26 octobre 2020

T-PD(2020)04Rev

COMITÉ CONSULTATIF DE LA CONVENTION POUR LA PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT AUTOMATISÉ DES DONNÉES À CARACTÈRE PERSONNEL

CONVENTION 108

Identités numériques

par

Pat Walshe

Direction Générale Droits de l'homme et État de droit

Les vues exprimées dans ce document sont de la responsabilité de leurs auteurs et ne reflètent pas nécessairement la ligne officielle du Conseil de l'Europe.

Table des matières

1. Introduction 2

2. Qu'est-ce que l'« identité numérique » ? 3

2.1 La numérisation de l'identité juridique 5

2.2 Biométrie et identité numérique : des corps informationnels 7

3. Scénarios de mise en place de l'identité numérique 10

3.1 Systèmes d'identification nationaux 10

3.1.1 Kenya : le système national d'identification numérique « Huduma Namba » et son examen par les instances judiciaires 13

3.1.2 Jamaïque : l'identifiant numérique national 14

3.2 Identité numérique et enregistrement de carte SIM obligatoire 15

3.3 Enregistrement des données d'utilisateurs de cartes SIM mobiles, services d'argent mobile et confidentialité des transactions 17

3.3.1 Inde – Système aadhaar, enregistrement des données d'utilisateurs de cartes SIM, vie privée et libertés 20

3.4 Identité numérique dans les contextes humanitaires : créée par qui et pour qui ? 21

4. Conclusions et éléments de réflexion pour les responsables politiques 26

PROJET NON DESTINÉ À ÊTRE CITÉ

La possession d'une identité numérique et la capacité de prouver qui l'on est apportent des avantages notables et des protections importantes dans de multiples contextes. Mais l'identité numérique comporte aussi des risques : discrimination, marginalisation, surveillance injustifiée, et jusqu'à la perte du contrôle par l'individu de son identité ou la représentation de son identité par d'autres. On assiste à un besoin sans précédent de créer « une identité pour tous » sous la forme d'« identifiants numériques » qui soulève de graves questions. Qui crée ces identités, pour qui sont-elles créées et qui pose les conditions ? Les systèmes d'identification numérique ont-ils une incidence sur la capacité d'agir des humains qu'ils sont censés servir ? Ces derniers contrôlent-ils encore la manière dont ils sont présentés au monde ? Quels sont les effets de l'identification numérique sur leurs expériences de vie[1] et sur leurs droits fondamentaux ?

1. Introduction

Il n'existe pas de définition unique et universelle de l'« identité numérique ». Ce terme prend des significations multiples et variées, dans la vie privée comme dans la sphère publique. Il est généralement admis que l'identité numérique est constituée d'un ensemble d'attributs traités électroniquement, qui désignent de manière unique et représentent une entité (personne ou dispositif numérique par exemple) dans des contextes donnés. Née du concept de gestion des identités et des accès – contrôle d'accès aux systèmes informatiques et aux biens électroniques –, l'identité numérique n'est pas et n'a pas besoin d'être une identité du monde réel.

Pourtant, les programmes d'orientation et les initiatives des États, des organisations internationales et du secteur privé favorisent la conceptualisation et le développement de l'« identité numérique » en tant que représentation numérisée de l'identité juridique sous la forme d'un « identifiant numérique » national. Cette reconceptualisation est favorisée par l'émergence d'initiatives de promotion des intérêts commerciaux et par la chosification de l'« identité numérique » en tant que « droit humain fondamental »[2].

L'« identité numérique » reconceptualisée est promue comme une identité numérisée et reconnue sur le plan légal (un « identifiant numérique »), et elle est dorénavant, dans bien des cas, un préalable nécessaire pour accéder aux services et aux droits essentiels dans de nombreux pays. Ces « identifiants numériques » s'appuient de plus en plus souvent sur des technologies biométriques, qui « *lisent les caractéristiques corporelles et comportementales des individus dans le but de leur attribuer une identité, de les authentifier ou de les trier, à partir de catégories et de logiques prédéfinies*[3]. » Les technologies d'identification biométrique rendent les individus lisibles par machine, en leur assignant un statut identitaire qui détermine s'ils peuvent bénéficier des services et des avantages que les systèmes d'identification numérique sont censés fournir ou s'ils en sont exclus. Les travaux menés dans le cadre du présent rapport montrent que la technologie de l'« identité numérique », voire la législation peuvent, bien que n'en ayant pas nécessairement l'intention, faciliter le profilage, la surveillance et l'exclusion des individus et des groupes qu'elles sont supposées servir[4].

[1] Voir note 115.
[2] « MasterCard joins ID2020 Alliance », https://mastercardcontentexchange.com/newsroom/press-releases/2020/may/mastercard-joins-id2020-alliance/.
[3] Martin et Whitley, « Fixing identity? Biometrics and the tensions of material practices », 2013, http://personal.lse.ac.uk/whitley/allpubs/MCS2013.pdf.
[4] La Cour a annulé la loi intitulée *National Identification and Registration Act* (loi relative à l'identification nationale et à l'enregistrement national), qui prévoyait le recueil de données biométriques dans l'ensemble de la population jamaïcaine et leur stockage dans une base de données centralisée. *Robinson c. Le Procureur général de Jamaïque*, https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf.

Field Code Changed

Nous nous intéressons ici à la manière dont a évolué l'« identité numérique » avec les avantages et les risques que présente un « identifiant numérique » national reconceptualisé, et à l'importance de prévoir des cadres juridiques et des sauvegardesgarde-fous suffisants pour protéger les droits de l'homme. Pour cela, nous nous appuyons sur des études de cas et des problématiques juridiques qui soulignent l'importance de bâtir des systèmes d'« identification numérique » (qui, intentionnellement ou non, deviennent *de facto* des systèmes nationaux d'identité) inclusifs qui reflètent un but légitime et qui, dans leur conception, leur mise en œuvre et leur exploitation donnent par défaut la priorité aux droits de l'homme. L'argument selon lequel « *un identifiant mondial unique semblerait être la solution pour attribuer à une personne une existence numérique officielle dans la Société de l'information*[5] » montre que cette réflexion est particulièrement de mise. Les travaux de recherche soulignent aussi que les approches adoptées dans ce domaine doivent prendre en compte le vécu des bénéficiaires présumés des systèmes d'identification numérique ainsi que leurs effets sur eux car ils pourraient être exposés « *aux plus grands risques liés à l'infrastructure, aux politiques et aux protocoles d'identification numérique*[6]. »

Une identité pour qui ? La question est essentielle. En effet, certaines études montrent que les systèmes d'identification numérique – publics et privés – pourraient se renforcer mutuellement, en croisant des identifiants ou en créant des identifiants nationaux mondiaux uniques qui laisseraient peu de chance aux humains de s'épanouir sans être surveillés ou sans craindre de l'être, par exemple. Se pose dès lors la question du « respect de la vie privée au sens d'épanouissement de l'être humain »[7] et du droit des individus à être libres de poursuivre le développement et l'épanouissement de leur personnalité, conformément à l'article 8 de la Convention européenne des droits de l'homme et de la jurisprudence correspondante[8]. Ainsi, les systèmes d'identification numériques et la mise en données des corps et des comportements pourraient laisser peu de place à l'épanouissement de l'être humain.

2. Qu'est-ce que l'« identité numérique » ?

Partout dans le monde, les heureux possesseurs d'un smartphone, d'une tablette ou d'un ordinateur connecté à l'internet à haut débit évoluent quotidiennement dans de multiples environnements virtuels. Pour communiquer sur les réseaux sociaux, effectuer des achats en ligne, regarder la télévision ou écouter de la musique diffusée en continu, ils sont invités à présenter leur « identité numérique », qui les identifie de manière unique. Dans ces environnements virtuels, l'identité numérique de l'utilisateur peut se limiter à ce que l'on appelle son « personnage en ligne »[9], qu'il peut créer lui-même ou qui lui est attribué lorsqu'il se connecte aux différents services. Ce « personnage » peut prendre plusieurs formes : adresse électronique personnelle, nom d'un profil sur un réseau social, numéro d'une carte prépayée, identifiant d'un appareil, etc. Une même personne peut avoir plusieurs « personnages » et choisir quelle identité présenter selon le contexte virtuel. Ces « identités numériques », conjuguées à un moyen d'identification (mot de passe, numéro d'identification personnel (PIN), etc.), sont souvent suffisantes pour s'assurer que la personne qui s'identifie

[5] UNESCO, Programme Information pour tous, *Étude sur les implications éthiques des nouvelles technologies*, 2007, *http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/ethical-implications-of-emerging-technologies-a-survey/*.
[6] The Engine Room, *Comprendre les effets vécus de l'identification numérique. Une étude transnationale*, 2020, https://digitalid.theengineroom.org/assets/pdfs/200123_FINAL_TER_Digital_ID_Report+Annexes_French_Interactive.pdf.
[7] Bart van der Sloot, JIPITEC, « Privacy as human flourishing: Could a shift towards virtue ethics strengthen privacy protection in the age of Big Data? », 2014, https://www.ivir.nl/publicaties/download/1558.pdf.
[8] Cour européenne des droits de l'homme, *Guide sur l'article 8 de la Convention européenne des droits de l'homme*, 2019, www.echr.coe.int/Documents/Guide_Art_8_FRA.pdf.
[9] National Institute of Standards and Technology (NIST), *Digital Identity Guidelines*, 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf.

est effectivement celle qu'elle prétend être, par exemple lorsqu'elle se connecte à son compte sur un réseau social. Ces « identités numériques » ne sont pas toujours et ne doivent pas nécessairement être l'identité réelle et vérifiée de l'utilisateur. Elles contribuent ainsi à lui apporter un certain niveau de confidentialité et de contrôle sur leur véritable identité.

Cependant, certains environnements virtuels, notamment les services financiers en ligne, exigent des niveaux de garantie plus élevés afin de renforcer leur confiance dans les personnes qui effectuent des transactions en ligne et de protéger ces dernières contre d'éventuelles conséquences préjudiciables. En outre, les prestataires de services financiers en ligne peuvent avoir l'obligation légale de vérifier l'identité des personnes pour être en conformité avec les réglementations en matière de vigilance à l'égard de la clientèle et de lutte contre le blanchiment des capitaux (LCB)[10]. Plus que jamais, l'identité numérique est considérée comme un élément « *d'une importance stratégique pour le futur des services numériques* »[11] et comme un fondement essentiel de l'économie numérique[12], de son bon fonctionnement et de sa création de valeur[13]. Ces évolutions ont contribué à l'émergence d'une industrie de l'identité numérique[14] et ont encouragé les pouvoirs publics à promouvoir l'instauration d'un écosystème de l'identité numérique[15] et la création de marchés de l'identité numérique pour soutenir l'économie numérique[16].

Il n'existe pas de définition unique et universelle de l'« identité numérique » et cette expression a de multiples significations dans la vie privée et dans la sphère publique. Mais pour le dire simplement, l'« identité numérique » peut être considérée, pour les organisations, comme un moyen de vérifier si une personne effectuant une transaction en ligne est bien celle qu'elle prétend être. La Banque mondiale considère que l'identité numérique est « *un ensemble d'attributs et d'authentifiants recueillis et stockés électroniquement qui peuvent identifier une personne de manière unique*. » Pour le Gouvernement britannique, l'identité numérique est un moyen fiable par lequel un citoyen ou un consommateur peut prouver la véracité d'« *un ou plusieurs attributs le concernant [...] et du lien établi entre ces attributs et lui-même en tant qu'individu identifiable de manière unique*[17]. » Dans une publication conjointe, la Banque mondiale, la GSMA et l'organisation Secure Identity Alliance donnent de l'identité numérique la définition suivante : « *ensemble d'attributs d'identité recueillis et stockés électroniquement qui décrivent une personne de manière unique dans un contexte donné et sont utilisés pour effectuer des transactions électroniques* », et pouvant comprendre des attributs biographiques tels que le nom, l'âge, le genre et l'adresse ou des données biométriques comme les empreintes digitales ou une image de l'iris[18]. Il importe de noter que selon le National Institute of Standards and Technology (NIST), si une « *identité numérique est toujours unique dans le contexte d'un service numérique donné* », il n'est pas toujours nécessaire d'identifier une personne de manière unique dans tous les contextes de

[10] GAFI, *Guidance on Digital Identity*, 2020, http://www.fatf-gafi.org/fr/publications/recommandationsgafi/documents/digital-identity-guidance.html.
[11] Nyst *et al.*, Consult Hyperion, *Digital Identity: Issue Analysis*, 2016, https://chyp.com/wp-content/uploads/2020/06/PRJ.1578-Digital-Identity-Issue-Analysis-Report-v1_6-1.pdf.
[12] UK Government Digital Service, « The Future of Digital Identity », 2019, *https://gds.blog.gov.uk/2019/03/25/the-future-of-digital-identity/*.
[13] GSMA, *Mobile Identity - Unlocking the Potential of the Digital Economy*, 2014 https://www.gsma.com/identity/wp-content/uploads/2014/10/GSMA-SIA-paper_FINALNov-2014.pdf.
[14] *Digital Identity Solutions Market worth $30.5 billion by 2024*, https://www.marketsandmarkets.com/PressReleases/digital-identity-solutions.asp.
[15] techUK,, *The case for digital IDs: A techUK white paper*, 2019, https://www.techuk.org/images/documents/digital_id_FINAL_WEBSITE.pdf.
[16] Gov.UK, « Minister confirms government ambition on digital identity », 2019, https://www.gov.uk/government/news/minister-confirms-government-ambition-on-digital-identity.
[17] DCMS, *Digital Identity: Call for Evidence*, 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/818801/Digital_Identity_-_Call_for_Evidence.pdf.
[18] Groupe Banque mondiale, GSMA, Secure Identity Alliance, *Digital Identity: Towards Shared Principles for Public and Private Sector Cooperation*, 2016, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/07/Towards-Shared-Principles-for-Public-and-Private-Sector-Cooperation.pdf.

transaction numérique et que « *l'accès à un service numérique n'implique pas nécessairement que l'identité réelle de la personne soit connue* » ou qu'elle doive l'être[19].

