera délivrée aux personnes âgées de plus de 16 ans.<sup>206</sup> La carte d'identité numérique Huduma Namba du Kenya capture les données biométriques des enfants de plus de six ans.<sup>207</sup> Dans la plupart des pays, les cartes SIM utilisées par les mineurs sont enregistrées soit à leur nom, comme en Tanzanie, soit à celui de leurs parents ou tuteurs dans d'autres juridictions.

Les missions étrangères telles que la Belgique recueillent les données biographiques des enfants de plus de 12 ans.<sup>208</sup> Selon VFS Global, les demandeurs de visa Schengen et britannique ne sont exemptés de la collecte d'empreintes digitales que s'ils ont moins de cinq ans, bien que leurs photographies numériques soient prises.<sup>209</sup> En outre, les enfants de moins de 14 ans qui demandent des visas américains et canadiens sont exemptés de l'obligation de fournir des données biométriques.<sup>210</sup> Tous les pays n'ont pas de dispositions aussi explicites dans leurs lois, politiques ou pratiques visant à protéger la vie privée des enfants, en particulier contre la collecte de leurs données biométriques.

<sup>201</sup> Sûreté et sécurité des frontières américaines : biométrie

<https://travel.state.gov/content/travel/en/us-visas/visa-information-resources/border-biometrics.html#:~:text=For%20U.S.%20Visas%20the%20chosen,officer's%20interview%20with%20the%20applicant>

<sup>202</sup> Quelles données biométriques sont recueillies et qui doit fournir leurs données biométriques

<https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/identity-management/biometrics/what.html>

<sup>203</sup> Que se passe-t-il au Centre de réception des demandes de visa ?

<https://visa.vfsglobal.com/sau/en/che/attend-centre/what-happens-at-centre>

<sup>204</sup> Inscription biométrique : orientations politiques

[https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/1091802/Biometric\\_information\\_-\\_enrolment.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091802/Biometric_information_-_enrolment.pdf)

<sup>205</sup> Règlement No 04/01-UEAC-089-CM-06 <http://www.droit-afrique.com/upload/doc/cemac/CEMAC-Règlement-2001-04-Code-de-la-route.pdf>

<sup>206</sup> La Zambie met en œuvre un système d'enregistrement d'identité biométrique <https://itweb.africa/content/nWJadMbeW5r7bjO1>

<sup>207</sup> Des enfants de six ans à obtenir ID dans Huduma plan <https://nation.africa/kenya/news/six-year-olds-to-get-ids-in-huduma-plan-2303574>

<sup>208</sup> Biométrie <https://www.cev-kin.eu/en/general-information/biometrics>

<sup>209</sup> Que se passe-t-il au Centre de réception des demandes de visa ? <https://visa.vfsglobal.com/jor/fr/cze/attend-centre/what-happens-at-centre>

<sup>210</sup> Sûreté et sécurité des frontières américaines : biométrie <https://travel.state.gov/content/travel/en/us-visas/other-visa-categories/safety.html>; Photos et empreintes digitales <https://www.ustraveldocs.com/ci/ci-niv-photoinfo.asp#:~:text=There%20are%20some%20applicants%20whose,over%20the%20age%20of%2079;Quelles%20donn%C3%A9es%20biom%C3%A9triques%20sont%20recueillies%20et%20qui%20doit%20fournir%20leurs%20donn%C3%A9es%20biom%C3%A9triques>

<https://www.canada.ca/en/immigration-refugees-citizenship/corporate/publications-manuals/operational-bulletins-manuals/identity-management/biometrics/what.html>

## 2.4 Justifications du traitement des données biométriques

En introduisant plusieurs programmes de collecte de données biométriques, les pays ont avancé diverses justifications, notamment la promotion de la sécurité nationale, de la stabilité et de la gestion efficace des informations d'identité. Parmi les autres raisons invoquées, citons le renforcement des efforts de transformation numérique d'un pays, l'élimination du vol d'identité, de la fraude et de la contrefaçon de documents officiels, l'amélioration du recouvrement des impôts, la facilitation des mouvements et du contrôle des frontières, la lutte contre la corruption et l'amélioration de la prestation de services.

Au Cameroun, l'objectif était de développer une base de données centralisée sur la population, d'améliorer la transparence, d'assurer la sécurité nationale, une identification fiable et une gestion des frontières, de lutter contre la contrefaçon de documents, de remédier aux irrégularités dans les systèmes papier et d'assurer l'alignement sur les normes internationales relatives aux passeports électroniques.<sup>211</sup> En République centrafricaine, la collecte des empreintes digitales lors de l'inscription des électeurs visait à renforcer la sécurité, à éliminer la fraude électorale et à améliorer l'identification. Lors de l'introduction du passeport biométrique, il a été déclaré qu'il garantirait le respect des normes internationales.

En République démocratique du Congo, l'installation de caméras de vidéosurveillance publiques à Kinshasa en 2016 visait à renforcer la sécurité de la ville et à promouvoir la discipline routière. Le passeport électronique a également été promu comme faisant partie des efforts déployés par l'État pour se conformer aux normes et exigences internationales au sein de la CAE et pour accroître l'efficacité. Les cartes d'identité biométriques et l'enregistrement des cartes SIM visent prétendument à lutter contre la criminalité, à réduire le vol d'identité et à améliorer l'identification.

Au Kenya, l'introduction de la Huduma Namba visait à disposer d'une base de données centrale « source unique de vérité » sur l'identité de tous les résidents, à améliorer la prestation de services, à améliorer l'identification des individus et la vérification de l'identité par les acteurs étatiques et non étatiques, et à lutter contre la fraude et la criminalité. En outre, il visait à réduire le coût du recensement de la population, à élargir l'assiette fiscale, à améliorer l'inscription des électeurs, à faciliter la délivrance des permis de conduire et à éliminer les doublons de documents d'identité requis pour accéder aux services gouvernementaux.<sup>212</sup> Le passeport électronique a été adopté dans le cadre de la conformité à la directive de l'EAC et pour améliorer le passeport de l'ancienne génération, améliorer l'efficacité aux points frontaliers, améliorer la sécurité du document et éviter sa duplication.

Au Lesotho, les principales raisons invoquées sont la lutte contre l'usurpation d'identité, l'aide aux enquêtes et à la prévention de la cybercriminalité, et la promotion de la prestation de services au moyen d'un document d'identité unique. Au Libéria, le programme d'identité numérique est mis en œuvre pour améliorer la gestion des ressources humaines au sein du gouvernement, réduire le coût de l'inscription sur les listes électorales et du recensement, améliorer le contrôle des frontières et la gestion électorale, l'accès aux services financiers, la fiabilité des documents de voyage, la collecte des impôts, l'accès aux filets de sécurité sociale et aux soins de santé universels, harmoniser les programmes d'identité entre les agences gouvernementales et dans la région de la CEDEAO.

Au Mozambique, des programmes d'identité ont été promus pour renforcer l'ordre public et la sécurité, créer une base de données d'information, faciliter les services publics et améliorer les communications. Au Nigéria, les principales justifications comprennent la promotion de la sécurité nationale par la lutte contre l'insécurité et la réduction de la criminalité; la création d'une base de données nationale sur l'identité de la population; améliorer l'identification des résidents avec des données précises; assurer une planification nationale stratégique; et améliorer la prestation de services et la collecte des impôts.

<sup>211</sup> 10 Questions à moins de défendre la refonte biométrique des listes électorales au Cameroun

<https://www.camerlex.com/10-questions-pour-comprendre-la-refonte-Biometrique-des-Listes-Electorales-au-Cameroun-12559/>

<sup>212</sup> Avantages <https://www.hudumanamba.go.ke/benefits/>

Au Libéria, l'augmentation des investissements dans la technologie devrait permettre de lutter contre la corruption dans l'administration publique et le système judiciaire.<sup>213</sup> En outre, l'identification numérique est utilisée pour faciliter l'accès aux services financiers et d'assurance et à signaler la corruption. Comme au Sénégal, la carte d'identité nationale biométrique, le permis de conduire et les cartes d'électeur visent à prévenir le vol d'identité et la fraude électorale; à promouvoir l'accès aux services; à réduire les accidents de la route; à se conformer aux normes et directives régionales de la CEDEAO; et à améliorer l'efficacité en éliminant la duplication des enregistrements.<sup>214</sup> Le système de vidéosurveillance proposé vise à améliorer la sécurité nationale.

Pour la Sierra Leone, l'introduction des cartes d'identité nationales et de la CEDEAO à usages multiples devait faciliter les transactions personnelles, les mouvements et l'identification des personnes.<sup>215</sup> Il était également prévu de lutter contre la fraude mobile, d'améliorer la prestation de services, de lutter contre la criminalité grâce à une meilleure information et de réduire le coût des processus de collecte de données trompeurs pour les élections et l'enregistrement des faits d'état civil.

En Tanzanie, les justifications de l'introduction de l'identification biométrique comprennent la modernisation des processus et de la gestion des dossiers sur papier vers les systèmes numériques; le renforcement de la sécurité nationale et la prévention de la criminalité; l'amélioration du bien-être social; la stimulation du développement économique; l'amélioration de l'accès aux services sociaux; la fourniture de données précises sur les résidents; l'amélioration de l'efficacité du service délivrée et l'amélioration de l'identification des résidents grâce à la délivrance de documents.

L'introduction du programme d'identification électronique du Togo s'inscrivait dans la promesse du gouvernement de numériser les services publics, de disposer d'une base de données centrale contenant des informations précises sur la population, de faciliter les processus administratifs, de faciliter le partage d'informations entre les agences et d'améliorer la planification future.<sup>216</sup> Ce faisant, il devrait faciliter l'accès au crédit, améliorer l'accès aux services de santé, prévenir la criminalité en disposant d'informations permettant d'identifier les criminels, réduire la fraude dans le secteur bancaire, assurer la distribution ciblée des services sociaux et publics et améliorer le suivi éducatif et administratif des citoyens.<sup>217</sup>

En Tunisie, les principales justifications de l'introduction de la vidéosurveillance étaient la promotion de la sécurité nationale et la lutte contre le terrorisme. Les passeports électroniques et les cartes biométriques nationales ont été déployés dans le cadre de la conformité aux normes internationales afin d'assurer la sécurité, l'intégrité et l'interopérabilité des documents de voyage. En outre, les programmes biométriques ont été mentionnés dans le cadre des efforts de modernisation visant à numériser les services administratifs afin d'améliorer la prestation de services, d'améliorer l'identification des résidents et de faciliter le partage d'informations.

Le lancement du passeport électronique ougandais devait contribuer à réduire la fraude, la falsification de documents et le vol d'identité en améliorant la confidentialité des renseignements du titulaire.<sup>218</sup> Le document devait également faciliter le traitement des entrées et des sorties à tous les postes frontaliers et renforcer l'intégrité du passeport de l'entreprise dans le monde entier. Parmi les autres justifications de l'introduction de systèmes biométriques figurent la promotion de la sécurité nationale et la lutte contre des crimes tels que la fraude, l'amélioration de l'efficacité de l'enregistrement et de l'exactitude de l'identification des résidents, la promotion du développement économique et technologique, l'amélioration de la prestation de services et de l'accès aux services gouvernementaux, la prévention de la fraude électorale, la réduction du coût de l'inscription, la facilitation de la planification nationale, la lutte contre la corruption et l'amélioration de la gestion des dossiers.

<sup>213</sup> L'augmentation des investissements dans la technologie peut réduire la corruption au Libéria

<https://frontpageafricaonline.com/news/tech/increased-investment-in-technology-can-reduce-corruption-in-liberia/>

<sup>214</sup> Les avantages de la carte d'identité biométrique de la CEDEAO partagée en Kaolack <http://www.osiris.sn/Les-avantages-de-la-carte-d.html>

<sup>215</sup> Confirmation et enregistrement des citoyens et des non-citoyens en Sierra Leone vont bientôt commencer

<https://www.thesierraleonetelgraph.com/confirmation-and-registration-des-citoyens-et-des-non-citoyens-en-sierra-leone-vont-commencer-bientot/>

<sup>216</sup> Le Togo est sur le point d'initier l'identification biométrique pour tous ses résidents

<https://www.m2sys.com/blog/e-governance/togo-initiate-biometric-id/>

<sup>217</sup> Le Togo espère lancer une nouvelle carte d'identité biométrique en 2021 <https://www.biometricupdate.com/202012/togo-hopes-to-launch-new-biometric-id-card-in-2021>

<sup>218</sup> Comment le passeport électronique facilitera les voyages Pour Ougandais <https://caa.go.ug/how-e-passport-will-ease-travel-for-ugandans/>

Lors du lancement du passeport électronique du pays, l'ancien président tanzanien John Pombe Magufuli (RIP) a salué le projet comme essentiel pour renforcer la sécurité nationale, contrôler les immigrants illégaux, améliorer la collecte des recettes, améliorer la productivité et simplifier la prestation de services.<sup>219</sup> En Zambie, l'introduction de la carte d'identité numérique biométrique devrait permettre de relever les défis du système papier vieux de plusieurs décennies, tels que la duplication des cartes d'identité, la fraude à l'identité, les difficultés dans les opérations de connaissance du client (KYC) et la perte de revenus pour les acteurs étatiques et non étatiques.<sup>220</sup> En outre, le système devrait améliorer la prestation de services, réduire la fraude électorale, éliminer les travailleurs fantômes et renforcer la sécurité nationale du pays, l'identification des résidents et les opérations KYC. En outre, le système devrait permettre de réaliser des économies dans les programmes de transferts sociaux en espèces et d'améliorer le respect des règles en matière de recouvrement des impôts nationaux et d'assurance maladie, tout en augmentant les recettes annuelles provenant des frais d'authentification et de vérification des institutions financières et des opérateurs de réseaux mobiles jusqu'à 410 millions USD.<sup>221</sup>

<sup>219</sup> La Tanzanie lance le passeport électronique comme Magufuli appelle à un contrôle plus strict des immigrants illégaux

<https://www.thecitizen.co.tz/tanzania/news/national/tanzania-launches-e-passport-as-magufuli-calls-for-tighter-control-of-illegal-immigrants-2621606#:~:text=President%20John%20Magufuli%20has%20on,key%20role%20in%20revenue%20collection>.

<sup>220</sup> Identification biométrique des citoyens pour améliorer l'inscription et l'identification des électeurs en Zambie

<https://www.biometricupdate.com/202004/biometric-citizen-identification-to-enhance-voter-registration-and-identification-in-zambia>

<sup>221</sup> Ibid.; Le gouvernement entame la mise en œuvre de la voiture d'immatriculation nationale biométrique

<https://www.lusakatimes.com/2022/03/15/government-begins-implementation-of-the-biometric-enabled-national-reCartes-de-gistraton/>; Mutati souligne le besoin d'identifications électroniques <https://diggers.news/local/2022/02/25/mutati-highlights-need-for-electronic-ids/>



3.0

# Discussion: tendances, risques potentiels, défis et lacunes

## 3.1 Campagnes limitées de mobilisation et de sensibilisation du public

Alors que la collecte de données biométriques a un impact prépondérant sur la vie privée, dans de nombreux pays, il y a eu un manque évident de sensibilisation, d'engagement et de consultations du public parmi les principales parties prenantes et le grand public sur les objectifs, les utilisations, la conception et la mise en œuvre des programmes de collecte de données biométriques. Dans les pays où des campagnes publiques ont été menées, les principes de protection des données, les droits des personnes concernées et les possibilités d'abus de données ont rarement été mis en avant malgré le faible niveau de sensibilisation des personnes concernées à la vie privée. Les gouvernements semblent avoir été pressés de lancer des programmes de collecte de données biométriques et de célébrer les numéros d'enregistrement plutôt que de donner la priorité aux consultations et à l'engagement du public qui sont essentiels à la réussite de ces projets.

Il a également été établi que dans de nombreux pays étudiés tels que l'Angola, le Libéria, le Nigéria, le Mozambique, la Tanzanie et la Zambie, la participation du public était minime ou limitée aux questions relatives aux programmes de collecte de données à caractère personnel, à leurs intentions et aux risques qui en découlent. En conséquence, et compte tenu de l'asymétrie de pouvoir entre les États et les personnes concernées, le public fournit des données biométriques sans question ni consentement préalables éclairés, mais par nécessité afin d'acquiescer des services critiques ou des documents officiels tels que des laissez-passer, des cartes d'identité nationales, des cartes d'électeur ou des permis de conduire.

Lorsqu'il y a eu des campagnes publiques, celles-ci ont été menées sur de courtes périodes et de manière sporadique, souvent avec des informations limitées et trompeuses sur les technologies et l'objectif des programmes, des directives coercitives pour assurer le respect sans poser de questions, et de nature obligatoire sans prévoir d'alternatives à l'enregistrement et à l'enrôlement. Par exemple, au Cameroun, les campagnes publiques d'Elections au Cameroun (ELECAM) et de l'Observatoire national de la jeunesse ont consisté à encourager les gens à s'inscrire biométriquement pour les élections et à obtenir respectivement la carte biométrique des jeunes. De même, au Kenya, les campagnes publiques menées par le ministère de l'Intérieur et la Commission électorale indépendante et des frontières (IEBC) se sont concentrées sur la contrainte des personnes à s'inscrire à la Huduma Namba avant le 25 mai 2019<sup>222</sup> et à s'inscrire comme électeurs avant le 4 mai 2022.<sup>223</sup> En Ouganda, les campagnes publiques qui ont précédé l'introduction de la carte d'identité nationale se sont concentrées sur l'inscription sans engagement similaire sur les mérites de la carte d'identité biométrique.

Au Sénégal, une campagne publique organisée du 9 au 21 novembre 2019 par la Direction générale des élections au Sénégal (DGE) visait à encourager et à mobiliser les citoyens à s'inscrire pour obtenir les cartes d'identité biométriques de la CEDEAO.<sup>224</sup> En Sierra Leone, l'Autorité nationale d'enregistrement des faits d'état civil (NCRA) et la Commission électorale nationale (NEC) ont mené des campagnes nationales pour que le public participe au système biométrique d'état civil et d'inscription des électeurs avant les élections de mars 2018, ce qui a permis d'inscrire 3,5 millions de citoyens avec la technologie de Smartmatic.<sup>225</sup>

<sup>222</sup> Président Uhuru étend la date limite d'inscription Huduma Namba

<https://www.standardmedia.co.ke/nairobi/article/2001325962/uhuru-extends-huduma-namba-registration-deadline#:~:text=President%20Uhuru%20Kenya%20at%20a,will%20end%20on%20June%206.>

<sup>223</sup> L'IEBC suspend l'exercice d'inscription des électeurs Sur Mercredi <https://www.capitalfm.co.ke/news/2022/05/iebc-to-suspend-voter-registration-exercise-on-wednesday/>

<sup>224</sup> Réunion de coordination - campagne de sensibilisation sur cartes November 6, 2019 <http://dgc.sn/fr/node/330>

<sup>225</sup> Inscription à l'état civil et sur les listes électorales - Sierra Leone 2017 [https://www.smartmatic.com/fileadmin/user\\_upload/CS\\_Sierra\\_Leone.pdf](https://www.smartmatic.com/fileadmin/user_upload/CS_Sierra_Leone.pdf)

Au Togo, l'Autorité de régulation des communications électroniques et des postes (ARCEP) et le ministère de l'Economie numérique ont mené une campagne nationale d'enregistrement des cartes SIM.<sup>226</sup> En 2021, l'Agence nationale d'identification du Togo (ANID) a mené une campagne pour mobiliser les gens à s'inscrire au projet national d'identification biométrique du pays, e-ID Togo, qui devrait fournir un numéro d'identification unique à tous les résidents.<sup>227</sup> De même, au Lesotho, les campagnes étaient principalement axées sur le processus sans fournir de détails sur les implications sur le droit des personnes à la vie privée.