Bien qu'il ne soit pas nécessaire qu'une « identité numérique » soit équivalente à une identité réelle, on observe de plus en plus que les organisations internationales, l'industrie et les pouvoirs publics définissent et défendent l'« identité numérique » comme étant un substitut de l'« identité juridique ». Le présent rapport porte précisément sur cet aspect de l'« identité numérique », autrement dit, à la numérisation de l'identité juridique en tant qu'identité numérique nationale représentée par un identifiant numérique.

2.1 La numérisation de l'identité juridique

L'interprétation des instruments de protection des droits de l'homme et les initiatives de développement au niveau international sont à l'origine de la numérisation de l'identité juridique et de sa transformation en une « identité numérique ». L'article 6 de la Déclaration universelle des droits de l'homme (DUDH)[20] et l'article 16 du Pacte international relatif aux droits civils et politiques[21] énoncent que chaque être humain a droit à la reconnaissance de sa personnalité juridique. Ces articles servent de base au programme des Nations Unies relatif à l'identité juridique[22] et à l'objectif de développement durable 16.9 des Nations Unies (ODD 16.9), lequel appelle à garantir « *à tous une identité juridique, notamment grâce à l'enregistrement des naissances* » d'ici à 2030[23]. L'ODD 16.9 ne précise pas ce qu'est l'« identité juridique », mais le Groupe d'experts des Nations Unies sur l'identité juridique en donne la définition suivante : « *caractéristiques de base constituant l'identité d'une personne, telles que le nom, le sexe et le lieu et la date de naissance, conférées après la naissance lorsqu'une autorité habilitée d'état civil enregistre la naissance et délivre l'acte qui l'atteste*[24]. »

Les autorités et systèmes chargés de l'enregistrement des faits d'état civil et des statistiques de l'état civil sont un moyen fondamental de conférer aux individus une identité juridique depuis le berceau jusqu'à la tombe, et de veiller à ce qu'ils aient accès aux services de protection sociale et à leurs droits fondamentaux[25]. Plus que jamais, les États subissent de multiples pressions pour numériser et renforcer leurs systèmes d'enregistrement des faits d'état civil et de statistiques de l'état civil et à les relier à l'identité nationale pour consolider leur rôle de « *registre fondateur au centre d'un écosystème des identités* »[26]. Le Centre d'excellence sur les systèmes d'enregistrement et de statistiques de l'état civil (ESEC) a, entre autres, proposé que les systèmes d'ESEC « *serv[ent] de fondement à un écosystème de l'identité plus étendu sur lequel d'autres pièces d'identité sont délivrées* »[27] et que les systèmes d'identification nationaux soient reliés aux systèmes d'ESEC « *soit en intégrant les deux systèmes de manière organique, soit en créant deux systèmes distincts sur le plan fonctionnel, mais interopérables*[28]*.* » Selon la Banque mondiale, « *les systèmes d'ESEC robustes reliés à des systèmes de gestion des identités et adaptés aux contextes locaux constituent le fondement de tous les secteurs et piliers de l'économie et contribuent à la*

[19] Voir note 1.
[20] https://www.un.org/fr/universal-declaration-human-rights/index.html.
[21] https://www.ohchr.org/FR/ProfessionalInterest/Pages/CCPR.aspx.
[22] https://unstats.un.org/legal-identity-agenda/.
[23] https://sustainabledevelopment.un.org/sdg16.
[24] Stratégie des Nations Unies pour une identité juridique pour tous, *Concept note developed by the United Nations Legal Identity Expert Group*, 2019, https://unstats.un.org/legal-identity-agenda/documents/UN-Strategy-for-LIA.pdf.
[25] Division de la statistique de l'ONU, *Handbook on civil registration, vital statistics and identity management systems : Communication for development*, https://unstats.un.org/legal-identity-agenda/documents/Final-CRVS-Handbook.pdf.
[26] Secure Identity Alliance, *Civil Registry Consolidation Through Digital Identity Management*, 2015, https://secureidentityalliance.org/publications-docman/public/7-15-12-17-civil-registry-consolidation-digital-identity-sia-final/file.
[27] Centre d'excellence sur les systèmes ESEC, *Recueil de bonnes pratiques pour relier les systèmes d'enregistrement et de statistiques de l'état civil (ESEC) et les systèmes de gestion de l'identité, 2019,* https://crvssystems.ca/sites/default/files/assets/files/CRVS_Compendium_f_WEB.pdf.
[28] Centre d'excellence sur les systèmes ESEC, *Établissement d'un lien entre les systèmes d'identification nationaux et les systèmes ESEC : Un impératif du développement inclusif*, 2019, https://crvssystems.ca/sites/default/files/inline-files/CRVS_Gender_2.3_ID_f.pdf.

réalisation des objectifs de développement durable pour que la pauvreté cesse et que chacun ait une vie prospère[29]. » Les travaux du Centre d'excellence sur l'identité, le commerce et l'économie numériques, fondé par la Commission économique des Nations Unies pour l'Afrique, attestent aussi de l'existence d'approches politiques visant à renforcer le rôle des systèmes d'ESEC dans les systèmes d'identification nationaux. L'un des domaines d'intérêt essentiels du centre est de soutenir l'harmonisation des systèmes d'enregistrement des faits d'état civil et d'identification numérique et d'appuyer « *la mise en œuvre d'une stratégie globale pour l'identification, le commerce et l'économie numériques en Afrique*[30]. »

L'organisation non gouvernementale Privacy International a appelé l'attention sur toute une série de projets concernant l'identité numérique qui sont encouragés par la volonté de réaliser l'ODD 16.9 et ne se limitent pas à la création de systèmes d'enregistrement des naissances[31]. Ainsi, les pouvoirs publics et l'industrie mettent actuellement en œuvre de multiples programmes et initiatives qui créent des impératifs stratégiques de numérisation de l'identité juridique et de création d'identités juridiques « numériques » par des « systèmes d'identification numérique »[32]. L'attrait que suscite, notamment grâce aux éléments de langage, l'assimilation de l'identité juridique à un « identifiant numérique » dans le but de renforcer la protection sociale – notamment l'inclusion financière –, la croissance de l'économie numérique et même la sécurité constitue pour de nombreux gouvernements un argument puissant, et les pressions exercées pour permettre l'utilisation de l'identité juridique sous la forme d'une « identité numérique » et le développement des systèmes de gestion de l'identité numérique sont fortes. Ainsi, dans un article sur ID4Africa, les Nations Unies affirment que « *l'identité juridique est un droit humain fondamental* », dans le contexte du développement des « *écosystèmes identitaires autour de l'identité numérique au service du développement, de l'action humanitaire, de la sécurité et de la facilitation*[33]. » Dans sa stratégie de transformation numérique pour 2020-2030, l'Union africaine s'appuie également sur l'ODD 16.9 et souhaite que « *99,9 % de la population africaine ait une identité légale numérique dans le cadre d'un processus d'enregistrement des actes d'état civil d'ici à 2030* », affirmant aussi que l'Afrique a une opportunité à saisir, celle d'adopter des solutions numériques comme élément moteur d'«*une croissance innovatrice, inclusive et durable »*[34]*. De même, s'exprimant sur les conditions du développement de l'économie numérique, le groupe de travail Union africaine-Union européenne sur l'économie numérique affirme que « la majorité des citoyens africains n'ont pas de documents d'identification émis par le gouvernement, ce qui les empêche d'accéder aux services publics et privés essentiels* »[35], et souligne « *les opportunités de création de valeur à travers la mise en place de l'identification numérique* », tout particulièrement dans des contextes transfrontaliers[36].

Dans un rapport de 2007, l'UNESCO laisse entrevoir qu'« *un identificateur mondial unique semblerait être la solution pour attribuer à une personne une existence numérique dans la*

[29] Banque mondiale, *Strengthening CRVS and national ID*, 2017, http://documents.worldbank.org/curated/en/306621510673094647/pdf/AUS16865-revised-public.pdf.
[30] https://www.uneca.org/fr/dite-africa/pages/quelle-est-la-voie-%C3%A0-suivre-pour-mettre-en-%C5%93uvre-renforcer-dite-en-afrique.
[31] Privacy International, *The Sustainable Development Goals, Identity, and Privacy: Does their implementation risk human rights?*, 2018, https://privacyinternational.org/long-read/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk.
[32] Banque mondiale, Rapport sur le développement dans le monde 2016, *Spotlight 4. Enabling Digital Development: Digital Identity,* http://documents.worldbank.org/curated/en/896971468194972881/310436360_20160263021000/additional/102725-PUB-Replacement-PUBLIC.pdf.
[33] *UN Legal Identity Agenda - ID4Africa 2019 Toolkit: Legal Identity for All*, https://unstats.un.org/legal-identity-agenda/documents/UN%20LIA%20ID4Africa%20Digital%20Toolkit-final.pdf.
[34] Union africaine, *Stratégie de transformation numérique pour l'Afrique (2020 -2030), 2020,* https://au.int/sites/default/files/documents/38507-doc-dts_-_french.pdf.
[35] Robert Viola, Directeur général de DG Connect, Commission européenne, *Putting the Digital Economy at the heart of EU-Africa cooperation, 2020,* https://ec.europa.eu/digital-single-market/en/news/africa-europe-alliance-european-commission-and-african-union-commission-welcome-digital-economy.
[36] Banque mondiale et Partenariat mondial pour l'inclusion financière, *G20 Digital Identity Onboarding, 2018,* https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf.

Société de l'information »[37] et que cela contribuerait à la stabilité des services financiers et des mesures de lutte contre les cyberattaques par exemple. Toutefois, le rapport met aussi en garde contre le risque qu'un tel identificateur mondial unique ne signe la fin de l'anonymat.

L'émergence de technologies d'identification numérique toujours plus intrusives et les capacités des plates-formes d'identification sur lesquelles s'appuient les initiatives de numérisation de l'identité juridique conduisent à la chosification de l'« identité juridique » telle qu'elle est perçue à travers la DUDH et les actions de développement menées au niveau mondial. Ainsi, les sociétés spécialisées dans l'identification numérique commencent à parler de l'« identité juridique » comme d'« *un droit humain fondamental* », comme d'un impératif découlant de l'ODD 16.9. Il est du reste inquiétant de constater que l'« identité » est aussi présentée comme un « *bien marchand facilement accessible* » pour lequel « *un nouvel écosystème d'applications diverses se crée naturellement* »[38]. Par ailleurs, MasterCard a récemment rejoint le partenariat sur l'identité ID2020 et s'est dit convaincu que « *l'identité numérique est un droit humain fondamental* »[39]. La chosification de l'identité juridique à travers une « identité numérique » dans la vie privée comme dans la sphère publique, et la création de systèmes d'identification numérique qui ambitionnent de donner effet à un « droit à l'identité » offrent une abondante matière à réflexion. Les systèmes d'identification numérique sont en plein essor et intègrent de plus en plus souvent des mesures de type biométrique (empreintes digitales, image de l'iris, etc.) ou des attributs comportementaux numériques[40] qui servent à créer et à vérifier une « identité numérique »[41].