Des acteurs non étatiques tels que les entreprises de télécommunications ont également effectué le traitement de données biométriques avec une participation limitée du public. Cela a été observé en République centrafricaine et en RDC, où ces entreprises ne notifiaient à leurs clients que l'obligation d'enregistrement de la carte SIM sans fournir de détails sur l'étendue des données à collecter. Par exemple, en RDC, Vodacom RDC a publié en 2016 un message sur Facebook demandant à ses abonnés de télécharger et de remplir un formulaire d'enregistrement de carte SIM et d'envoyer le formulaire avec leur carte d'identité nationale à l'adresse e-mail de l'opérateur.<sup>228</sup>

L'incapacité de certains gouvernements à faire preuve de transparence et de responsabilité en divulguant de manière proactive des informations sur les programmes ne fait qu'alimenter la suspicion, la spéculation et le scepticisme du public quant aux intentions du gouvernement, aussi nobles soient-elles. De nombreux programmes biométriques relèvent des ministères de l'Intérieur et sont souvent classés comme des projets de « sécurité nationale », ce qui ajoute un épais nuage de secret autour de leur conception, de leur approvisionnement, de leur coût et de leur mise en œuvre. Il y a un mécontentement dans des pays comme le Nigeria, le Kenya et l'Ouganda au sujet des investissements dans des régimes d'enregistrement biométrique bureaucratiques coûteux et multiples introduits au cours des trois à cinq dernières années. Les programmes recherchent des informations identiques ou similaires et exigent que le public soit physiquement présent, fasse la queue pendant des heures, parcoure de longues distances et enregistre ses données biométriques.

Cependant, la société civile, au Kenya, au Sénégal, en Sierra Leone, en Tunisie, en Ouganda et en Zambie, s'est opposée à l'introduction de programmes de collecte biométrique en l'absence de cadres politiques, législatifs et institutionnels complets. Au Sénégal, par exemple, la société civile a critiqué le permis de conduire biométrique comme étant illégal, coûteux, excessif, intrusif et dangereux,<sup>229</sup> tandis que l'enregistrement obligatoire de la carte SIM a été critiqué pour son non-respect de la loi sur la protection des données et de la réglementation de la Commission des données personnelles (CDP).<sup>230</sup> En Sierra Leone, des militants se sont opposés à des modifications législatives visant à faire de l'identité numérique une exigence pour voter aux élections de 2023. Au Kenya, le projet d'identification numérique obligatoire Huduma Namba, dirigé par le gouvernement, a été contesté devant les tribunaux en 2019 pour ingérence dans le droit constitutionnel à la vie privée, absence de loi sur la protection des données et incitation du gouvernement à mener une analyse d'impact sur la protection des données.<sup>231</sup>

En juin 2017, la Commission ougandaise des communications (UCC) a ordonné aux opérateurs de télécommunications d'utiliser les numéros d'identification nationaux (NIN) des abonnés pour vérifier les cartes SIM. Cette décision a été condamnée par la société civile car le pays n'avait pas encore adopté de loi sur la protection de la vie privée et des données qui aurait guidé le processus de collecte et de partage des données.<sup>232</sup>

<sup>226</sup> L'arrêté limitant le nombre de cartes SIM expliqué par l'ARCEP, Togo Cellulaire et Moov Afrique Togo

<https://arcep.tg/larrete-portant-limitation-du-nombre-de-cartes-sim-explique-par-larcep-togo-cellulaire-et-moov-afrique-togo/>

<sup>227</sup> Le gouvernement prépare une campagne de communication pour le projet e-ID Togo

<https://www.togofirst.com/en/public-management/0106-7945-government-prepares-communication-campaign-for-e-id-togo-project>

<sup>228</sup> Vodacom RDC

[https://web.facebook.com/VodacomRDC/posts/bonjour-chers-fanscliquez-sur-ce-lien-httpsdrivegooglecomfiled0b4fqidasrlpiy2llx/903542726420149/?\\_rdc=1&\\_rdr](https://web.facebook.com/VodacomRDC/posts/bonjour-chers-fanscliquez-sur-ce-lien-httpsdrivegooglecomfiled0b4fqidasrlpiy2llx/903542726420149/?_rdc=1&_rdr)

<sup>229</sup> Le permis de conduire biométrique : un projet illégal, coûteux, excessif, intrusif et dangereux <http://www.osiris.sn/Permis-de-conduire-biometrique-Un.html>; Asutique: « Le permis de conduire biométrique est dangereux et illégal » [https://senego.com/asutic-le-permis-de-conduire-biometrique-est-dangereux-et-illegal\\_1010014.html](https://senego.com/asutic-le-permis-de-conduire-biometrique-est-dangereux-et-illegal_1010014.html)

<sup>230</sup> Avis trimestriel N° 01-2021 de la Commission de Protection des Données Personnelles du Sénégal (CDP)

<https://www.cdp.sn/content/avis-trimestriel-n%C2%B0-01-2021-de-la-commission-de-protection-des-donnees-personnelles-du-0>; [https://cipesa.org/?wpfb\\_dl=291](https://cipesa.org/?wpfb_dl=291)

<sup>231</sup> Nubian Rights Forum & 2 autres c. Attorney General & 6 autres; Société de protection de l'enfance & 9 autres (Parties intéressées) [2020] eKLR

<http://kenyalaw.org/kenyalaw/cases/view/189189/>

<sup>232</sup> Un témoin indésirable condamne l'utilisation criminelle des données biographiques des citoyens et appelle le gouvernement à formuler des mesures de protection pour protéger les vies et les biens.

<https://www.unwantedwitness.org/unwanted-witness-condemns-the-criminal-use-of-citizens-bio-data-calls-on-govt-to-formulate-safeguards-to-protect-lives-and-property/>

## 3.2 Cadres juridiques inadéquats augmentant les risques pour la vie privée

L'un des principaux risques pour la vie privée est la mise en œuvre de programmes de biométrie numérique en l'absence de cadres politiques, juridiques et institutionnels adéquats ou complets pour la protection de la vie privée et des données. Cela inclut des mécanismes visant à mettre en œuvre les principes de protection des données, tels que la minimisation des données et le consentement, qui sont viciés par le caractère obligatoire des programmes. Par exemple, ces cadres sont absents au Cameroun, en République centrafricaine, en République démocratique du Congo, au Libéria, au Nigéria, en Sierra Leone et en Tanzanie. Dans les pays où les lois sont présentes, dans certains cas, elles sont faibles, fragmentées, dépassées, mal appliquées et ne prévoient pas de mécanismes de surveillance solides et indépendants pour la protection de la confidentialité des données ou des recours efficaces, mais les gouvernements ont intensifié le déploiement de technologies de collecte de données telles que la vidéosurveillance avec la technologie de reconnaissance faciale automatisée.

De nombreux gouvernements n'ont pas mis en place de procédures ou de garanties appropriées pour le partage des données entre les institutions de l'État. En Tanzanie, les accords de partage de données entre le NIDA et d'autres agences ne sont pas divulgués au public. Au Sénégal, la centralisation des bases de données et le manque d'informations sur les niveaux d'accès à ces bases alimentent également les craintes d'abus des données. De même, au Sénégal, le manque de transparence autour de la carte biométrique unifiée utilisée comme carte d'identité nationale et carte d'électeur a alimenté les spéculations sur d'éventuels abus de la part des politiciens pour cibler les électeurs dans des zones spécifiques.

Dans la plupart des pays où l'enregistrement de la carte SIM est systématique, on craint que les fournisseurs de services ne soient contraints, en vertu des lois existantes sur l'interception des communications, de faciliter les activités de surveillance de l'État en fournissant des informations sur les abonnés aux agents de la sécurité de l'État. Cela a été observé au Togo où, en l'absence d'une loi sur la protection de la vie privée, trois journalistes, Komlanvi Ketohou, Ferdinand Ayité et Luc Abaki, figuraient sur une liste de 300 personnes potentiellement ciblées pour la surveillance via leurs téléphones par des clients de la société israélienne NSO Group utilisant le logiciel espion Pegasus.<sup>233</sup> Des pays comme le Maroc, le Mozambique, le Rwanda et la Zambie ont été signalés comme utilisant Pegasus, tandis que ses infections ont été signalées en Algérie, en Côte d'Ivoire, en Égypte, au Libéria, en Ouganda et en Afrique du Sud.<sup>234</sup>

En Tunisie, la loi sur la protection des données, vieille de plusieurs décennies, est obsolète et n'a pas encore été mise à jour pour refléter les tendances mondiales actuelles et les développements en matière de confidentialité des données. D'une manière générale, l'absence de cadres réglementaires clairs et solides dans les pays ouvre la voie à l'abus des droits des personnes concernées.

La majorité des pays étudiés n'ont pas ratifié la Convention de Malabo de l'Union africaine de 2014, qui vise à guider les États membres dans l'élaboration d'un régime juridique harmonisé en matière de protection des données. Seuls 14 pays sont signataires et 13 ont ratifié l'Accord sur 55 États membres, à savoir l'Angola, le Cap-Vert, le Congo, le Ghana, la Guinée, le Mozambique, l'île Maurice, la Namibie, le Niger, le Rwanda, le Sénégal, le Togo et la Zambie.<sup>235</sup>

<sup>233</sup> « Il y a pas de vie privée » : trois journalistes togolais réagissent à leur sélection pour la surveillance par logiciel espion  
<https://cpj.org/2021/09/togolese-journalists-spyware-surveillance/>

<sup>234</sup> Comment les outils d'espionnage numérique exacerbent l'autoritarisme en Afrique  
<https://www.brookings.edu/techstream/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/>

<sup>235</sup> Liste des pays qui ont signé, ratifié ou adhéré à l'Union africaine convention sur la cybersécurité et la protection des données personnelles,  
[https://au.int/sites/default/files/treaties/29560-sl-AFRICAN\\_UNION\\_CONVENTION\\_ON\\_CYBER\\_SECURITY\\_AND\\_PERSONAL\\_DATA\\_PROTECTION.pdf](https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf)

Cela implique que l'Afrique n'a pas encore adopté d'approche réglementaire commune pour accélérer la protection de la vie privée et adopter une compréhension générale de la manière de faire face aux menaces émergentes à la vie privée à l'ère du numérique. Certains des avantages des approches communes, comme l'élaboration d'outils, de politiques et de lignes directrices pertinents à l'échelle locale; un contenu de formation unifié et des programmes de renforcement des capacités; et le transfert de technologie et de compétences, qui ont profité à des juridictions comme l'Union européenne, pourraient également être appréciés en Afrique.<sup>236</sup> Le besoin persistant de programmes de données biométriques en Afrique doit être complété par des cadres politiques, réglementaires et institutionnels appropriés pour protéger la vie privée des personnes concernées et protéger leurs données biométriques.