« *L'expansion de l'identité numérique, de la gouvernance électronique et de la technologie biométrique a rapidement accru l'intérêt et les investissements des gouvernements, des partenaires au développement et des acteurs du secteur privé pour les systèmes d'identification*[42]. »

2.2 Biométrie et identité numérique : des corps informationnels

Par biométrie, on entend généralement une méthode automatisée de reconnaissance des individus à partir de leurs caractéristiques physiques ou comportementales. Diverses sources s'accordent à voir dans les technologies biométriques un « *moyen d'identifier spécifiquement chaque être humain* », en tant que personne physique, grâce à la conversion des attributs uniques d'une identité physique en une identité numérique, en un « identifiant numérique »[43]. Ces technologies sont vues, et cela est problématique, comme un moyen de créer « *une vérité unique et universelle concernant le corps en tant qu'identité* »[44] et comme une « *source de*

[37] UNESCO, Programme Information pour tous, *Étude sur les implications éthiques des nouvelles technologies*, 2007, http://www.unesco.org/new/fr/communication-and-information/resources/publications-and-communication-materials/publications/full-list/ethical-implications-of-emerging-technologies-a-survey/.
[38] Thales, « Legal identity: A proxy for inclusion », https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/legal-identity.
[39] « MasterCard joins ID2020 Alliance », https://mastercardcontentexchange.com/newsroom/press-releases/2020/may/mastercard-joins-id2020-alliance/.
[40] Université d'Exeter et Coelition, *Building Digital identities. The challenges, risks and opportunities of collecting behavioural attributes for new digital identity systems*, 2017, http://socialsciences.exeter.ac.uk/media/universityofexeter/collegeofsocialsciencesandinternationalstudies/lawimages/research/Buiding_Digital_Identities_with_Behavioural_Attributes.pdf.
[41] Telefonica, *New paradigms of Digital Identity. Authentication and Authorization as a Service*, 2016, https://www.wholesale.telefonica.com/en/information-centre/multimedia/new-paradigms-of-digital-identity-authentication-and-authorization-as-a-service/.
[42] Centre d'excellence sur les systèmes ESEC, Recueil de bonnes pratiques pour relier les systèmes d'enregistrement et de statistiques de l'état civil (ESEC) et les systèmes de gestion de l'identité, https://crvssystems.ca/sites/default/files/assets/files/CRVS_Compendium_f_WEB.pdf.
[43] UNESCO, Programme Information pour tous, *Étude sur les implications éthiques des nouvelles technologies*, 2007, http://www.unesco.org/new/fr/communication-and-information/resources/publications-and-communication-materials/publications/full-list/ethical-implications-of-emerging-technologies-a-survey/.
[44] Rao et Greenleaf, « Subverting ID from above and below: The uncertain shaping of India's new instrument of e-governance », 2013, https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/India_ID.

PROJET NON DESTINÉ À PUBLICATION

vérité objective et vérifiable concernant nos identités »[45]. En cherchant à transformer « *les surfaces et les caractéristiques d'un corps en un ensemble de codes et de cryptages numériques "lisibles" par machine* »[46], les technologies biométriques « *changent de manière irrévocable la relation entre le corps et l'identité* »[47]. Elles modifient aussi la relation de pouvoir entre l'État et le citoyen. L'identité biométrique lisible par machine détermine automatiquement le statut de l'individu, avec pour conséquence qu'il peut donc se voir refuser la participation et l'accès aux opportunités et aux services que le système d'identification numérique fondé sur la biométrie est censé fournir.

En 2007, Wickins soutenait que « *l'essence même d'un système biométrique est l'exclusion : ceux qui ne possèdent pas les identifiants corrects se voient refuser l'accès à ce que le système protège*[48]. » Cette analyse souligne bien la nécessité d'examiner, sur le plan social et politique et au niveau de la modélisation, la nature excluante de ces technologies biométriques, et d'étudier les postulats sous-jacents selon lesquels le corps est une source objective de vérité concernant l'identité qui peut, de façon générale, être reproduite et rendue lisible par machine à tout moment et pour tous les individus et tous les groupes. Cette réflexion a toute son importance dans le contexte des systèmes d'identification numérique nationaux qui s'appuient sur la biométrie pour vérifier les identités et sont susceptibles de causer de multiples préjudices. Ces systèmes pourraient notamment conduire à l'exclusion de certaines personnes et de certains groupes ~~pour diverses raisons non négligeables~~. Certains pourraient craindre ~~, craignant~~ que les systèmes d'identification biométrique ne soient utilisés contre eux et ~~, pourraient~~ refuser de s'y inscrire avec pour conséquence de ne pas avoir ~~, et, ce faisant, n'auraient pas~~ accès aux protections et aux services que ces systèmes sont censés apporter[49]. D'autres pourraient être exclus parce qu'ils ne seraient~~ont~~ pas en mesure d'enregistrer leurs caractéristiques biométriques ou de les faire valider par le système ultérieurement. Par exemple, il peut être impossible d'enregistrer certaines empreintes digitales ou de les vérifier en tant qu'identifiant biométrique unique, en raison d'une maladie de peau[50] ou parce qu'elles sont trop usées[51]. De même, des anomalies de l'iris, une maladie des yeux[52] ou une chirurgie oculaire, voire l'âge peuvent compromettre l'enregistrement et l'utilisation ultérieure d'un iris en tant qu'identifiant biométrique unique et comme moyen de vérifier l'identité biométrique de l'utilisateur[53].

La technologie, les choix de conception et la stratégie qui préside à ces choix peuvent avoir de lourdes conséquences pour les personnes, ne pas tenir suffisamment compte de leurs droits fondamentaux et les mettre en danger, en particulier si leur corps ou leur comportement ne correspond pas à une vision prédéfinie de l'identité. Dans une résolution de 2011, le Conseil de l'Europe exprimait la crainte que la large portée de la technologie biométrique, son

[45] Martin et Whitley, « Fixing identity? Biometrics and the tensions of material practices », 2013, http://personal.lse.ac.uk/whitley/allpubs/MCS2013.pdf.
[46] Irma van der Ploeg, « The Illegal body: 'Eurodac' and the Politics of biometric identification », 1999, https://link.springer.com/article/10.1023/A:1010064613240.
[47] Groupe de travail « Article 29 » sur la protection des données, *Avis 3/2012 sur l'évolution des technologies biométriques*, 2012, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_fr.pdf.
[48] Wickins, « The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification », 2007, http://newton.ee.auth.gr/biometrics/images/docs/ethics.pdf.
[49] Hindustan Times, « Assam to introduce biometric tracking for suspected illegal immigrants », 2019, https://www.hindustantimes.com/india-news/assam-to-introduce-biometric-tracking-for-suspected-illegal-immigrants/story-WPXUBWRm4EPapkiTktxQTP.html, et Data & Society, *Digital Identity in the Migration & Refugee Context: Italy Case Study*, 2019, https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf.
[50] Drahansky *et al.*, « Influence of Skin Diseases on Fingerprint Recognition », 2012, https://www.hindawi.com/journals/bmri/2012/626148/.
[51] L'association mondiale des opérateurs de téléphonie mobile, GSMA, a signalé qu'au Kenya, dans le cadre d'un programme de protection sociale, les personnes âgées et les travailleurs manuels n'ont pas pu apporter la preuve de leur identité (appelée « preuve de vie » dans le programme) parce que leurs empreintes digitales n'étaient plus lisibles par le scanner biométrique. GSMA, *Opportunities for Improving Digital Identification in Social Cash Transfers*, 2020, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/04/SCT_Report_R_WebSingles.pdf.
[52] Aslam *et al.*, « Iris recognition in the presence of ocular disease », 2009, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2659699/.
[53] Voir *The Wire*, « Unable to Verify Fingerprints or Iris, Aadhaar Denies Leprosy Patients Basic Services », https://thewire.in/government/unable-verify-fingerprints-iris-aadhaar-denies-leprosy-patients-basic-services.

PROJET NON DÉFINITIF

évolution rapide et son utilisation à des fins multiples ne portent atteinte à certains droits de l'homme essentiels[54]. L'organisation attirait l'attention sur le fait que la législation d'un pays peut ne pas refléter de façon appropriée la technologie lorsqu'elle est utilisée et la nécessité de sauvegarder les droits de l'homme, et appellait les États membres à réviser sans tarder leur législation en matière de protection des données. En outre, la résolution appelait les Parties à promouvoir le respect de la proportionnalité dans l'adoption des technologies biométriques et à *« évaluer les risques potentiels pour les droits de l'homme et les libertés fondamentales qui pourraient découler de l'utilisation de la biométrie »*. Il est à noter qu'en 2018, le Haut-Commissaire des Nations Unies aux droits de l'homme a lui aussi fait une mise en garde, soulignant que « *la création de bases de données biométriques de masse soulève d'importantes préoccupations touchant aux droits de l'homme* » et qu'il est inquiétant de constater que certains États semblent adopter ce type de mesures sans avoir mis en place des garanties juridiques et procédurales adéquates[55]. Depuis l'adoption de la résolution en question, la Convention 108 modernisée du Conseil de l'Europe (Convention 108+)[56] et, au niveau de l'Union européenne, le Règlement général sur la protection des données (RGPD) et la directive « police »[57] considèrent désormais que les « données biométriques » sont une catégorie spéciale de données qui exige un niveau élevé de protection des personnes contre les effets néfastes de leur utilisation.

À ce jour, 142 pays environ ont adopté une législation en matière de protection des données[58]. Or ces législations ne stipulent pas toutes expressément que les données biométriques doivent être réglementées. Par ailleurs, ces 142 pays n'ont pas tous mis en place des autorités de supervision pour veiller à la bonne application de ces législations ou contribuer à « *garantir, pour tout individu, des recours effectifs en cas de violation de ses droits et libertés fondamentales* »[59]. Les données de la Banque mondiale montrent que 168 pays environ ont mis en place des systèmes d'« identifiant national ». Sur ces systèmes, 159 environ sont classés dans la catégorie « système d'identifiant numérisé », et parmi ceux-ci, 103 environ recueillent des données biométriques sous la forme d'empreintes digitales ou d'image de l'iris[60]. Mais peut-on affirmer que tous les pays qui adoptent des systèmes d'identification numérique nationaux reposant sur la biométrie ont mis en place des lois et des garanties juridiques adaptées en matière de protection des données qui soient fondées sur les droits de l'homme ? Cette question revêt une importante toute particulière, car « *avec la diminution rapide du coût de la technologie biométrique et la promotion – par les sociétés mondiales et les donateurs tels que la Banque mondiale – de l'utilisation de cette technologie dans les pays en développement, de plus en plus de pays incluent la totalité de leur population dans des programmes de biométrie*[61]. »

PROJET NON DESTINÉ À ÊTRE CITÉ

[54] Conseil de l'Europe, Résolution 1797 (2011), « La nécessité de mener une réflexion mondiale sur les implications de la biométrie pour les droits de l'homme », http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-fr.asp?fileid=17968&lang=fr.

[55] *Le droit à la vie privée à l'ère du numérique. Rapport du Haut-Commissaire des Nations Unies aux droits de l'homme, août 2018, https://undocs.org/A/HRC/39/29.*

[56] Au paragraphe 58 du Rapport explicatif sur la Convention 108+, les données biométriques sont considérées comme étant des « données résultant d'un traitement technique spécifique de données relatives aux caractéristiques physiques, biologiques ou physiologiques d'un individu qui permet l'identification ou l'authentification uniques de ce dernier » et leur traitement « est également considéré comme ayant un caractère sensible lorsqu'il est précisément utilisé pour identifier de façon unique la personne concernée. » https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726.

[57] Voir le site d'information de la Commission européenne, « Protection des données dans l'UE », qui fournit des informations sur le règlement général sur la protection des données et sur la directive « police » ainsi que des liens vers ces instruments, https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_fr.

[58] Greenleaf et Cottier, « 2020 ends a decade of 62 new data privacy laws », janvier 2020, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3572611.

[59] Résolution 1797 (2011) du Conseil de l'Europe.

[60] Banque mondiale, Identification For Development (ID4D) Global Dataset, 2018, https://id4d.worldbank.org/global-dataset.

[61] Kloppenburg et Ploeg, « Securing Identities: Biometric Technologies and the Enactment of Human Bodily Differences », 2018, https://www.tandfonline.com/doi/full/10.1080/09505431.2018.1519534.