Au Cameroun, en République centrafricaine, en République démocratique du Congo, au Libéria, au Nigéria, en Sierra Leone et en Tanzanie, il n'existe pas d'autorités indépendantes chargées de superviser la collecte et le traitement des données dans le cadre des programmes de collecte de données biométriques. Au Lesotho, l'État n'a pas encore établi sa Commission de protection des données plus d'une décennie après l'entrée en vigueur de sa loi de 2011 sur la protection des données.<sup>237</sup> En outre, le pouvoir de collecter et de traiter des données biométriques pour les services essentiels est fragmenté entre de multiples lois et institutions fonctionnant en vase clos, sans cadres clairs ou communs pour guider la conception, la mise en œuvre et le déploiement de ces programmes. En conséquence, les acteurs étatiques et non étatiques continuent de mettre en œuvre des programmes non réglementés de collecte massive de données biométriques dans des systèmes et des processus mal gérés sans assumer la responsabilité des risques potentiels pour la vie privée, tout en restant opaques et non responsables de leurs actions et des atteintes potentielles à la vie privée qui pourraient en résulter.

L'absence de cadres juridiques efficaces et d'un contrôle indépendant, l'utilisation de bases de données centralisées, la faiblesse des garanties en matière de partage de l'information et le manque de transparence et de responsabilité dans la gestion de ces bases de données sont des failles qui créent inévitablement des possibilités d'abus de la part d'acteurs étatiques et non étatiques ayant accès à l'information.

### 3.3 Exclusion de l'accès aux services essentiels

Les programmes de collecte de données biométriques tels que les identifications numériques sont mis en œuvre dans des sociétés ayant des contextes culturels, sociétaux, économiques et politiques spécifiques, et ceux-ci doivent être pris en compte dans leur conception et les systèmes adaptés au contexte.<sup>238</sup> Sinon, ils risquent de numériser des problèmes préexistants avec les systèmes de gestion de l'identité existants, dont certains portent des reliques coloniales, et la discrimination historique. Dans les pays étudiés, l'enregistrement des programmes de données biométriques est souvent lié à la possession par une personne de documents d'identité officiels primaires tels que les cartes nationales d'identité, les certificats de naissance et les permis de conduire. Ainsi, l'absence de tels documents par une personne pourrait entraîner son exclusion de l'accès aux services de base, y compris le suffrage des adultes, les services financiers, l'emploi, l'éducation, la santé, les services sociaux, les voyages, l'enregistrement d'une entreprise, la possession d'une carte SIM et, par conséquent, l'accès à Internet.<sup>239</sup>

<sup>236</sup> La technologie de surveillance une préoccupation pour beaucoup en Afrique <https://newafricadaily.com/surveillance-technology-concern-many-africa>

<sup>237</sup> Lesotho <https://www.dataguidance.com/jurisdiction/lesotho>

<sup>238</sup> La technologie biométrique dans les programmes de protection sociale est-elle illégale ou arbitraire ? Une analyse de la vie privée et de la protection des données [https://www.ilo.org/wcmsp5/groups/public/---ed\\_protect/---soc\\_sec/documents/publication/wcms\\_631504.pdf](https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---soc_sec/documents/publication/wcms_631504.pdf); L'identité à l'ère numérique : Infrastructures pour Inclusive Développement [https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY\\_IN\\_A\\_DIGITAL\\_AGE.pdf](https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf); Identification numérique 101 : donner un sens à l'extrémité cléogy <https://www.africaportal.org/features/digital-id-101-making-sense-key-terminology/>; L'identité dans un monde numérique Un nouveau chapitre dans le contrat social [https://www3.weforum.org/docs/WEF\\_INSIGHT\\_REPORT\\_Digital%20Identity.pdf](https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf)

<sup>239</sup> voir, par exemple, pas de services gouvernementaux sans la Carte Huduma puisque la carte d'identité nationale cesse en décembre 2021 <https://www.citizen.digital/news/no-govt-service-without-huduma-card-as-use-of-national-id-to-cease-in-december-2021-646968>

Selon l'ensemble de données mondiales ID4D 2018 de la Banque mondiale, 81% des personnes dans le monde qui ont du mal à prouver leur identité en raison d'un manque de documents d'identité officiels se trouvent en Afrique subsaharienne (494 millions) et en Asie du Sud (312 millions).<sup>240</sup> De plus, les femmes sont plus susceptibles de ne pas avoir de pièce d'identité que les hommes. Cet écart est plus important dans les pays à faible revenu où une femme sur deux n'a pas de preuve officielle d'identité.<sup>241</sup> Selon l'ensemble de données ID4D Global, les 10 premiers pays d'Afrique ayant les niveaux les plus élevés de populations non enregistrées en 2018 étaient la Somalie (77%), le Nigeria (72%), l'Érythrée (70%), l'Éthiopie (65%), l'Angola (56%), la Zambie (56%), le Soudan du Sud (53%), le Tchad (53%), la Guinée équatoriale (53%) et l'Ouganda (49%).<sup>242</sup>

De nouveaux programmes pourraient également exacerber les injustices historiques de l'époque coloniale associées à l'exclusion de l'accès à l'identité juridique. Au Kenya, une affaire contestant le projet Huduma Namba a soulevé l'aspect de la discrimination numérique qui affecterait les membres des communautés nubiennes et somaliennes qui faisaient déjà l'objet d'une surveillance et d'obstacles supplémentaires pour établir leur citoyenneté et demander des documents d'identité. Ils risquaient maintenant d'être exclus de l'accès aux services en raison de l'absence de Huduma Namba.<sup>243</sup> En 2016, le Kenya comptait environ 18 500 communautés apatrides telles que les Makonde, les Shona et les Pemba qui vivaient dans le pays depuis plus de 80 ans sans être reconnues comme kenyannes et n'avaient donc pas reçu de documents d'identité.<sup>244</sup> Le gouvernement n'a reconnu que les 8 000 Makondés en 2016 et les 3 500 Shona en 2021,<sup>245</sup> tandis qu'environ 400 000 Pemba attendent une reconnaissance légale jusqu'à ce jour.<sup>246</sup>

De même, au Togo, de nombreuses personnes n'ont pas de pièces d'identité légales de base telles que des certificats de naissance, des cartes nationales d'identité ou des passeports, ce qui les empêche d'ouvrir des comptes bancaires pour accéder à des facilités de crédit, inscrire leurs enfants à l'école, souscrire une assurance maladie, bénéficier de programmes de protection sociale ou enregistrer leurs cartes SIM.<sup>247</sup> Le programme d'aide du pays, Novissi - Programme de Revenu Universel de Solidarité, qui a été mis en œuvre à la suite de la pandémie de COVID-19, a été critiqué pour avoir exigé des citoyens qu'ils présentent leur carte d'électeur avant d'accéder aux services de secours. L'opposition a lancé un appel public au boycott de l'exercice car il serait exclusif.<sup>248</sup>

En Ouganda, on s'est plaint que le programme d'identification biométrique ne couvre pas les zones reculées, ce qui oblige de nombreuses personnes dans ces régions à se rendre dans les zones urbaines pour accéder aux services. En outre, le processus d'enregistrement des cartes d'identité nationales a exclu les personnes marginalisées sur la base de leur incapacité et de leur appartenance ethnique.<sup>249</sup> Par exemple, les personnes handicapées, telles que celles qui n'ont pas les mains, ont été refusées faute d'empreintes digitales au lieu de bénéficier d'un autre mécanisme. Certaines minorités ethniques telles que les Maragoli ne sont pas reconnues comme un groupe ethnique en Ouganda et se sont vu refuser l'enregistrement.<sup>250</sup> Parmi les autres pratiques discriminatoires, on peut citer le refus d'accès à l'enregistrement en raison de longues distances à parcourir pour se rendre aux centres d'enregistrement, des barrières linguistiques et du manque de documents justificatifs tels que les certificats de mariage.

<sup>240</sup> Le défi mondial de l'identification : Qui sont les 1 milliard de personnes sans preuve d'identité ?

<https://blogs.worldbank.org/voices/global-identification-challenge-who-are-1-billion-people-without-proof-identity>

<sup>241</sup> ID4D Data: Le défi mondial de l'identification en chiffres <https://id4d.worldbank.org/global-dataset>

<sup>242</sup> Ensemble de données mondial 2018 <https://datacatalog.worldbank.org/cee776e9-8c54-47dd-90bd-1163315183e8>

<sup>243</sup> Affaire déposée to Arrêter le nouveau registre d'identification numérique au Kenya

<https://namati.org/news-stories/case-filed-stop-new-digital-id-system-kenya/>

<sup>244</sup> Des millions de personnes invisibles d'Afrique survivent avec sur les documents d'identité <https://www.equaltimes.org/africa-s-invisible-millions?lang=en>

<sup>245</sup> Joie alors que le Kenya accorde la citoyenneté à des descendants apatrides de migrants du Zimbabwe <https://www.fairplanet.org/story/joy-aS-Kenya-octroie-la-citoyennete-a-la-descendance-apatride-des-migrants-du-Zimbabwe/>; La fin de l'apatridie en vue pour Shona alors que le Kenya délivre des certificats de naissance <https://www.reuters.com/article/us-global-rights-stateless-kenya-feature-idUSKBN1WN15Q>

<sup>246</sup> La minorité Pemba apatride au Kenya <https://ghrd.org/the-pemba-minority-stateless-in-Kenya/>

<sup>247</sup> Le Togo espère lancer une nouvelle carte d'identité biométrique en 2021 <https://www.biometricupdate.com/202012/togo-hopes-to-launch-new-biometric-id-card-in-2021>

<sup>248</sup> Togo : Tâtonner Avec Une identification numérique tout en étant actif Surveillance Citoyens <https://cipesa.org/2022/04/togo-fumbling-with-a-digital-id-while-Citoyens-surveillants activement/>

<sup>249</sup> Ouganda : Les identités numériques sont-elles un outil d'inclusion ou d'exclusion ? <https://researchchictafrica.net/2021/06/23/uganda-are-digital-ids-a-tool-for-inclusion-or-exclusion/>

<sup>250</sup> Maragoli contre l'agro-industrie et la République de l'Ouganda

<https://indigenousofuganda.org/the-maragoli-of-uganda/#:~:text=Despite%20having%20been%20present%20in,only%20to%20recognized%20%E2%80%99Ctribes%E2%80%9D>

En 2021, jusqu'à un tiers des Ougandais n'avaient pas de carte d'identité biométrique, sept ans après l'introduction du système, les excluant ainsi des services sociaux et de soins de santé vitaux,<sup>251</sup> les femmes et les personnes âgées étant principalement touchées.<sup>252</sup> En outre, le projet d'identité appelé localement « Ndanga Muntu » est considéré comme un instrument de sécurité nationale, et l'absence d'identité pourrait laisser une personne considérée comme un étranger. Certaines cartes ont été signalées comme présentant des erreurs, où la correction des erreurs ou le remplacement des cartes coûte 50 000 UGX (13,05 USD), ce qui est inabordable pour beaucoup. En mars 2021, le gouvernement a été poursuivi pour avoir rendu obligatoire pour les citoyens de présenter leur carte ou numéro d'identité national (NIN) afin d'accéder à la vaccination contre la COVID-19, qui est en attente de détermination.<sup>253</sup> En outre, l'absence de carte d'identité a été identifiée comme un obstacle à l'ouverture de comptes bancaires, à l'achat de cartes SIM, à l'acquisition de passeports et à l'obtention d'un emploi formel.