On notera qu'au Maroc, en août 2019, la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), qui est l'autorité marocaine chargée de la protection des données, a interdit l'utilisation de la reconnaissance faciale pour une durée de sept mois. Prenant en considération le volume croissant de la jurisprudence sur l'identité numérique et les aspects relatifs au respect de la vie privée, la CNDP a fait valoir que « *l'informatique est au service du citoyen et évolue dans le cadre de la coopération internationale. Elle ne doit pas porter atteinte à l'identité, aux droits et aux libertés collectives ou individuelles de l'Homme. Elle ne doit pas constituer un moyen de divulguer des secrets de la vie privée des citoyens*[62]. »

À noter également en Tunisie, en 2018, le retrait d'une proposition et d'un projet de loi relatifs à la mise en place d'une carte d'identité biométrique. Ces faits soulignent le contrôle accru de la proportionnalité et de la nécessité des systèmes d'identification biométrique et de leur incidence sur les droits de l'homme et les libertés fondamentales[63].

Pour les raisons évoquées ci-dessus, le traitement des données personnelles et des données biométriques dans des systèmes d'identité numérique devrait être explicitement réglementé par les législations nationales qui prennent en compte, dès le début, leur impact et les risques pour les droits de l'Homme et adoptent des sauvegardes appropriées.

3. Scénarios de mise en place de l'identité numérique

3.1 Systèmes d'identification nationaux

De plus en plus de pays envisagent ou adoptent des systèmes d'identification nationaux centralisés au motif qu'ils sont nécessaires pour offrir à l'État et à ses citoyens de multiples avantages : protection sociale, accès aux services publics, efficacité et transparence des pouvoirs publics, renforcement du commerce transfrontalier, migration, sécurité, et contribution à la réalisation des objectifs de l'économie numérique. Le plus souvent, ces systèmes consistent avant tout à créer un numéro d'identification national unique et une identité unique. L'identité numérique nationale comprend non seulement des données démographiques comme la date de naissance, le nom complet et l'adresse de la personne, mais aussi, de plus en plus, ses empreintes digitales, une image de son iris et une empreinte faciale, et parfois son origine ethnique.

Les systèmes d'identification nationaux sont de plus en plus souvent le résultat de pressions exercées pour que soit créée une « identité juridique pour tous », en vue de réaliser l'ODD 16.9 des Nations Unies ou des objectifs de l'économie numérique nationale ou régionale. Dans sa Stratégie de transformation numérique pour l'Afrique (2020-2030), l'Union africaine (UA) souligne que *« l'identification numérique constitue un mécanisme clé pour promouvoir le concept des Nations Unies d'"identité juridique pour tous" »* et que *« les individus qui n'ont pas d'identité juridique ont des difficultés à faire valoir leurs droits, y compris leurs droits de citoyenneté.* » L'UA précise que « *la modernisation et l'urbanisation rapides des sociétés africaines, ainsi que la sophistication croissante des transactions commerciales, augmentent le besoin d'identification juridique. Une carte d'identité est nécessaire pour obtenir des services de santé, des certificats fiscaux, des documents de voyage, ouvrir des comptes bancaires, exercer une franchise, établir un crédit, etc.*[64] » L'identifiant numérique national est vu comme la numérisation de l'identité, comme l'unique identification de l'individu, et comme

[62] CNPD, Délibération nº D-194-2019 du 30 août 2019 relative à un moratoire sur la reconnaissance faciale, https://www.cndp.ma/images/deliberations/deliberation-n-D-194-2019-30-08-2019.pdf.
[63] Access Now, « Biometric ID vs. privacy: Tunisians win on privacy! But it's not over yet. », 2018, https://www.accessnow.org/biometric-id-vs-privacy-tunisians-stood-privacy-not-yet/.
[64] Union africaine, *Stratégie de transformation numérique pour l'Afrique (2020 -2030)*, 2020, https://au.int/sites/default/files/documents/38507-doc-dts_-_french.pdf.

PROJET NON DESTINÉ À ÊTRE CITÉ

une « composante essentielle » de l'économie numérique. L'attrait de l'« identifiant numérique » semble être pour les États désireux de doper l'économie numérique une occasion unique à ne pas manquer. À titre d'exemple, le McKinsey Global Institute a entrepris une analyse sur le Brésil, la Chine, l'Éthiopie, l'Inde et le Nigéria, et a récemment indiqué que les programmes d'identification numérique pourraient entraîner une augmentation du PIB comprise entre 3 % à 13 % à l'horizon 2030[65]. Pour les pays qui cherchent à réduire la pauvreté et à offrir à tous des opportunités, cette perspective est très prometteuse.

Les systèmes d'identification nationaux sont vus comme des systèmes d'identification fondateurs couvrant l'ensemble de la population et qui peuvent de plus en plus chercher à s'appuyer~~ant~~ sur les systèmes officiels d'enregistrement et de statistiques de l'état civil (ESEC). L'enregistrement auprès de~~de~~ l'état civil est un événement important dans la vie d'une personne ; il établit son~~l'~~ identité ~~de la personne~~ depuis sa naissance en consignant des informations essentielles sur elle (date et lieu de naissance, nom, informations sur les parents)~~,~~ et lui confère une identité juridique. Les systèmes d'ESEC servent aussi à enregistrer des événements essentiels ultérieurs de la vie personnelle : changement de nom, mariage, divorce, décès, etc. Ils sont un moyen fondateur qui permet à la personne d'apporter à l'État la preuve de son identité et de sa situation de famille et leur importance ne peut pas être surestimée. Des efforts croissants sont déployés pour numériser ces systèmes dès le recueil de données à la naissance, en vue de renforcer leur rôle dans la gestion des identités et intensifier l'utilisation d'« *identifiants uniques de certificat de naissance* » dans les systèmes d'identification nationaux[66]. La numérisation de l'enregistrement des naissances est un point jugé essentiel à la généralisation de cet acte officiel et à la diffusion des avantages qu'il procure. Cela encourage les États à adopter des systèmes d'enregistrement numérique des naissances au moyen, par exemple, de la téléphonie mobile[67]. De plus en plus, o~~O~~n considère que les systèmes d'ESEC constituent l'élément central des systèmes d'identification numérique[68], et leur numérisation renforce ce rôle fondamental. Ce que l'on constate est que p~~P~~olitique globale[69] et technologie se rencontrent pour créer une identité numérique unique qui suit les individus du berceau à la tombe[70].

Si les mesures de centralisation des systèmes d'identification nationaux et d'incorporation des données d'ESEC, voire de numérisation de l'enregistrement des naissances, partent assurément d'une bonne intention, elles présentent cependant des risques pour les personnes et les groupes. L'un des risques majeurs est que ces systèmes peuvent exclure et marginaliser ceux qui ne peuvent pas apporter la preuve de leur identité juridique parce qu'ils ne figurent dans aucun registre d'état civil et qu'ils ne sont pas en mesure d'apporter cette preuve par d'autres moyens. De même, la numérisation générale des systèmes d'enregistrement des naissances risque d'exclure des personnes et des ~~les~~ groupes déjà marginalisés[71] qui n'ont pas accès aux infrastructures numériques (même celles reposant sur la téléphonie mobile), et de creuser les inégalités. Ces systèmes numérisés pourraient

[65] McKinsey, *Digital identification: A key to inclusive growth*, avril 2019, https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20identification%20A%20key%20to%20inclusive%20growth/MGI-Digital-identification-Report.ashx.
[66] Banque mondiale et Organisation mondiale de la Santé, *Global Civil Registration and Vital Statistics: Scaling up Investment Plan 2015-2024*, 2014, https://www.worldbank.org/content/dam/Worldbank/document/HDN/Health/CRVS%20Scaling-up%20plan%20final%205-28-14web.pdf.
[67] GSMA, *Innovations in Mobile Birth Registration: Insights from Tanzania and Pakistan*, 2017, https://www.gsma.com/mobilefordevelopment/programme/digital-identity/innovations-in-mobile-birth-registration-insights-from-tanzania-and-pakistan/.
[68] Banque mondiale, *Identification For Development (ID4D) Integration Approach*, 2015.
[69] Nations Unies, *Lancement du Programme des Nations Unies relatif à l'identité juridique : une approche globale de l'enregistrement des faits d'état civil, des statistiques de l'état civil et de la gestion de l'identité. Rapport du Secrétaire général*, 2019, https://digitallibrary.un.org/record/3841896.
[70] GSMA, *Roadmap for Digital Birth Registration: Identity for every child through the power of mobile*, 2018, https://www.gsma.com/mobilefordevelopment/resources/roadmap-for-digital-birth-registration-identity-for-every-child-through-the-power-of-mobile/. « En tant qu'enregistrement officiel et permanent de l'identité d'un enfant, l'enregistrement des naissances peut contribuer à donner accès à un certain nombre de services essentiels tels que les soins médicaux et les vaccinations, l'éducation et les prestations sociales. »
[71] Plan International, *Identifying and addressing risks to children in digitised birth registration systems. A step-by-step guide,* https://www.ohchr.org/Documents/Issues/Children/BirthRegistrationMarginalized/PlanInternationalGeneva_4.pdf.

POUR COMMENTAIRE PUBLIC

accentuer les fractures numérique, sociale et économique, et refuser à certains l'accès aux soins de santé, à l'éducation, au logement et à d'autres prestations sociales et droits essentiels qui dépendent de la capacité des personnes à présenter une identité numérique nationale. ~~-~~

Les personnes qui ne peuvent pas présenter leur « identité juridique » ou dont le corps n'est pas compatible avec certains systèmes biométriques technologiquement limités qui ne pourrait pas être « lu par une machine » pourraient se voir refuser la représentation en justice ou le bénéfice des services que les systèmes d'identification nationaux sont censés appuyer. Il est essentiel que les systèmes d'identification nationaux prennent dûment en compte les réalités humaines et les droits de l'homme, et qu'ils soient pensés en fonction de ces réalités et de ces droits, afin de limiter~~,~~ entre autres, les risques d'exclusion, de discrimination ou d'atteinte à la vie privée et à l'identité de la personne. Parmi les pays qui mettent en œuvre ou renforcent ces systèmes, beaucoup sont signataires de traités internationaux en matière de droits de l'homme qui leur imposent de respecter, de réaliser et de protéger les droits fondamentaux, notamment le droit à la vie privée et le droit à la reconnaissance de la personnalité juridique, et de veiller à ce que ces droits s'appliquent sans discrimination fondées sur la race, la couleur, la langue, la religion ou l'origine nationale ou sociale[72]. Toute ingérence dans l'exercice de ces droits doit avoir un fondement juridique clair dans la législation et « *poursuivre un but légitime [et être] nécessaire et proportionné à ce but*[73]. »

Certains systèmes d'identification numérique ont été interdits ou limités dans leur usage parce que l'humain n'avait pas été privilégié au stade de la conception et que les droits de l'homme n'étaient pas pris en compte au niveau politique, juridique et technique. De fait, l'obligation impérieuse de prendre en considération les droits de l'homme « dès la conception » figure dans plusieurs instruments relatifs à la protection des données. Ainsi, l'article 1er de la Convention 108+ du Conseil de l'Europe énonce que le but de ce traité est de « *protéger toutes les personnes physiques, quelles que soient leur nationalité ou leur résidence, à l'égard du traitement des données à caractère personnel, contribuant ainsi au respect de leurs droits de l'homme et des libertés fondamentales, et notamment de leur droit à la vie privée*. » Plus loin, l'article 10 impose que les responsables du traitement, et le cas échéant les sous-traitants, doivent procéder, « *préalablement au commencement » de tout traitement, « à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées* » et « *doivent concevoir le traitement de données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et libertés fondamentales*[74]. » De même, le Règlement général sur la protection des données de l'UE (RGPD) a pour but de protéger les « *libertés et droits fondamentaux des personnes physiques, et en particulier leur droit à la protection des données à caractère personnel*[75] ». Le RGPD exige des organisations qu'elles examinent les risques que présente le traitement des données à caractère personnel pour les libertés et droits des personnes, et qu'elles adoptent une approche de protection des données dès la conception et de protection des données par défaut.

Exemples de systèmes qui ont été interdits ou ~~dont l'usage a été~~ limités par des cours sur la base de considérations touchant aux droits de l'homme ci-dessous.

[72] Article 14 de la Convention européenne des droits de l'homme, https://www.echr.coe.int/Documents/Convention_FRA.pdf ; article 7 de la Déclaration universelle des droits de l'homme, https://www.un.org/en/universal-declaration-human-rights/ ; article 26 du Pacte international relatif aux droits civils et politiques, https://www.ohchr.org/FR/ProfessionalInterest/Pages/CCPR.aspx.
[73] A. Beduschi, « Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights », 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3419039.
[74] https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726.
[75] Voir https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A02016R0679-20160504.

3.1.1 Kenya : le système national d'identification numérique « Huduma Namba » et son examen par les instances judiciaires

Dans les années 1980, le Kenya a mis en place une carte nationale d'identité (*national ID Card*). Comme dans bon nombre de pays, cette carte fait office d'identité fonctionnelle et elle est nécessaire ou exigée pour accéder à certains services publics ou privés. Il faut même parfois prouver son identité (au moyen de cette carte ou d'un passeport) pour accéder à un bureau ou entrer dans un bâtiment officiel. Mais « *du fait de la pratique coloniale persistante consistant à ne reconnaître que 42 tribus indigènes sur l'ensemble des groupes ethniques présents au Kenya, certains rencontrent des difficultés à déposer leur demande de document d'identité nationale, notamment les Somalis, les Nubiens, les Shonas, les Massaïs, les Teso et les Arabes*[76]. » Depuis longtemps, il est indispensable au Kenya de posséder une carte nationale d'identité pour acheter un téléphone portable, voter ou bénéficier de la plupart des services publics[77]. Ceux qui n'en possèdent pas sont plus marginalisés que les autres et subissent davantage de discriminations.

En 2019, le Gouvernement kényan a décidé de mettre en place un identifiant numérique national pour remédier aux problèmes causés par la multiplicité des systèmes d'identification indépendants en vigueur à l'époque. L'objectif était de créer une source de vérité unique concernant l'identité des personnes en instaurant un Système national intégré de la gestion de l'identité (NIIMS, *National Integrated Identity Management System*). Le NIIMS avait pour but « *de créer et d'exploiter un registre national de la population qui soit une source unique d'information sur les citoyens kényans et les ressortissants étrangers résidant dans le pays*[78]. » Outre l'enregistrement obligatoire de toute une série de données démographiques, le NIIMS devait aussi contenir un ensemble de mesures biométriques (y compris l'ADN) ainsi que les coordonnées GPS du domicile. Une fois enregistrée dans le NIIMS, la personne devait recevoir un numéro d'identification unique appelé « *Huduma Namba* »[79]. Dans le système proposé, l'enregistrement dans le NIIMS était obligatoire et de plus indispensable pour bénéficier des services publics essentiels.

Mais en l'absence de véritable consultation publique, l'*Huduma Namba* n'est pas parvenu, sur le plan politique, juridique et technologique, à résoudre et à prévenir les problèmes de discrimination et de marginalisation créés depuis longtemps par la carte nationale d'identité. En février 2019, l'Huduma Namba a été contesté sur le plan juridique au motif qu'il portait atteinte aux droits constitutionnels que sont le respect de la vie privée, l'égalité et la non-discrimination[80]. L'affaire a été entendue par la Haute Cour du Kenya en avril 2019. Tout en autorisant la poursuite de la collecte de données biométriques, et dans l'attente d'un jugement ultérieur, la Cour a décidé que l'enregistrement dans le système NIIMS n'était désormais plus obligatoire et que l'accès aux services publics ne pouvait pas être refusé aux personnes non enregistrées. La Cour a également mis fin à l'obligation de faire enregistrer son ADN et les coordonnées GPS de son domicile[81]. Cependant, malgré cette décision favorable, le système de l'Huduma Namba risquait toujours d'accroître la marginalisation et la discrimination des individus et des communautés.

PROJET NON DESTINÉ À ÊTRE CITÉ

[76] Caribou Digital, « Kenya's Identity Ecosystem », 2019, https://www.cariboudigital.net/wp-content/uploads/2019/10/Kenyas-Identity-Ecosystem.pdf.
[77] *ibid.*
[78] Justice Initiative, *Kenya's National Integrated Identity Management Scheme (NIIMS)*, 2020, https://www.justiceinitiative.org/publications/kenyas-national-integrated-identity-management-scheme-niims.
[79] National Government Communications Centre, *Brochure NIIMS*, 2019, https://www.hudumanamba.go.ke/wp-content/uploads/2019/03/NIIMS-BROCHURE-suggested-edits.pdf.
[80] Namati, « Case Filed to Stop New Digital ID Register in Kenya », 2019, https://namati.org/news-stories/case-filed-stop-new-digital-id-system-kenya/.
[81] Privacy International, « Civil society achieves change, but risks still remain in Kenya's new biometric ID system », 2019, https://privacyinternational.org/news-analysis/2774/civil-society-achieves-change-risks-still-remain-kenyas-new-biometric-id-system.

Une seconde audience s'est donc tenue en septembre 2019 devant la Haute Cour du Kenya. Cette dernière a rendu sa décision en janvier 2020[82], portant un coup d'arrêt à la mise en place de l'*Huduma Namba*, aux motifs suivants :

- *« les données biométriques et à caractère personnel figurant dans le NIIMS ne doivent être traitées que s'il existe un cadre juridique approprié intégrant des garanties suffisantes pour protéger les droits fondamentaux » ;*
- la mise en place du NIIMS ne pourra se poursuivre *« qu'à la condition qu'un cadre réglementaire régissant la mise en œuvre du NIIMS, complet, approprié et conforme aux exigences constitutionnelles en vigueur identifiées dans le présent arrêt soit mis en place» ;*
- *« le recueil de l'ADN et des coordonnées GPS aux fins de l'identification est intrusif et non nécessaire. »*

Le cas[83]~~'affaire~~ de *l'Huduma Namba* est une bonne illustration des excès qui guettent les systèmes nationaux d'identification numérique et de l'absence d'évaluation et de prise en compte des droits de l'homme dans les exigences politiques, juridiques, technologiques et de gouvernance de ces systèmes. Il~~Elle~~ soulève une fois de plus la question de l'identité par qui et pour qui, et la nécessité de veiller à ce que ~~souligne l'obligation de bâtir d~~les systèmes d'identité numérique ~~qui~~ soient inclusifs et bâtis sur le respect et la protection des ~~fs. C'est une leçon édifiante qui nous rappelle l'absolue nécessité de respecter et de sauvegarder les~~ droits de l'homme et des libertés fondamentales.

3.1.2 Jamaïque : l'identifiant numérique national

Dans un arrêt de 2019, la Cour suprême de Jamaïque a déclaré « *inconstitutionnelle, nulle, non avenue et de nul effet* », la loi intitulée *National Identification and Registration Act* (loi sur l'identification nationale et l'enregistrement national) ou loi NIRA[84]. Cette loi portait création d'un système d'identification national (NIDS) rendant obligatoire le recueil de données biométriques dans l'ensemble de la population jamaïcaine et leur stockage dans une base de données centralisée, et attribuant à chaque citoyen un numéro d'identification national unique.

Pour justifier sa décision, la Cour a fait valoir que « *le caractère obligatoire de la disposition et la portée de cette dernière ainsi que l'absence d'un droit de ne pas participer ne sont ni justifiés ni justifiables dans une société libre et démocratique*. » La Cour a également redéfini le concept juridique de vie privée en Jamaïque. Après avoir examiné diverses jurisprudences internationales relatives à l'identité nationale et au respect de la vie privée, elle a déclaré que « *la vie privée, telle qu'on l'entend aujourd'hui, présente au moins trois aspects : vie privée de la personne, protection des informations à caractère personnel et confidentialité du choix. Ces différents aspects existent non pas parce qu'ils sont conférés par l'État, mais parce qu'ils appartiennent à tous les êtres du simple fait qu'ils sont humains*. »

Dans son arrêt, la Cour apporte des éclaircissements sur l'application d'exceptions aux droits de l'homme et à l'inférence touchant à ces droits. Elle analyse par le détail ce qui peut être jugé proportionné et nécessaire dans la mise en place du système national d'identification numérique proposé pour atteindre l'objectif légitime de l'État dans une société démocratique. L'analyse de la proportionnalité et les « éléments de proportionnalité » fournissent des orientations très utiles aux États qui cherchent à mettre en place un système national d'identification numérique. Par exemple, dans la recherche de l'élément nécessaire de proportionnalité, la Cour suprême de Jamaïque a fait valoir que toute mesure empiétant sur

[82] http://kenyalaw.org/caselaw/cases/view/189189/.
[83] *Nubian Rights Forum et autres c. Attorney General*
[84] *Robinson c. Le Procureur général de Jamaïque*, https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf.

un droit doit être « *soigneusement conçue pour atteindre l'objectif visé* » et « *doit le moins possible porter atteinte au droit ou à la liberté en question.* » Et même si « *un objectif est suffisamment important et que les deux premiers éléments du test de proportionnalité sont satisfaits, il est encore possible que, du fait de la gravité des effets délétères de la mesure sur des individus ou des groupes d'individus, celle-ci ne soit pas justifiée par les objectifs qu'elle est censée servir.* » Comme dans l'affaire de l'*Huduma Namba*, cet arrêt montre bien qu'il est important d'évaluer l'incidence des systèmes d'identification numérique sur les droits de l'homme et sur la discrimination et la marginalisation. Il facilite l'interprétation de l'application des articles 11 (Exceptions et restrictions) et 10 (Obligations complémentaires) de la Convention 108+.

Il est à~~encourageant de~~ noter que, également en l'absence de politique nationale ou de considération des droits de l'homme dans la règlementation dans les systèmes d'identité numérique, le Centre for Internet and Society (CIS) a élaboré une grille d'évaluation pour la gouvernance des systèmes d'identification numérique[85]. Cette grille peut aider à identifier les conséquences de ces systèmes sur la vie privée, la surveillance, la marginalisation et la discrimination. Le CIS l'a déjà appliquée à une étude de cas, en l'occurrence l'*Huduma Namba*[86]. Ce type d'approche pourrait être utile à l'élaboration de bonnes pratiques pour la prise en compte des droits de l'homme dès la conception dans les systèmes d'identification numérique.

La publication d'un « Guide to Litigating Digital Identity System [87]» par l'ONG Privacy International est aussi intéressant à noter. Ce guide reflète une série de cas de jurisprudence sur des problèmes posés par des systèmes d'identité numérique et leurs conséquences négatives sur les droits de l'homme. Il est pensé comme une aide apportée aux groupes et à la société civile dans leurs actions pour que les systèmes d'identité numérique respectent les droits de l'homme et les libertés fondamentales, y compris sur les sujets de la nécessité et de la proportionnalité de ces systèmes.

Les problèmes juridiques évoqués ci-dessus, ainsi que l'engagement actif de la société civile, démontrent qu'il est nécessaire d'élaborer une méthodologie d'évaluation de l'impact sur les droits de l'homme (AIHR). Cela pourra aider à garantir que les droits de l'homme soient correctement pris en compte dans l'élaboration des politiques et dans les technologies et la gestion des systèmes d'identité. Une approche basée sur l'AIRH pourrait en particulier permettre l'identification et la réduction des risques et des dommages pour ceux « *qui pourraient être les plus vulnérables, le plus marginalisés et les plus discriminés* [88]».

3.2 Identité numérique et enregistrement de carte SIM obligatoire

Nous sommes plusieurs milliards dans le monde à utiliser un téléphone portable et à passer par les réseaux mobiles pour téléphoner, envoyer des sms et surfer sur internet. Nous avons besoin pour cela d'une carte SIM (*Subscriber identity module*). Sans SIM (ou eSIM)[89], il n'est pas possible d'utiliser un téléphone portable pour passer des appels, envoyer des sms ou accéder à internet sur un réseau d'opérateur mobile. Les opérateurs utilisent la carte SIM pour

[85] Voir https://cis-india.org/internet-governance/blog/governing-id-a-framework-for-evaluation-of-digital-identity.
[86] The Centre for Internet & Society, *Governing ID: Kenya's Huduma Namba Programme, 2020*, https://cis-india.org/internet-governance/digital-id-kenya-case-study.

[87] Privacy International, (2020) A Guide, Identity Systems: An Introduction https://privacyinternational.org/report/4156/guide-litigating-identity-systems-introduction

[88] Götzmann, (2019), The Danish Institute for Human Rights, Handbook on Human Rights Impact Assessment https://www.researchgate.net/institution/The_Danish_Institute_for_Human_Rights
[89] Voir Nubian Rights Forum et autres c. Attorney General https://www.gsma.com/esim/

authentifier les abonnés et contrôler leur accès aux réseaux et aux services mobiles, ce qui n'est pas sans incidences notables sur l'identité numérique et les droits de l'homme de milliards de personnes dans le monde.

Une carte SIM est rattachée à deux principaux identifiants : l'IMSI (*International mobile subscriber identity*), identifiant électronique unique stocké dans la carte SIM associé à un numéro de téléphone portable, qui permet au réseau mobile d'identifier et d'authentifier la carte SIM ; et l'ICCID (*Integrated circuit card identifier*), numéro imprimé généralement sur la face externe de la carte SIM. L'ICCID est le numéro de série unique mondialement qui identifie la carte SIM elle-même. Il contient également le numéro d'identification de l'abonné chez l'opérateur du réseau mobile et permet de garantir que les services consommés sont bien facturés.