En Tanzanie, la désactivation des cartes SIM en 2020<sup>254</sup> et la radiation des cartes soupçonnées d'avoir été utilisées pour commettre des crimes<sup>255</sup> ont empêché de nombreux citoyens d'accéder à Internet en raison de leur non-réenregistrement.

En Zambie, la mise en œuvre du nouveau processus national d'enregistrement de l'identité biométrique n'a pas encore été achevée. En outre, la discrimination à l'égard des femmes et des filles dans le pays, en particulier par le biais de règles et de pratiques traditionnelles, limite leur accès aux documents d'identité et leur utilisation.<sup>256</sup> En outre, l'obligation d'obtenir un certificat de naissance pour obtenir les cartes d'enregistrement nationales ou l'utilisation de cartes d'enregistrement nationales pour accéder aux cartes SmartCare de soins de santé, aux services financiers tels que les comptes bancaires et les services bancaires mobiles, à l'inscription par carte SIM ou à l'inscription des électeurs, rend difficile l'accès des femmes à ces services en raison de leur niveau de propriété inférieur à celui des hommes.<sup>257</sup> En 2016, la Zambie avait le quatrième taux d'enregistrement des naissances le plus bas au monde pour les enfants de moins de cinq ans, avec une couverture inférieure à 15%.<sup>258</sup>

### 3.4 Amélioration de la surveillance, du profilage et du ciblage

L'utilisation de la vidéosurveillance avec des technologies de reconnaissance faciale intégrées devient de plus en plus accessible et répandue sur le continent, mais ces systèmes ont tendance à être intrusifs. Ces systèmes peuvent suivre les mouvements des personnes, reconnaître les plaques d'immatriculation des véhicules à moteur et faire correspondre les images en direct des personnes dans le public avec les images des personnes figurant sur une « liste de surveillance » en fonction de leur capacité à reconnaître des caractéristiques faciales spécifiques et uniques, semblables à la prise d'empreintes digitales.<sup>259</sup>

<sup>251</sup> L'arrêté limitant le nombre de cartes SIM expliqué par l'ARCEP, Togo Cellulaire et Moov Afrique Togo L'Ouganda poursuivi en justice pour un système d'identification numérique qui exclut des millions de personnes <https://www.reuters.com/article/uganda-tech-biometrics-idUKL3N2X32RG>

<sup>252</sup> Le système d'identification ougandais exclut près d'un tiers des soins de santé, selon un rapport <https://www.theguardian.com/global-development/2021/jun/09/ugandas-id-scheme-excludes-nearly-a-third-from-healthcare-says-report>; Chassé et parti mourir <https://chrgj.org/wp-content/uploads/2021/06/CHRGJ-Report-Chased-Away-and-Left-to-Die.pdf>

<sup>253</sup> Vaccin contre le Covid-19 : les OSC saisissent la justice pour contester de présenter une carte d'identité nationale <https://www.unwantedwitness.org/covid-19-vaccine-csos-petition-court-challenging-national-id-requirement/>

<sup>254</sup> Xinhua, « Le régulateur tanzanien bloque plus de 650 000 utilisateurs de téléphones mobiles », *The East African*, 21 janvier 2020, <https://www.theeastafrican.co.ke/tea/news/east-africa/tanzanian-regulator-locks-out-over-650-000-mobile-phone-users-1435268>

<sup>255</sup> ShAron Sauwa, « 18 000 cartes SIM bloquées en Tanzanie », *The Citizen*, 29 juillet 2021, <https://www.thecitizen.co.tz/tanzania/news/national/18-000-sim-cards-blocked-in-Tanzania-3490770>

<sup>256</sup> Identité numérique Country Profile: Zambie <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report-Zambia.pdf>

<sup>257</sup> Identité numérique Profil Pays: Zambie <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/02/Digital-Identity-Country-Report-Zambia.pdf>

<sup>258</sup> Analyse des systèmes d'identification pour le développement (ID4D) : évaluation de pays Zambie <https://openknowledge.worldbank.org/bitstream/handle/10986/25106/108360.pdf?sequence=4&isAllowed=y>

<sup>259</sup> Collecte de données biométriques et reconnaissance faciale <https://www.mediadefence.org/ereader/publications/advanced-modules-on-digital-rights-and-freedom-of-expression-online/module-4-privacy-and-security-online/collection-of-biometric-data-and-facial-recognition/>



Ces systèmes posent plusieurs problèmes dans la région africaine. Premièrement, ils sont mis en œuvre passivement, collectent des images indiscriminées de personnes et ne nécessitent pas la connaissance, le consentement ou la participation des personnes concernées, et sont donc moins sujets à la suspicion.<sup>260</sup> L'introduction de systèmes de surveillance sur le continent, tels que Safe City de Huawei et les projets Smart City de ZTE, a été présentée par les gouvernements comme cruciale pour renforcer la sécurité. Cependant, ils ont été critiqués comme représentant des menaces pour les libertés civiles et ne produisant pas les dividendes promis tels que la réduction de la criminalité et l'amélioration de la gestion centralisée de la ville.<sup>261</sup>

Deuxièmement, lorsque les images de vidéosurveillance sont combinées avec des données biométriques et des informations biographiques capturées à partir du programme d'identification numérique de masse, elles peuvent créer un puissant outil de surveillance qui rend les résidents plus vulnérables au profilage ciblé, au suivi, à la surveillance politique et à la répression.<sup>262</sup> Partout sur le continent, les entités commerciales telles que les banques et les entreprises de télécommunications au Kenya ont de plus en plus accès aux bases de données gouvernementales pour leur permettre d'authentifier les documents officiels. En outre, les entreprises qui développent des systèmes biométriques tels que Zetes, Smartmatic, Huawei et ZTE sont souvent cooptés en tant que fournisseurs et exécutants de projets. Cependant, la transparence et la responsabilisation de ces entités sont limitées, y compris la divulgation des ententes de partage de données décrivant la nature et les types de données partagées, la façon dont elles sont utilisées et les personnes responsables de prendre des décisions à ce sujet.

Dans la plupart des pays examinés, l'enregistrement de la carte SIM est obligatoire et est lié aux données d'état civil telles que les cartes d'identité nationales qui sont utilisées pour la vérification de l'identité avant l'enregistrement. En outre, dans le cadre du processus d'enregistrement, les abonnés sont tenus de fournir des informations biométriques et biographiques complètes les concernant. Ces informations sont fournies aux télécoms et peuvent dans certains cas être consultées par les régulateurs locaux et les agences de l'État sur demande, dans certains cas avec un contrôle judiciaire rigoureux. Le principal risque est que les informations obtenues à partir de l'enregistrement de la carte SIM, y compris les données de géolocalisation des téléphones cellulaires lorsqu'elles sont croisées avec les bases de données du registre civil et les flux en direct des caméras de vidéosurveillance avec capacité de reconnaissance faciale, puissent être utilisées pour la surveillance et la triangulation de l'emplacement des cibles de l'État.

Dans de nombreux pays où ces nouveaux programmes de collecte de données biométriques sont lancés, les principales raisons de leur introduction sont notamment la sauvegarde de la sécurité nationale et la lutte contre la criminalité. Toutefois, comme indiqué plus haut, dans un certain nombre de ces pays, les garanties en matière de confidentialité des données sont faibles, de sorte que les abus sont perpétrés par l'absence d'une surveillance indépendante. En effet, il existe des craintes légitimes de glissement fonctionnel lorsque des gouvernements autoritaires détournent ces programmes de numérisation et utilisent légitimement les informations collectées à des fins qui n'étaient pas autrement prévues, et qui ne sont pas réglementées sans procédures ni surveillance claires. Par exemple, les données d'état civil peuvent être utilisées pour vérifier les informations dans les bases de données criminelles, valider l'enregistrement de la carte SIM et pour la vérification et l'authentification pour accéder aux services financiers, l'inscription des électeurs et pour la fourniture d'assurance maladie.

<sup>260</sup> Technologie de reconnaissance faciale <https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology>

<sup>261</sup> Au-delà de la guerre froide numérique : récits occidentaux, orientaux et méridionaux d'échecs et de succès numériques <https://www.cigionline.org/articles/beyond-the-digital-cold-war-western-eastern-and-southern-tales-of-digital-failure-and-success/>

<sup>262</sup> La technologie de surveillance une préoccupation pour beaucoup en Afrique <https://newafricadaily.com/surveillance-technology-concern-many-africa>

En Angola, en RDC, au Mozambique, au Nigeria et en Ouganda, la vidéosurveillance, l'enregistrement de la carte SIM et la carte d'identité nationale ont ajouté aux craintes qu'ils ne soient utilisés pour profiler, surveiller, suivre et arrêter les détracteurs du gouvernement, les journalistes, les manifestants et les dirigeants de l'opposition.<sup>263</sup> À la suite de la campagne de #EndSARS au Nigeria en octobre 2020, certains manifestants comme Bolatito Oduala, plus connu sous le nom de Rinu, et 19 autres ont été suivis et leurs comptes bancaires gelés par la Banque centrale du Nigeria (CBN) et accusés de blanchiment d'argent et d'erreur. En outre, Modupe Odele, qui a fourni une aide juridique aux manifestants, a vu son passeport international saisi par le Service nigérien de l'immigration (NIS) alors qu'elle se rendait aux Maldives. En Ouganda, à la suite des manifestations antigouvernementales de novembre 2020, la police a utilisé des images du système de vidéosurveillance pour retrouver et arrêter plus de 836 personnes soupçonnées d'avoir participé aux manifestations.<sup>264</sup>