Les identifiants de la carte SIM, associés à l'identifiant électronique unique du terminal portable[90], sont enregistrés généralement par les opérateurs de réseau mobile lorsque l'on passe ou reçoit un appel. C'est ce qui constitue les statistiques d'appel d'une personne et permet de tracer en détail son comportement et ses habitudes, notamment sur les réseaux sociaux[91]. Ces identifiants mobiles uniques rattachés au compte et au service[92] servent de plus en plus à créer des identités numériques – y compris biométriques – liées à des personnes. Dans de nombreux pays, l'identité numérique mobile est rattachée à l'identité civile et au numéro national d'identité, ce qui risque de créer les bases d'une surveillance pouvant avoir de lourdes conséquences en matière de droits de l'homme, d'autant que l'utilisation de ces identifiants comme identité numérique échappe au contrôle des personnes concernées.

Nous subissons une série de pressions socioéconomiques et politiques qui nous poussent à utiliser des téléphones et des services mobiles devenus nécessaires ou essentiels (surtout en période de crise) et que les stratégies et initiatives de l'économie numérique cherchent à encourager. Lors du Sommet Connect Africa tenu à Kigali en 2007, le Président rwandais Paul Kagame a déclaré qu'en « *dix ans seulement, le téléphone portable, qui était auparavant considéré comme un luxe et un privilège, est devenu totalement indispensable en Afrique, aussi bien en ville qu'à la campagne* »[93]. Une étude menée auprès de consommateurs au Royaume-Uni montre que les services internet et de téléphonie mobile sont jugés essentiels à différents égards[94]. Pour certains groupes, notamment les réfugiés, le fait d'avoir un téléphone portable compte parfois autant que de pouvoir boire et se nourrir[95], car cela peut être un moyen de protection indispensable[96], une véritable bouée de sauvetage[97].

D'après la Global Mobile Trade Association (GMSA), on compte actuellement dans le monde 5,2 milliards d'abonnés uniques aux services mobiles[98], c'est-à-dire 5,2 milliards de cartes SIM mobiles avec plusieurs identités numériques uniques qui, dans de nombreux cas, peuvent être liées officiellement à des identifiants nationaux ou fonctionnels, notamment un

[90] Connu sous l'acronyme IMEI (« international mobile equipment identity » ou « identité internationale d'équipement mobile ») ; la GSMA délivre les IMEI et les conserve dans sa base de données mondiale (https://imeidb.gsma.com/imei/index#) ; voir également, GSMA IMEI Services https://www.gsma.com/services/gsma-imei/
[91] Wikipedia, entrée sur les statistiques d'appel, https://fr.wikipedia.org/wiki/Statistiques_d%27appel
[92] GSMA, (2018), « Data attributes as the new digital identity currency » https://www.gsma.com/identity/wp-content/uploads/2018/03/Data-Attributes-as-the-New-Digital-Identity-Currency-deck-FINAL.pdf
[93] *The New Times*, (2007) « ICT no longer luxury for Africans – Kagame » https://www.newtimes.co.rw/section/read/1640
[94] OFCOM, (2014) « Mobile and internet services now 'essential' to consumers » https://www.ofcom.org.uk/about-ofcom/latest/media/media-releases/2014/essential-comms-services
[95] The Conversation, 2019, « For young refugees, a mobile phone can be as important as food and water when arriving in a new country » https://theconversation.com/for-young-refugees-a-mobile-phone-can-be-as-important-as-food-and-water-when-arriving-in-a-new-country-122077
96 Latonero *et al.*, *Data & Society*, (2019) « Digital Identity in the Migration & Refugee Context: Italy Case Study » https://datasociety.net/wp-content/uploads/2019/04/DataSociety_DigitalIdentity.pdf
[97] HCR, (2016) « CONNECTING REFUGEES: How Internet and Mobile Connectivity can Improve Refugee Well-Being and Transform Humanitarian Action » https://www.unhcr.org/uk/news/latest/2016/9/57d7d4478/mobile-connectivity-lifeline-refugees-report-finds.html
[98] GSMA Intelligence, https://www.gsmaintelligence.com/data/

numéro de carte nationale d'identité ou un numéro de passeport[99]. Il arrive de plus en plus fréquemment dans bon nombre de pays que l'on soit tenu légalement pour obtenir une carte SIM mobile de fournir une preuve de son identité civile qui peut inclure le numéro national d'identité unique et de la faire enregistrer. Les dispositions législatives concernant l'enregistrement des données d'utilisateurs des cartes SIM imposent aussi parfois l'enregistrement d'éléments biométriques, y compris d'images faciales[100], pour obtenir un simple téléphone portable. Ces politiques réglementaires offrent les bases d'un suivi et d'une surveillance de masse qui passent par différentes dimensions de l'activité mobile liée à une identité mobile numérique, par exemple, les services monétaires mobiles.

3.3 Enregistrement des données d'utilisateurs de cartes SIM mobiles, services monétaires mobiles et confidentialité des transactions

D'après la GSMA, en janvier 2020, **environ 155 pays** avaient adopté des lois relatives à l'enregistrement obligatoire des données d'utilisateurs de cartes SIM qui empêchent d'obtenir une carte SIM mobile ou d'accéder aux services mobiles sans preuve officielle d'identité civile. Ces dispositions créent d'abord un obstacle majeur pour ceux qui ne possèdent pas de justificatifs d'identités reconnus par les autorités. Cela les prive d'accéder aux services mobiles et, par conséquent aux services publics et exacerbe les inégalités et la discrimination. En l'absence de lois énonçant objectivement la nécessité et la proportionnalité des mesures d'enregistrement des données d'utilisateurs de cartes SIM, mais aussi en l'absence de protections juridiques adéquates, y compris de loi sur la protection des données reflétant la Convention 108+, l'enregistrement de ces données risque d'interférer avec le droit au respect du caractère privé des communications, le droit à une identité et au développement personnel et le droit de communiquer de manière anonyme (comme aspect du droit à la liberté d'expression)[101]. L'enregistrement des données d'utilisateurs de cartes SIM soumet les personnes à la surveillance de leur identité numérique dans de multiples dimensions de leurs activités mobiles connectées.

Certains gouvernements, ajoutant une pression politique pour s'assurer du respect de la loi relative à l'enregistrement des données d'utilisateurs de cartes SIM et limitant ainsi l'espace privé et d'autres droits fondamentaux, ont ordonné aux opérateurs de téléphonie mobile de désactiver les cartes SIM des personnes qui ne se soumettent pas à l'obligation d'enregistrer une identité civile reconnue par l'État[102]. Des millions de personnes peuvent se voir refuser l'accès au réseau mobile pour cette raison et être privées de l'économie numérique et des services publics nécessitant un téléphone mobile, ainsi que de leur droit à la liberté d'expression[103], par exemple. Dans certains pays, les organismes de réglementation ont infligé de lourdes amendes aux opérateurs de téléphonie mobile n'ayant pas respecté les

[99] Il est peu probable que le chiffre de 5,2 milliards corresponde au nombre d'abonnés uniques ; cela correspond plutôt au nombre de cartes SIM activées uniques, sachant qu'une seule et même personne peut posséder et utiliser plusieurs cartes SIM.
[100] Radio Free Asia, (2019) « Chinese Telecoms Companies Confirm Mandatory Facial Recognition For New Numbers » https://www.rfa.org/english/news/china/facial-recognition-12052019162028.html
[101] Voir, par exemple, l'arrêt *Breyer c. Allemagne* (2020) de la Cour européenne des droits de l'homme sur l'enregistrement et le stockage de données d'utilisateurs de cartes SIM prépayées, https://hudoc.echr.coe.int/eng-press#{"itemid":["003-6624862-8792771"]}. Il convient de noter en particulier dans cette affaire l'opinion dissidente du juge Ranzoni (page 44) qui a marqué son désaccord avec l'avis majoritaire de la Cour, affirmant que l'enregistrement des données relatives aux utilisateurs de cartes SIM n'était pas proportionné au but légitime poursuivi et constituait par conséquent une violation de l'article 8 (droit au respect de la vie privée). Il est probable que ce point soit revu dans la CEDH.
[102] Par exemple, après les instructions émises par la Tanzania Communications Regulatory Authority, environ 3 millions de cartes SIM ont été désactivées, les personnes en leur possession n'étant pas titulaires de cartes nationales d'identité ni de passeport comme l'exige la loi relative à l'enregistrement des données biométriques d'utilisateurs de cartes SIM. Quinze millions de cartes SIM supplémentaires vont être désactivées (https://www.theeastafrican.co.ke/business/Tanzania-to-switch-off-sim-cards/2560-5437128-ws8o5nz/index.html). À Myanmar, des millions de personnes verront leurs cartes SIM désactivées si elles n'enregistrent pas un document d'identité valable d'ici le 30 juin 2020 (https://www.mmtimes.com/news/millions-myanmar-risk-having-mobile-phones-cut-after-sim-registration-deadline.html). De même, au Ghana, le gouvernement prévoit de désactiver les cartes non enregistrées avec un justificatif d'identité d'ici juin 2020 (https://www.moc.gov.gh/meet-press-statement).
[103] Article 19, (2020) « Tanzania: SIM card deactivation poses a significant threat to freedom of expression » https://www.article19.org/resources/tanzania-sim-card-deactivation-poses-a-significant-threat-to-freedom-of-expression/

exigences gouvernementales pour les cartes SIM[104]. Cette situation risque en outre d'inciter les personnes qui ne disposent pas des justificatifs d'identité civile nécessaires reconnus par l'État à se tourner vers le marché noir pour se procurer une carte SIM et, dès lors, à se mettre en infraction. Dans une décision de la Cour suprême de la Jamaïque, les juges présidant la Cour ont mis en garde contre le fait que « *le pouvoir coercitif ultime de l'État ne serve à garantir le respect des règles* » par des mesures relatives à l'identité[105], comme c'est le cas avec l'enregistrement obligatoire des données d'utilisateurs de cartes SIM au niveau national.

Martin (2019) examine de quelle manière les plateformes monétaires mobiles, qui jouent un rôle crucial en Afrique pour faciliter les prêts, les paiements et les transferts d'argent, exploitent les données d'utilisateurs de cartes SIM pour mieux connaître les clients et effectuer les vérifications requises. L'enregistrement des données liées à la carte SIM, en plus des données du terminal mobile et des opérations effectuées facilite la surveillance des utilisateurs de services monétiques mobiles[106]. Cette surveillance cachée peut être effectuée par des établissements financiers ou par des opérateurs mobiles qui fournissent eux-mêmes des services financiers sous une licence de services monétiques mobiles. Dans un tel contexte, les possibilités d'échapper à la surveillance de l'État et de structures privées et de jouir d'un droit à la confidentialité des transactions sont de plus en plus réduites. Cela soulève des questions de transparence effective[107] pour les utilisateurs de services monétaires mobiles, d'efficacité de la protection juridique et de surveillance dans plusieurs domaines réglementaires, d'autant que certains pays n'ont pas nécessairement de cadres en vigueur de protection des données et de la confidentialité ni de supervision réglementaire indépendante. Selon Martin, il est particulièrement préoccupant que « *des organismes gouvernementaux aient manifesté un vif intérêt pour des formes plus invasives de surveillance réglementaire en accédant directement aux données de plateformes monétaires mobiles* ». Bien que cet intérêt ne soit pas nécessairement motivé par des questions de sécurité mais relève plutôt de considérations fiscales, le risque de dérives et d'abus de fonctions reste cependant absent des mesures de protection juridique, réglementaire et technique.

Comme indiqué précédemment, dans 155 pays environ, il est désormais obligatoire de posséder une identité civile et de pouvoir la justifier pour obtenir une carte SIM. Sans preuve d'identité officielle, pas de carte SIM. L'enregistrement des données relatives à la carte SIM lie plusieurs identifiants de SIM et de terminaux mobiles aux identifiants civils et nationaux d'une même personne et aux identifiants utilisés par les prestataires de services monétaires mobiles, afin d'identifier une personne de manière unique et de créer ainsi une *« identité économique* ». Il est avancé que les services d'argent mobile nécessitent une identité économique, définie comme « *une forme d'identité fonctionnelle, car ayant pour objet de permettre l'accès à un ensemble spécifique de services* »[108].