### 3.5 Conflits d'intérêts et pouvoir des tiers

Le développement et le déploiement de la gestion de l'identité ont été largement dirigés par des entreprises du secteur privé, diverses organisations multilatérales, entreprises, ONG internationales et donateurs étrangers fournissant des prêts et un soutien technique. Parmi les risques associés, on peut citer la dépendance accrue à l'égard des systèmes propriétaires fournis par certains fournisseurs qui sont parfois retenus à des coûts exorbitants, l'hébergement de bases de données critiques en dehors de la juridiction du pays et le manque de transfert de technologie et de compétences après le déploiement. Cela laisse souvent les agences gouvernementales d'exécution à la merci des fournisseurs, car elles ont un contrôle limité de leurs informations et de leurs systèmes. L'utilisation de systèmes propriétaires, par opposition aux systèmes open source, peut également affecter la capacité des gouvernements à contracter différents fournisseurs de services. Au Kenya, par exemple, Smartmatic International, qui a été engagé par l'organisme électoral IEBC, a refusé d'accorder l'accès aux images du serveur en invoquant une violation de ses droits de propriété intellectuelle, malgré une ordonnance du tribunal rendue par la Cour suprême en août 2022.<sup>265</sup>

En outre, le rôle des entreprises chinoises telles que Huawei et ZTE en Europe et aux États-Unis a suscité des inquiétudes quant aux ramifications de leur implication dans le développement de nouveaux réseaux 5G à la suite d'accusations d'installation de portes dérobées utilisées pour espionner pour le compte du gouvernement chinois, ce que les entreprises ont nié.<sup>266</sup> De même, il y a des inquiétudes en Afrique car Huawei aurait construit environ 70% des réseaux 4G africains est accusé de vendre aux gouvernements africains, potentiellement des technologies représentatives dans le cadre de l'initiative Safe City dont les technologies pourraient porter atteinte aux droits de l'homme.<sup>267</sup> Ces préoccupations en matière de sécurité ont été éclipsées par la demande d'accès à Internet sur le continent et l'absence d'alternatives moins chères.<sup>268</sup>

La société civile a également évoqué l'utilisation de l'aide de l'Union européenne en Afrique de l'Ouest pour le développement de programmes d'identité légale et de surveillance dans plusieurs pays dans le cadre d'une mission plus large de contrôle des migrations.<sup>269</sup> En novembre 2020, des organisations de la société civile ont condamné l'utilisation des programmes d'aide et de coopération de l'UE pour former et équiper les forces de sécurité en Afrique avec des techniques de surveillance.<sup>270</sup> Un rapport de Privacy International a révélé que l'Agence de l'Union

<sup>263</sup> (Ngali – Surveillance des espaces publics et des communications en RDC (Projet Politique des médias et démocratie, p. 8) : <https://www.mediaanddemocracy.com/research.html>

<sup>264</sup> La police ougandaise accusée d'utiliser un système de reconnaissance faciale pour alimenter les violations des droits humains <https://www.biometricupdate.com/202011/ugandan-police-accused-of-using-facial-recognition-system-to-fuel-rights-abuses>

<sup>265</sup> Pétition pour un sondage au Kenya : Smartmatic refuse d'ouvrir les serveurs IEBC à Raila Odinga <https://www.theeastafrican.co.ke/tea/news/east-africa/smartmatic-refuses-to-open-iebc-servers-to-raila-odinga-3933676>

<sup>266</sup> Huawei dit sa surveillanceLa technologie assurera la sécurité des villes africaines, mais les activistes craignent qu'elle ne soit utilisée à mauvais escient <https://qz.com/africa/1822312/huaweis-surveillance-tech-in-africa-worries-activists/>

<sup>267</sup> Ibid.

<sup>268</sup> Pour l'Afrique, l'Internet construit en Chine vaut mieux que pas d'Internet du tout <https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/>

<sup>269</sup> Le prochain budget de l'UE est une énorme menace pour la vie privée - voici ce qui doit être fait <https://privacyinternational.org/advocacy/2548/eus-next-budget-huge-threat-privacy-heres-what-must-be-done>; Programme de gestion des frontières pour la région du Maghreb (BMP-Maghreb) <https://ec.europa.eu/trustfundforafrica/sites/default/files/t05-eutf-noa-reg-07.pdf>

<sup>270</sup> Des groupes de la société civile dénoncent l'implication de l'Union européenne dans la surveillance en Afrique <https://cipesa.org/2020/11/civil-society-groups-denounce-the-european-unions-involvement-in-surveillance-in-africa/>

européenne pour la formation en sciences juridiques (CEPOL) avait formé des services de police et de sécurité en Algérie, au Maroc et en Tunisie à la surveillance téléphonique et sur Internet, y compris la surveillance des médias sociaux, l'analyse des métadonnées des télécommunications, les enquêtes sur les appareils et l'extraction de données.<sup>271</sup> Il a également été signalé que les autorités frontalières et migratoires de l'Algérie, de l'Égypte, du Niger, de la Libye, du Maroc et de la Tunisie avaient suivi une formation similaire et avaient reçu du matériel technique.<sup>272</sup>

L'UE a soutenu la Commission de la CEDEAO à hauteur de 24 millions de dollars pour renforcer ses capacités en matière de gestion des données migratoires, de gestion des frontières, de migration de main-d'œuvre et de lutte contre la traite.<sup>273</sup> Il a également soutenu le gouvernement sénégalais avec 27 millions de dollars pour le développement de systèmes d'identification numérique biométrique à travers le « Fonds fiduciaire d'urgence pour l'Afrique ». <sup>274</sup> Une partie de l'appui apporté au Niger par le Fonds comprenait 11,1 millions de dollars pour la fourniture de drones de surveillance, de caméras de surveillance, de logiciels de surveillance, d'un centre d'écoute électronique et d'un collecteur international d'identité d'abonné mobile (IMSI).<sup>275</sup> La Côte d'Ivoire s'est vu allouer 29 millions d'euros pour le développement de son système d'identité biométrique universelle afin de permettre l'identification des Ivoiriens en séjour irrégulier en Europe afin « d'organiser plus facilement leur rapatriement ». <sup>276</sup>

Dans le cadre du projet d'identification unique pour l'intégration et l'inclusion régionales en Afrique de l'Ouest, la Banque mondiale a fourni 273 millions de dollars pour aider les États de la CEDEAO tels que le Bénin, le Burkina Faso, la Côte d'Ivoire, la Guinée, le Niger et le Togo à mettre en œuvre des systèmes d'identification fondamentaux.<sup>277</sup> La première phase des projets d'identification électronique a débuté en 2018 avec la Côte d'Ivoire et la Guinée pour un coût de 395,1 millions de dollars.<sup>278</sup>

Notamment, tous les pays ou entités privées, qu'ils soient européens, chinois ou américains, impliqués dans des projets de données biométriques, sont désireux de promouvoir leurs propres intérêts politiques, technologiques ou commerciaux, ce qui peut se faire au détriment de la vie privée des individus. Par conséquent, il est essentiel que les pays africains, dans leur engagement dans de tels partenariats, se méfient de la colonisation émergente des données et de la dépendance vis-à-vis des fournisseurs, et donnent plutôt la priorité à l'adoption de systèmes qui ne compromettent pas la vie privée et la protection des données au détriment des intérêts personnels, politiques, commerciaux ou autres.

<sup>271</sup> Voici comment une entreprise de sécurité bien connectée construit discrètement des bases de données biométriques de masse en Afrique de l'Ouest avec des fonds d'aide de l'UE <https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric>

<sup>272</sup> Frontières sans frontières : comment l'UE exporte la surveillance dans le but d'externaliser ses contrôles aux frontières <https://privacyinternational.org/long-read/4288/borders-without-borders-how-eu-exporting-surveillance-bid-outsource-its-border>

<sup>273</sup> La CEDEAO lance un projet de 26 millions € financé par l'UE sur la migration [https://www.ilo.org/africa/whats-new/WCMS\\_242035/lang--en/index.htm](https://www.ilo.org/africa/whats-new/WCMS_242035/lang--en/index.htm)

<sup>274</sup> Urgence de l'UE Fonds d'affectation spéciale pour l'Afrique <https://bit.ly/3SIQsZM>; CIVIPOL <https://bit.ly/3Px6OSI>

<sup>275</sup> Frontières sans frontières : comment l'UE exporte la surveillance dans le but d'externaliser sa frontière Contrôles <https://privacyinternational.org/long-read/4288/borders-without-borders-how-eu-exporting-surveillance-bid-outsource-its-border>

<sup>276</sup> L'avenir du fonds fiduciaire de l'UE pour l'Afrique <https://privacyinternational.org/sites/default/files/2019-09/EUTF%20Policy%20Séance%20d'information.pdf>

<sup>277</sup> Le Togo, le Bénin, le Burkina Faso et le Niger rejoignent le programme régional d'identification en Afrique de l'Ouest pour aider des millions de personnes à accéder au Services <https://www.worldbank.org/en/news/press-release/2020/04/28/Togo-Bénin-Burkina-FASO-et-Niger-join-Ouest-Afrique-Régionale-Identification-Programme-pour-aider-des-millions-de-personnes-a-céder-services->

<sup>278</sup> Ibid.

### 3.6 Capacité et formation limitées

Lorsque des autorités de protection des données ont été établies, comme au Ghana, au Kenya, en Ouganda et en Zambie, elles en sont relativement à leurs balbutiements et n'ont pas l'indépendance institutionnelle et financière nécessaire pour s'acquitter efficacement de leur mandat. En outre, ils ne disposent pas de ressources suffisantes et dépendent fortement de leurs ministères d'origine pour le personnel et les budgets, ce qui affecte également leur travail. En outre, les exemptions de sécurité nationale prévues dans les lois nationales protègent les agences de sécurité de l'État de l'examen et de la responsabilité des organismes de protection des données, ce qui contribue à de nouveaux abus des données biométriques.

En outre, dans des pays tels que la République centrafricaine, le Kenya, la Sierra Leone et l'Ouganda, la compétence du personnel des institutions publiques responsables de la collecte des données biométriques a été considérée par les répondants comme un défi. En République centrafricaine, certains membres du personnel ne sont pas bien formés aux moyens efficaces de protéger la vie privée des informations des utilisateurs lors des processus de collecte de données, par exemple à des fins d'inscription des électeurs. En Sierra Leone, certains membres du personnel de ces institutions peuvent difficilement apprécier l'éthique requise en matière de données personnelles dans l'exercice de leurs fonctions. Au Kenya et en Ouganda, certains membres du personnel ont eu des difficultés à utiliser les appareils numériques utilisés pour collecter des données biométriques.

# Conclusion and Recommendations

## 4.1 Conclusion

Ce rapport a passé en revue l'évolution de la collecte et du traitement des données biométriques dans 16 pays d'Afrique. Il couvre les pratiques émergentes et actuelles des gouvernements dans l'espace civique numérique. Les domaines d'intérêt spécifiques comprennent le déploiement de programmes nationaux fondés sur la technologie biométrique et le mode de mise en œuvre, les lacunes et les défis associés ainsi que les risques posés à la protection des données et de la vie privée et à d'autres droits numériques.

Les progrès technologiques s'accompagnent de multiples avantages, défis et risques. L'Afrique a connu une croissance exponentielle de la technologie, ce qui a donné naissance à plusieurs programmes de transformation numérique. Par conséquent, les programmes de collecte de données biométriques basés sur la technologie sont devenus attrayants pour les gouvernements qui cherchent à numériser leurs services d'enregistrement des faits d'état civil et d'administration en ligne et à développer leurs économies.

Les pays sont de plus en plus désireux d'améliorer et d'intégrer la collecte de données biométriques dans les bases de données démographiques pour les systèmes d'identification fondamentaux, les élections, les soins de santé, l'immigration, l'éducation, la protection sociale, les institutions financières, l'enregistrement des réfugiés et les systèmes de sécurité nationale pour la surveillance en temps réel. De même, à mesure que les technologies biométriques deviennent plus omniprésentes, elles deviennent également plus sophistiquées, plus fiables et plus utilisées dans une variété d'applications au sein de la société, chacune ayant un impact significatif sur les droits de l'homme.

Si la collecte de données biométriques dans le cadre de divers programmes peut apporter plusieurs avantages, elle peut également causer des dommages compte tenu des risques qu'elle présente et qui menacent les données personnelles et la vie privée. Les données biométriques, contrairement à d'autres formes de fichiers utilisés pour l'authentification comme les mots de passe et les codes, ne peuvent pas être changées ou modifiées. Il reste le même pendant toute la vie d'une personne, assurant ainsi la sécurité des données biométriques.<sup>279</sup> Ces programmes devront collecter et diffuser des données personnelles sensibles sur une grande partie des 1,4 milliard d'Africains, mais les investissements dans les garanties juridiques, techniques, réglementaires et procédurales de la vie privée pour sécuriser les informations et les mesures visant à atténuer les dommages et les effets négatifs sont largement insuffisants.

<sup>279</sup> Pourquoi l' Huduma Namba est importante pour l'avenir de l'identité numérique, et pas seulement au Kenya  
<https://privacyinternational.org/news-analysis/3350/why-huduma-namba-ruling-matters-future-digital-id-and-not-just-kenya>

Les systèmes de collecte de données biométriques reposent sur la connectivité Internet, les réseaux informatiques, les appareils numériques et les bases de données pour la mise en œuvre efficace de fonctions clés telles que l'enregistrement, l'identification, l'authentification et la vérification de l'entité d'identification. Les principaux risques pour la sécurité de ces systèmes comprennent le piratage et les violations de données, les cyberattaques, le vol d'identité et la fraude. Ces risques pourraient être aggravés lorsque les données sont stockées dans des bases de données centralisées et que les politiques, procédures et pratiques en matière de sécurité de l'information sont inadéquates. Cela est particulièrement vrai lorsque les bases de données sont interconnectées avec d'autres organismes gouvernementaux et liées pour faciliter les services tels que l'authentification pour les services financiers, les élections, l'enregistrement de la carte SIM ou la fourniture de services sociaux, sans tenir dûment compte des conséquences du partage généralisé des données ou de l'évaluation des risques pour la confidentialité des informations.<sup>280</sup>

En outre, même dans les 30 pays dotés de lois sur la protection des données et de la vie privée, les lois sont faibles avec des mécanismes de surveillance et des institutions inadéquats pour protéger complètement la vie privée des individus, tandis que les recours en cas de violation sont inefficaces et souvent inconnus de la personne concernée moyenne. De nombreux pays n'ont pas de lois spécifiques en matière de protection des données et de protection des données, ce qui signifie que le droit à la vie privée et à la protection des données à caractère personnel ne peut être effectivement garanti.

Le droit à la vie privée est essentiel dans une société démocratique car il joue un rôle essentiel dans la réalisation et la jouissance des droits à la liberté d'expression, d'association, de réunion et d'accès à l'information. Dans le Global Freedom Score 2022,<sup>281</sup> l'Angola, le Cameroun, la République centrafricaine et la République démocratique du Congo sont classés comme « non libres », tandis que le Lesotho, le Libéria, le Kenya, le Mozambique, le Nigeria, le Sénégal, la Sierra Leone, la Tanzanie, le Togo, la Tunisie et la Zambie sont classés comme « partiellement libres ». En outre, l'Angola, le Kenya, le Nigeria, la Tunisie, l'Ouganda et la Zambie sont classés comme « partiellement libres » par le score de liberté sur Internet 2021.<sup>282</sup> En outre, l'indice interne de protection de la vie privée, qui détaille la mesure dans laquelle les pays ont pris des mesures pour protéger la vie privée en ligne, a classé la Tunisie au premier rang parmi les pays africains inclus dans l'évaluation avec 45 sur 110 pays étudiés. Il était suivi par le Sénégal (54), le Kenya (57), le Libéria (69), le Nigeria (79), la Zambie (84), la Sierra Leone (85), la Tanzanie (88), l'Ouganda (89), le Togo (91), l'Angola (93), le Mozambique (100) et le Cameroun (102). La République centrafricaine, la République démocratique du Congo et le Lesotho n'ont pas été classés.<sup>283</sup> Il ressort de ce qui précède que la plupart des pays examinés sont pour la plupart mal classés car ils ont certains des niveaux les plus bas de protection des droits politiques, des libertés civiles, de la liberté de l'internet et de la vie privée.

Par conséquent, la mise en œuvre de programmes biométriques dans des pays où les droits numériques sont médiocres, où la démocratie décline et où l'autoritarisme numérique monte n'inspire pas confiance et jette le doute sur l'intégrité des bases de données biométriques. Les programmes de collecte de données doivent être maintenus et exempts d'abus. Ces bases de données, malgré leur coût élevé de mise en œuvre, peuvent également créer des incitations au vol d'identité, à la discrimination et à l'exclusion de l'accès aux services. Cependant, la centralisation, la consolidation et la liaison des informations collectées dans les bases de données numériques biométriques nationales avec les informations des individus exploitées à partir de programmes d'identification numérique, de caméras de vidéosurveillance avec reconnaissance faciale, d'enregistrement obligatoire de la carte SIM, dans des environnements où les lois sur la protection de la vie privée sont faibles et les lois omniprésentes sur la surveillance des communications et une surveillance insuffisante est un problème croissant. Considérés collectivement, les développements, les tendances et les risques décrits dans ce rapport ne peuvent qu'accroître les inquiétudes face aux menaces croissantes au droit à la vie privée des données personnelles et aux violations potentielles des droits numériques sur le continent.

<sup>280</sup> Comprendre les effets vécus de l'identité numérique, Une étude multi-pays

[https://digitalid.theengineeroom.org/assets/pdfs/200310\\_TER\\_Digital\\_ID\\_Report+Annexes\\_English\\_Interactive\\_Edit3.pdf](https://digitalid.theengineeroom.org/assets/pdfs/200310_TER_Digital_ID_Report+Annexes_English_Interactive_Edit3.pdf)

<sup>281</sup> Score de liberté mondiale 2022 <https://freedomhouse.org/countries/freedom-world/scores>

<sup>282</sup> Score de liberté sur Internet 2021 <https://freedomhouse.org/countries/freedom-net/scores>

<sup>283</sup> Indice de confidentialité <https://bestvpn.org/privacy-index/#tab-con-11>



## 4.2 Recommandations

Cette section présente des recommandations à diverses parties prenantes, y compris le gouvernement, la société civile, les médias, le secteur privé et le milieu universitaire, qui, si elles sont mises en œuvre, contribueront grandement à combler les lacunes, les risques et les défis en matière de protection des données et de la vie privée dans les pays étudiés.

### Government

- Mettre en œuvre les lois et les cadres politiques sur les systèmes d'identité et la protection des données et de la vie privée tout en accordant une attention particulière au respect des principes et des normes minimales reconnus aux niveaux régional et international en matière de protection des données et de la vie privée pour la collecte de données biométriques et exiger l'adoption d'approches fondées sur les droits de l'homme. Ces lois et politiques devraient être revues régulièrement et à l'épreuve du temps pour relever les défis de l'innovation technologique.
- Les pays dépourvus de lois sur la protection des données et de la vie privée, tels que le Libéria, le Mozambique, la Sierra Leone et la Tanzanie, devraient accélérer le processus de promulgation de lois appropriées sur la protection des données afin de garantir la protection des données et le droit à la vie privée de leurs citoyens. Le processus de promulgation de ces lois devrait tenir compte des principes et pratiques de protection des données acceptés aux niveaux régional et international afin de couvrir l'ensemble du cycle de vie des données et de les aligner sur ceux-ci.
- Mettre en place des organismes de surveillance indépendants et solides chargés de réglementer la protection des données et de la vie privée, y compris les données biométriques. Les organes devraient bénéficier d'un niveau louable d'autonomie et bénéficier d'une aide suffisante avec les ressources nécessaires pour qu'ils fonctionnent efficacement, en toute indépendance et avec un minimum d'influence extérieure sur leur mandat. Ils devraient être habilités à faire appliquer les lois, à recevoir et à instruire les plaintes, à effectuer des contrôles de conformité de routine et à contrôler rigoureusement la conduite des audits de protection des données et des évaluations d'impact sur les droits de l'homme à chaque étape des programmes de collecte de données biométriques proposés et en cours.
- Les pays étudiés, en particulier l'Afrique du Sud, l'Algérie, le Botswana, le Cameroun, l'Égypte, l'Éthiopie, la Côte d'Ivoire, le Kenya, le Libéria, Madagascar, le Maroc, le Nigéria, la Sierra Leone, la Tanzanie, l'Ouganda et le Zimbabwe, devraient ratifier rapidement la Convention de l'Union africaine sur la cyber sécurité et la protection des données à caractère personnel (Convention de Malabo). La Convention de Malabo est un instrument d'orientation essentiel pour l'harmonisation et le renforcement de la législation nationale existante et future en matière de cyber sécurité en Afrique. La ratification témoignera de l'engagement en faveur de la protection des données et de la vie privée, y compris des données biométriques, de cyber sécurité et de la société de l'information.
- Renforcer les capacités des responsables gouvernementaux responsables des programmes de collecte de données biométriques, y compris les organismes de protection des données, les forces de l'ordre, les poursuites, les régulateurs et le pouvoir judiciaire, en matière de protection efficace des données. Le renforcement des capacités peut aller jusqu'à leur qualification conformément aux principes de protection des données et aux droits des personnes concernées. Cela renforcera la protection des données et garantira un traitement approprié et légal des données personnelles.
- Promouvoir des consultations publiques continues et significatives et des engagements multipartites avec les principales parties prenantes telles que la société civile, le secteur privé, les universités, la communauté technique et les médias sur la protection des données et de la vie privée, y compris la biométrie. Cet engagement, lorsqu'il est étayé par une divulgation proactive des informations avant le début et en continu pendant la mise en œuvre des programmes biométriques, peut contribuer à promouvoir la transparence, à lutter contre la discrimination, à développer des solutions appropriées, à instaurer la confiance et à éliminer les idées fausses et les soupçons concernant la mise en œuvre des systèmes biométriques.