Avec le passage des paiements en espèces aux paiements numériques et le passage à un modèle de paiement via des plateformes[109], l'« identité économique » et la surveillance des opérations facilitées par ces modèles soulèvent de multiples questions quant à la proportionnalité, la nécessité et l'intérêt de lier plusieurs identités, mais aussi à la facilitation

[104] Au Nigeria, l'opérateur de téléphonie mobile MTN a été condamné à payer une amende de 5,2 milliards USD, ramenée à 1,7 milliard USD, à l'issue d'un procès (https://en.wikipedia.org/wiki/MTN_$5.2_billion_fine). En Tanzanie, la Tanzania Communications Regulatory Authority a infligé des amendes de plusieurs millions de shillings tanzaniens à six opérateurs de réseaux mobiles (https://itweb.africa/content/DZQ587VPoxgqzXy2).
[105] Voir la note de bas de page 2.
[106] Martin, A (2019) *Mobile Money Platform Surveillance* https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/12924
[107] Bowers *et al.*, (2017) « *Regulators, Mount Up! Analysis of Privacy Policies for Mobile Money Services* ». Il ressort d'une étude menée sur 54 applications d'argent mobile que 44 % de ces applications n'ont pas de politique de confidentialité et que parmi les politiques de confidentialité existantes, 33 % ne sont pas « rédigées dans les langues les plus couramment utilisées dans les pays concernées » et « 50 % n'indiquent pas à l'utilisateur quelles données sont utilisées et collectées » (https://www.usenix.org/system/files/conference/soups2017/soups2017-bowers.pdf).
[108] GSMA, (2019) *State of the Industry Report on Mobile Money* https://www.gsma.com/sotir/wp-content/uploads/2020/03/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2019-Full-Report.pdf
[109] Ibid.

PRIVILEGED AND CONFIDENTIAL

de la surveillance. En Tanzanie, d'après le règlement adopté récemment sur la procédure d'enregistrement des cartes SIM, si les noms présentés pour le réenregistrement d'une carte SIM diffèrent de ceux détenus par la National Identification Authority, l'opérateur mobile est habilité à vérifier à qui appartient la carte SIM en consultant les transactions mobiles du client – ce que l'on qualifie d'« identité économique »[110]. Le passage aux transactions monétaires par voie numérique et aux plateformes d'argent mobile signifie aussi un changement profond de l'identité numérique et du contrôle de l'utilisateur sur ses identités et sur sa vie privée à titre individuel comme à titre collectif[111].

Certains gouvernements ont proposé des plateformes ou des cadres régionaux d'enregistrement des cartes SIM pour lutter contre la criminalité, ce qui n'a fait qu'exacerber les préoccupations que suscitent les systèmes nationaux d'enregistrement des données d'utilisateurs de cartes SIM en matière de droits de l'homme. En Afrique de l'Est, par exemple, le Kenya, le Rwanda, l'Ouganda et le Soudan du Sud ont étudié la possibilité d'établir un cadre harmonisé d'enregistrement des cartes SIM[112]. En Asie du Sud-Est, l'organisme de régulation des télécommunications de la Thaïlande a proposé que le dispositif national d'enregistrement des cartes SIM soit étendu au Laos, au Cambodge et à Myanmar[113]. L'East African Communications Organisation a constitué un groupe de travail chargé d'élaborer un cadre réglementaire pour la mise en œuvre d'un processus d'enregistrement des cartes SIM dans les États membres de la Communauté de l'Afrique de l'Est[114]. Alors que l'enregistrement des données liées aux cartes SIM au niveau national soulève de multiples inquiétudes quant au rattachement d'identifiants mobiles uniques aux identifiants officiels émis par l'État au niveau national, l'absence de cadres et de règles de protection et de confidentialité des données décidées d'un commun accord et compatible au niveau transfrontalier pour régir l'accès des services répressifs aux données relatives à l'identité et l'utilisation que ces derniers en font, par exemple, rend la situation encore plus problématique.

Comme indiqué précédemment, les identifiants numériques découlant de la loi relative à l'enregistrement obligatoire des données d'utilisateurs de cartes SIM peuvent être rattachés à des identifiants nationaux et autres identifiants fonctionnels, ce qui est susceptible d'aboutir à un identifiant unique mondial. Cela permet d'observer la plupart des aspects de la vie d'une personne passent par les appareils mobiles. Avec cette configuration stratégique d'identification numérique, les angles morts sont rares dans le système de surveillance et il reste peu de place pour l'épanouissement personnel. Le fait que les politiques et les lois nationales relatives à l'identité et/ou les identités connexes obligatoires puissent porter atteinte au droit à la vie privée d'une manière qui érode d'autres libertés a été pointé du doigt dans deux arrêts de Cours suprêmes, en Inde et en Jamaïque.

PROJET – NON FINALISÉ

[110] Voir « Electronic and Postal Communications (Sim Card Registration) 2020 » https://tanzlii.org/content/electronic-postal-communications-sim-card-registration-regulations2020 et https://aloysassociates.co.tz/2020/02/22/the-electronic-and-postal-communications-sim-card-registration-regulations-2020/

[111] Alors que les services financiers numériques permettent une certaine confidentialité par rapport au paiements immédiats en espèces dans le cercle social et familial, comme il a été soulevé par Riley (https://novafrica.org/wp-content/uploads/2019/05/Hiding_loans_in_the_household_using_mobile_money__Experimental_evidence_on_microenterprise_investment_in_Uganda-4.pdf) et Hamdan (https://www.diw.de/documents/publikationen/73/diw_01.c.669402.de/diw_roundup_131_en.pdf), les services financiers numériques peuvent impliquer une surveillance cachée dont les conséquences ne sont pas évidentes au premier abord et échappent au contrôle des utilisateurs.

[112] The Exchange, (2015) « East African Countries Move Closer to Common Sim Registration » https://theexchange.africa/trending/east-africa-countries-move-closer-to-common-sim-card-registration/

[113] ITU News, (2016) « SIM registration: A new Thai model for regional collaboration » https://news.itu.int/sim-registration-a-new-thai-model-for-regional-collaboration/

[114] East Africa Communications Organisation. WG 1: ICTs Policy and Regulatory Frameworks Harmonization. http://www.eaco.int/pages/working-groups

3.3.1 Inde – Système Aadhaar, enregistrement des données d'utilisateurs de cartes SIM, vie privée et libertés

« *Ce n'est pas l'État qui est transparent pour le citoyen, mais le citoyen qui devient transparent pour l'État* »[115].

En 2009, le Gouvernement indien a lancé un programme de protection sociale ayant pour but la délivrance d'un numéro d'identification unique appelé « *Aadhaar* » à tous les résidents du pays[116]. *Aadhaar* a créé une base de données centralisée rattachant un numéro d'identification unique à une grande variété de données démographiques concernant les personnes, notamment leurs éléments biométriques (les dix empreintes digitales, l'image des deux iris et une image faciale)[117]. En Inde, l'enregistrement de la carte SIM est obligatoire depuis environ 2005. Cette procédure contraint les opérateurs mobiles à collecter et enregistrer environ 31 catégories de données personnelles, démographiques et financières et relatives au compte, à la carte SIM et au terminal en plus d'informations biométriques telles que les empreintes digitales et les images de l'iris. Les opérateurs mobiles sont tenus de transmettre les données recueillies à une base de données de l'État.

En 2014, le ministère des Télécommunications de l'Inde a donné la consigne à tous les opérateurs de téléphonie mobile du pays leur demandant de collecter et d'enregistrer le numéro unique « *aadhaar* » de leurs clients dans le cadre du processus d'enregistrement obligatoire des données d'utilisateurs de cartes SIM[118]. En 2017, le ministère a ordonné à tous les opérateurs mobiles de revérifier les comptes clients existants au moyen d'un dispositif de connaissance du client par voie électronique basé sur le système *aadhaar*, et de contrôler les nouveaux clients par ce même processus[119]. Ces consignes et exigences ministérielles ont eu pour effet de rattacher de multiples identifiants personnels, de terminaux mobiles et de comptes au système *aadhaar*, qui devenait de fait à tous les égards à un système d'identification national. On pourrait soutenir que le fait de lier l'enregistrement des données d'utilisateurs de cartes SIM à ce système créé les bases d'une surveillance portant atteinte au droit fondamental à la vie privée, considéré comme un droit constitutionnel dans un arrêt marquant de la Cour suprême de l'Inde de 2017[120]. L'affirmation de la Cour selon laquelle « *la vie privée est […] nécessaire à la fois mentalement et physiquement comme facilitateur des libertés garanties* » et du développement de la personnalité[121] prend tout son sens, étant donné l'importance de la vie privée pour l'épanouissement personnel évoquée dans ce rapport et la façon dont les perceptions de la surveillance peuvent influer sur le comportement et sur l'image de soi et de l'identité.

Le programme *aadhaar* a fait l'objet de diverses contestations judiciaires depuis 2012[122], au motif qu'il était inconstitutionnel. Un recours a abouti à une décision de la Cour suprême en 2018[123], jugeant qu'il était conforme à la Constitution en vertu de la loi relative au système *aadhaar*[124] d'utiliser un numéro d'identification unique pour établir l'identité d'une personne ayant droit à des prestations sociales, par exemple, sous forme de combustible pour la cuisine

[115] Cour suprême de l'Inde, (2018) « Justice Puttaswamy (Retd.) and Anr. vs Union of India and Ors. Writ Petition (Civil) n° 494 of 2012 » https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf
[116] Voir https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html
[117] Voir https://uidai.gov.in/my-aadhaar/about-your-aadhaar.html
[118] Ministère des Télécommunications (2014), Dossier n° 800-09/2010 VAS « *Collecting Aadhaar numbers along with Customer Acquisition Form (CAF) of mobile telephone applications* » *https://dot.gov.in/sites/default/files/doc.pdf*
[119] Voir https://dot.gov.in/sites/default/files/Re-verification%20instructions%2023.03.2017.pdf?download=1
[120] Cour suprême de l'Inde, (2017) « *Justice Puttaswamy (Retd.) and Anr. vs Union of India and Ors* » https://uidai.gov.in/images/Right_to_Privacy.pdf
[121] Ibid.
[122] Voir https://economictimes.indiatimes.com/news/politics-and-nation/chronology-of-aadhaar-case/articleshow/65965443.cms?from=mdr
[123] Cour suprême de l'Inde, (2018) « Justice Puttaswamy (Retd.) and Anr. v Union of India and Ors. Writ Petition (Civil) No 494 of 2012 » https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_26-Sep-2018.pdf
[124] Il était prévu que le programme aadhaar donne effet à la loi encadrant le système aadhaar (fourniture ciblée de subventions, d'avantages et de services financiers et autres) de 2016, modifiée en 2019 après l'arrêt de la Cour suprême (https://uidai.gov.in/images/news/Amendment_Act_2019.pdf).

ou de céréales alimentaires. Il importe toutefois de noter qu'entre autres décisions, la Cour a estimé que le rattachement obligatoire de l'identité liée à l'enregistrement de la carte SIM à une identité unique dans le système *aadhaar* « *n'avait aucun fondement juridique* » *et ne satisfaisait pas « à l'exigence de proportionnalité* » et de nécessité. La Cour a fait valoir que « *l'on ne pouvait exposer la population tout entière au risque d'intrusion dans sa vie privée* » si quelques personnes venaient à « *utiliser les données des cartes SIM de manière abusive* ». Elle a statué que le décret gouvernemental imposant de rattacher les identités *aadhaar* aux identités des abonnés mobiles relevait d'une *« contrainte étatique disproportionnée et déraisonnable* ». Elle a déclaré le décret inconstitutionnel et demandé qu'il soit invalidé.

L'arrêt de la Cour suprême a souligné que « *la simple existence d'un objectif légitime de l'État ne saurait justifier les moyens adoptés* ». La Cour a fait valoir que si l'on rend « *aadhaar* obligatoire pour d'autres activités telles que le transport aérien, le transport ferroviaire… il ne restera quasiment plus de domaine d'activité échappant à la surveillance de l'État, ce qui aura un effet paralysant sur les citoyens », partant du principe que la vie privée est un facteur d'épanouissement personnel.

L'arrêt de la Cour suprême sur le système *aadhaar* illustre l'importance d'adopter une approche fondée sur les droits de l'homme dans l'élaboration des politiques et des technologies et leur application, en veillant à ce que les mesures soient nécessaires et proportionnées au but légitime poursuivi, tout en atténuant les risques pour les droits de l'homme. La Cour a reconnu en outre l'importance d'un régime solide pour la protection des données, observant que *« l'absence de cadres réglementaires ou l'inadéquation des cadres existants a des conséquences sociétales et éthiques et présente un risque permanent que les principes de vie privée, de liberté et d'autres droits fondamentaux soient mal compris, érodés ou dépréciés »*. La Cour a déclaré également que « *l'élaboration de lois strictes sur la protection de la vie privée et l'instauration de garanties peuvent répondre à ou tout du moins apaiser certaines préoccupations associées au programme aadhaar, qui risque de porter gravement atteinte à l'autodétermination informationnelle, à la vie privée individuelle, à la dignité et à l'autonomie* ». Bien qu'un projet de loi relative à la protection des données[125] ait été élaboré en Inde, il demeure nécessaire d'établir une approche stratégique, juridique et réglementaire harmonisée de l'identification numérique pour que les terminaux mobiles servent d'intermédiaire entre différents services réglementés.