- Les efforts délibérés visant à promouvoir l'inclusion et à éliminer les obstacles à l'exclusion et à l'inégalité auxquels sont confrontés les groupes vulnérables, marginalisés et minoritaires, y compris les personnes handicapées, les femmes, les jeunes, les personnes vivant dans des zones à faible revenu et les communautés rurales, les personnes âgées, les minorités sexuelles, les migrants et les réfugiés dans la fourniture de services sociaux et économiques essentiels en utilisant des justifications telles que la non-acquisition de documents d'identité légaux comme les certificats de naissance, les cartes d'identité nationales et les passeports et la non-inscription aux programmes nationaux de collecte de données biométriques comme motif de refus de services. En outre, des moyens d'identification complémentaires ou alternatifs devraient être acceptables pour accéder aux services publics essentiels.
- Avant la mise en œuvre des programmes biométriques, les gouvernements devraient investir dans la réalisation d'activités préparatoires telles que des évaluations des besoins, des études de faisabilité, des essais pilotes, des programmes de formation et de renforcement des capacités, ainsi que des programmes de sensibilisation du public susceptibles d'éclairer la conception, le choix et le type de technologies appropriées et adaptées au contexte. Le calendrier de ces activités devrait être bien planifié, le financement obtenu et l'approvisionnement effectué à temps afin d'éviter les retards et autres difficultés de mise en œuvre.
- Promouvoir l'utilisation de systèmes ouverts et de normes de mise en œuvre pour assurer l'interopérabilité, et éviter la dépendance vis-à-vis des fournisseurs afin de promouvoir la concurrence dans les marchés publics, de réduire les coûts et d'assurer la flexibilité.
- Effectuer une diligence raisonnable et des évaluations des risques sur les fournisseurs de technologies biométriques avant leur approvisionnement afin de s'assurer que leurs produits, processus et services sont conformes aux normes applicables en matière de droits de l'homme.

## Société civile

- Travailler main dans la main avec d'autres parties prenantes, y compris le gouvernement, le secteur privé, la communauté technique, les médias et le public pour promouvoir la compréhension et la démystification de la biométrie, notamment par la sensibilisation et le renforcement des capacités des principaux acteurs de la protection des données et de la vie privée. Un tel partenariat peut améliorer la compréhension, les compétences et les compétences nécessaires pour répondre aux questions, défis et opportunités émergents en matière de protection des données et de la vie privée.
- En tant que chiens de garde des droits de l'homme, s'engager dans le plaidoyer et faire pression sur les gouvernements pour qu'ils élaborent, mettent en œuvre et appliquent des politiques, des lois et des cadres institutionnels en matière de protection de la vie privée et des données qui sont conformes aux normes minimales régionales et internationales en matière de droits de l'homme.
- Pousser spécifiquement les gouvernements à ratifier la Convention de l'UA de cyber sécurité et la protection des données personnelles (Convention de Malabo) afin de garantir l'engagement du gouvernement en faveur de la protection régionale des données et de la vie privée afin de les tenir responsables.
- Surveiller, documenter et rendre compte des risques, des menaces, des abus et des violations de la vie privée et des droits de l'homme associés aux programmes de collecte de données biométriques, et proposer des solutions efficaces pour protéger les droits conformément aux normes internationales en matière de droits de l'homme.
- Signaler constamment les cas de violation de la protection des données et de la vie privée aux mécanismes internationaux des droits de l'homme tels que l'Examen périodique universel (EPU) et la Commission africaine des droits de l'homme et des peuples (CADHP). Des rapports constants et progressifs peuvent potentiellement conduire à des changements positifs, car ils sont essentiels pour évaluer le bilan du pays en matière de droits de l'homme. C'est aussi un outil pour renforcer la responsabilité et la transparence de l'État qui a agi en violation.
- S'engager dans des litiges stratégiques et collaboratifs d'intérêt public devant les tribunaux nationaux et régionaux pour contester les violations des données et de la vie privée par des acteurs étatiques et non étatiques dans le but de les tenir responsables et d'obtenir des recours efficaces pour les personnes concernées ou les personnes lésées.

## Media

- Documenter, rapporter et publier progressivement des initiatives telles que le plaidoyer et par la société civile et d'autres parties prenantes pour suivre les développements. L'engagement continu des médias peut servir d'outil de réflexion et de suivi de la responsabilité et de la transparence par le principal responsable - le gouvernement - en matière de protection des données et de la vie privée.
- En collaboration avec d'autres parties prenantes telles que la société civile, le secteur privé et les universités, sensibiliser le public avec des informations factuelles et objectives grâce à une couverture plus large des défis, des risques, des menaces, des opportunités, des avantages et des implications des programmes de collecte de données biométriques et de leur impact sur leur vie privée et d'autres droits de l'homme.
- Mener un journalisme d'investigation pour identifier et exposer les violations de la vie privée découlant de la mise en œuvre de programmes de collecte de données biométriques. Le journalisme d'investigation a le potentiel d'améliorer la responsabilité et la transparence en matière de protection des données et de la vie privée.
- Renforcer les capacités des journalistes, par exemple grâce à une formation sur mesure pour comprendre la protection des données et de la vie privée et à des reportages efficaces sur ce sujet. Le renforcement des capacités pourrait potentiellement améliorer la compréhension, le suivi et le reportage des journalistes sur les développements et les tendances dans les programmes de collecte de données biométriques, ce qui à son tour conduit à une couverture efficace des problèmes.

## Secteur privé

- S'efforcer délibérément de veiller à ce que tous leurs programmes et systèmes respectifs de collecte de données biométriques soient élaborés, mis en œuvre et gérés conformément aux meilleures pratiques de collecte de données prescrites par les normes et pratiques nationales, régionales et internationales en matière de droits de l'homme en matière de protection de la vie privée et des données, y compris les Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme.
- Veiller à ce qu'ils adoptent et développent progressivement des politiques internes de confidentialité complètes pour guider la collecte, le stockage et le traitement des données personnelles. Les politiques internes de protection des données garantiront, grâce à des initiatives telles que les évaluations de l'impact sur la confidentialité des données, un traitement et une gestion transparents et responsables des données à caractère personnel.
- Déployer des efforts délibérés visant à impliquer les personnes concernées dans le contrôle et la gestion de leurs données personnelles en fournissant des informations en temps opportun sur les demandes d'informations externes. Cela pourrait potentiellement renforcer la participation du public et éliminer les cas de suspicion et de mauvaise gestion des données à caractère personnel.
- S'opposer fermement à toute demande et pratique illégale de données personnelles de la part des gouvernements et publier fréquemment des rapports de transparence. Cela renforcera potentiellement la confiance dans le secteur privé et améliorera également la gestion responsable et transparente des données à caractère personnel.
- Adopter progressivement la protection de la vie privée centrée sur les personnes, ainsi que la protection de la vie privée et la sécurité dès la conception dans l'élaboration et la mise en œuvre de systèmes de manière à placer le contrôle des données personnelles entre les mains des personnes concernées.
- En collaboration avec d'autres parties prenantes telles que la société civile, les universités et les médias, soutenir le renforcement des capacités des décideurs politiques à comprendre les défis, les risques, les opportunités et les implications des programmes de collecte de données biométriques axés sur l'élaboration de politiques efficaces et progressistes, de lois sur la protection des données et de la vie privée.
- Créer un mécanisme de réponse rapide pour leur clientèle à tout cas de violation de données, et s'engager continuellement dans la sensibilisation et l'éducation sur les programmes pour le public grâce à la publication proactive d'informations importantes. Cela renforcera potentiellement la confiance et la compréhension du public quant à l'interaction entre la protection des données et de la vie privée et les programmes de collecte de données associés.

## Milieu Universitaire

---

- Conduire des recherches fondées sur des données probantes sur la protection des données et de la vie privée, y compris la biométrie, mettant en évidence les défis, les risques, les avantages et les tendances des programmes de collecte de données biométriques. La recherche, une fois largement diffusée, peut éclairer le débat, les litiges et le plaidoyer en faveur de la réforme et de la progression au-delà de diverses frontières telles que les mécanismes internationaux de surveillance des droits de l'homme.
- Collaborer avec d'autres parties prenantes clés et s'engager dans des initiatives qui améliorent, protègent et promeuvent la protection des données et les droits à la vie privée. Ces initiatives comprennent le plaidoyer tel que les litiges et la publication et le renforcement des capacités des principales parties prenantes par la formation.
- Participer et contribuer à l'élaboration des politiques et des lois sur les régimes de protection des données et de la vie privée en intervenant en temps opportun dans les processus. Une intervention en temps utile peut être réalisée en fournissant directement des commentaires sur les projets de politiques et de lois, ainsi qu'en fournissant des orientations sur le contenu, la forme et l'orientation des politiques, lois et instruments axés sur la protection des données et la vie privée.





**Collaboration on International ICT Policy for East and Southern Africa (CIPESA)**

☎ +256 414 289 502

✉ [programmes@cipesa.org](mailto:programmes@cipesa.org)

🐦 @cipesaug    📘 facebook.com/cipesaug    🔗 LinkedIn/cipesa

🌐 [www.cipesa.org](http://www.cipesa.org)