3.4 Identité numérique dans les contextes humanitaires : créée par qui et pour qui ?

Les organisations humanitaires et de développement sont de plus en plus nombreuses à adopter des systèmes de gestion de l'identité censés les aider à atteindre des objectifs cruciaux de leurs programmes, que ce soit la fourniture de prestations sociales aux personnes touchées par des crises ou la recherche des familles de réfugiés fuyant la guerre civile. Dans son Manuel sur la protection des données (version actualisée, en anglais), le Comité international de la Croix-Rouge (CICR) reconnaît que ces organisations « *n'ont pas toujours besoin de connaître l'identité civile de personnes* »[126] pour les aider. Dans une démarche louable d'adoption de principes de protection des données bien établis, notamment de minimisation des données et de limitation des finalités, le CICR soutient qu'au lieu de commencer par la question « *qui êtes-vous ?* », les organisations devraient plutôt commencer par se demander : « *que dois-je savoir de cette personne pour lui apporter une aide ou une assistance ?* ». Cette démarche vise également à garantir que le système d'identification adopté et les données utilisées pour l'alimenter et aider les bénéficiaires sont proportionnés, nécessaires et non excessifs pour atteindre un objectif clairement identifié et légitime,

[125] Voir https://www.medianama.com/2020/02/223-joint-parliamentary-committee-consultation-pdp-bill-2019/
[126] Comité international de la Croix-Rouge, (2020) *Handbook on Data Protection in Humanitarian Action – Second Edition* https://shop.icrc.org/handbook-on-data-protection-in-humanitarian-action.html

conformément aux cadres de protection des données tels que la Convention modernisée 108+[127].

On peut se demander dans ce cas quel système d'identité est adéquat et à qui il sert. Deux types de systèmes d'identité sont utilisés généralement dans la majorité des pays[128] :

- un système d'« identité fonctionnelle » qui limite le processus d'identification, d'authentification et d'autorisation à une fin et un service bien définis. Par exemple, une identité fonctionnelle peut servir à accéder à des services de santé ou permettre le versement de prestations sociales ou encore servir à obtenir une inscription sur les listes électorales. Les organisations humanitaires peuvent créer et délivrer une identité fonctionnelle pour permettre aux bénéficiaires d'accéder à des services essentiels ;
- un système d'identité fondamentale qui couvre l'ensemble de la population d'un pays et fait office de système d'identification de portée générale fournissant une preuve d'identité civile officielle acceptable à de multiples fins dans les services publics et privés[129]. Les systèmes d'identification fondamentaux peuvent inclure des systèmes d'identification nationaux, des systèmes d'enregistrement des faits d'état civil et des systèmes d'enregistrement de la population qui peuvent en retour prendre en charge des systèmes d'identité fonctionnelle.

Dans son Manuel sur la protection des données (2020), le CICR indique qu'un certain nombre d'initiatives sont en cours pour développer des systèmes d'identification numérique comme forme d'identité fondamentale pouvant servir d'identité reconnue officiellement et donnant accès aux cartes SIM mobiles, aux comptes bancaires et aux services monétaires mobiles. Un défi essentiel dans le contexte humanitaire consiste à faciliter l'accès à des formes d'identité reconnues légalement qui sont souvent une condition préalable à l'obtention d'une carte SIM mobile ou à l'accès à des services d'argent mobile, par exemple. Le Haut-Commissariat des Nations Unies pour les réfugiés, qui est l'une des organisations humanitaires les plus importantes et les plus influentes au plan mondial, s'est engagé à soutenir l'adoption d'« *une identité reconnue légalement, mais aussi numérique* » pour tous les réfugiés, les rapatriés, les demandeurs d'asile, les apatrides et toutes les personnes déplacées de force. Dans cette optique, le HCR soutient également la mise en place de systèmes d'enregistrement séparé des réfugiés que les gouvernements peuvent « *inclure dans leurs systèmes d'identité nationaux, car cela présente des avantages pour tout le monde »*[130].

Le HCR a adopté une politique sur la protection des données de haut niveau [131] énonçant des principes et des règles pour aider à protéger les données personnelles et la vie privée des bénéficiaires, et qui est développée plus en détail dans des orientations sur la protection des données[132]. Ces orientations tiennent compte des principaux concepts et des définitions des principes de gouvernance et des droits individuels cités dans les cadres européens de protection des données tels que la Convention 108 du Conseil de l'Europe et le Règlement général sur la protection des données de l'Union européenne. Bien que les orientations du

[127] Voir, par exemple, l'article 5 sur la légitimité du traitement, en particulier le paragraphe 40 du Rapport explicatif portant sur l'article 5.
[128] Le rapport se limite aux systèmes d'identité fonctionnelle et fondamentale utilisés par la majorité des pays et ne porte pas sur d'autres types d'identités récents tels que l'identité auto-souveraine (SSI) : https://sovrin.org/faq/what-is-self-sovereign-identity/ Ces nouvelles formes d'identité mériteraient un examen approfondi.
[129] Adapté de Banque mondiale, (2019) *ID4D Practioner's Guide* http://documents.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf et GAFI, *Guidance on Digital Identity* (2020) http://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html
[130] HCR (2018), *UNHCR Strategy on Digital Identity and Inclusion* https://www.unhcr.org/blogs/wp-content/uploads/sites/48/2018/03/2018-02-Digital-Identity_02.pdf
[131] HCR, (2018) *Policy on the Protection of Personal Data of Persons of Concern to UNHCR* https://www.refworld.org/pdfid/55643c1d4.pdf
[132] HCR, (2018) *Guidance on the protection of personal data of persons of concern to the UNHCR* https://www.refworld.org/docid/5b360f4d4.html

HCR ne contiennent pas de partie portant spécifiquement sur « l'identité », elles insistent sur la nécessité de protéger l'identité des personnes concernées, en utilisant par exemple des pseudonymes comme identifiants. Les orientations ne traitant pas expressément de « l'identité », le HCR a élaboré des lignes directrices distinctes sur l'enregistrement et la gestion de l'identité[133], qui préconisent l'utilisation de son écosystème d'enregistrement des populations et de gestion d'identité (PRIMES)[134]. Ce système permet également « *d'aider les États par l'utilisation conjointe de ses outils numériques, y compris ses fonctionnalités biométriques* »[135]. S'il convient de saluer le HCR pour avoir adopté à la fois une politique et des orientations visant à assurer la protection des données personnelles et de la vie privée des bénéficiaires, des études montrent qu'il est nécessaire de revoir la manière dont celles-ci peuvent se traduire concrètement, par des expériences constructives en matière de vie privée pour les communautés que le système d'identification est censé aider.

En 2018, le HCR a mis en œuvre un programme visant à créer « *une base de données unifiée à des fins de protection, de gestion de l'identité, de documentation, de fourniture d'assistance, de statistiques démographiques et, au final, de solutions pour les 900 000 réfugiés, selon les estimations, qui ont fui le Myanmar le Bangladesh par vagues successives de déplacements forcés* »[136]. L'organisation non gouvernementale The Engine Room a mené des recherches récemment et publié une étude sur plusieurs systèmes d'identification numérique utilisés au Bangladesh, en Éthiopie, au Nigéria, au Zimbabwe et en Thaïlande[137]. The Engine Room pose les limites de ses recherches tout en s'efforçant de comprendre l'expérience des systèmes d'identification numérique sous l'angle des personnes concernées, sans pouvoir « *nécessairement extrapoler l'expérience d'une personne par rapport à la norme, même si, à certains moments toutes les personnes interrogées ont vécu un aspect du système de la même manière* ». Le rapport intègre les résultats de recherches menées dans le cadre du système conjoint de vérification d'identité du HCR et du Gouvernement du Bangladesh établi pour fournir une assistance aux réfugiés rohingyas[138]. Le processus de vérification consistait notamment en « *la collecte de trois types de données biométriques : des photographies du visage, les dix empreintes digitales et l'image des deux iris pour les personnes âgées de 13 ans et plus* », et la remise aux réfugiés de cartes d'identité à puce[139].

Dans son rapport, The Engine Room évoque les multiples craintes et inquiétudes que le processus d'identification numérique des réfugiés rohingyas a suscité quant à sa finalité et l'utilisation et la confidentialité des données. Les réfugiés rohingyas ont cru à tort qu'accepter une carte d'identité numérique conduirait à leur rapatriement vers le Myanmar et à la situation même qui les avait incités à fuir leur pays. Cela a poussé nombreux d'entre eux à refuser de s'inscrire sur les registres. Force est de rappeler que la confiance doit être la base même de l'identification numérique et que les organisations devraient s'interroger sur ce qui risque de l'entraver et d'y remédier. Cela nécessite la participation et la compréhension de la communauté, qui devraient être des conditions essentielles des procédures d'identification numérique.

L'étude de The Engine Room a révélé en outre que beaucoup de personnes parmi celles interrogées *« ne savaient pas du tout lire, tandis que d'autres ne lisaient ni l'anglais ni le bengali »*, ce qui, du point de vue de la protection des données, soulève de multiples questions

[133] Voir https://www.unhcr.org/registration-guidance/
[134] HCR, (2017) « Modernizing Registration and Identity Management in UNHCR: Introducing PRIMES » https://www.unhcr.org/blogs/modernizing-registration-identity-management-unhcr/
[135] HCR, (2019) *Displaced and Disconnected* https://www.unhcr.org/innovation/displaced-and-disconnected/
[136] Voir « Joint Bangladesh/UNHCR verification of Rohingya refugees gets underway » https://www.unhcr.org/en-us/news/briefing/2018/7/5b3f2794ae/joint-bangladeshunhcr-verification-rohingya-refugees-gets-underway.html
[137] The Engine Room, (2020) *Understanding the Lived Effects of Digital ID: A Multi-Country Study* https://digitalid.theengineroom.org/assets/pdfs/200128_FINAL_TER_Digital_ID_Report+Annexes_English_Interactive_Edit1.pdf
[138] Note de bas de page 113.
[139] Note de bas de page 114.

et préoccupations. Par exemple, la transparence est la pierre angulaire des lois relatives à la protection des données dans le monde : elle est essentielle pour aider les personnes à comprendre ce que l'utilisation de leurs données pourra leur apporter, mais aussi tous les risques potentiels et les mesures de sauvegarde adoptées pour les atténuer. La transparence est essentielle également pour aider les gens à comprendre la base juridique sur laquelle repose le traitement de leurs données personnelles, la façon dont ces données seront utilisées, leurs droits et les choix possibles liés à cette utilisation et comment les exercer conformément aux cadres internationaux de protection des données et à la politique de protection des données du HCR[140]. Pour assurer une véritable transparence et faciliter la compréhension, les organisations doivent tester l'efficacité des mesures de « transparence ». D'après les autorités chargées de la protection des données dans l'UE, si les organisations « *ne sont pas certaines du niveau d'intelligibilité et de transparence des informations et de l'efficacité des interfaces utilisateurs, des avis, des politiques, etc., elles peuvent les tester, par exemple, au moyen de mécanismes tels que les panels d'utilisateurs et les tests de lisibilité* »[141]. The Engine Room précise également dans son rapport que « *les réfugiés ont montré de faibles niveaux de compréhension de la finalité de la composante biométrique du système d'identification numérique et des conséquences d'une éventuelle fuite de données* ». Reconnaissant le besoin urgent d'aider les réfugiés rohingyas en situation critique et compte tenu du fait que des efforts ont été déployés, semble-t-il, par le biais de leaders communautaires pour améliorer la transparence, l'étude dégage divers enseignements et laisse entendre qu'il est nécessaire de revoir les mesures à prendre en vue d'améliorer la compréhension parmi les réfugiés vulnérables et de légitimer le traitement des données personnelles.

On ne sait pas non plus de manière certaine sur quelle base légitime le HCR s'est appuyé[142] pour inscrire les réfugiés rohingyas dans le système d'identification numérique conjoint du HCR et du Gouvernement du Bangladesh. Comme le souligne The Engine Room dans son étude, les orientations du HCR en matière de protection des données[143] ne prescrivent pas de base légitime sur laquelle s'appuyer, mais laissent de manière ambiguë ces décisions au « *contrôleur des données, assisté par le point focal de la protection des données* ». Les lignes directrices indiquent que, même s'il existe un « besoin de principe » d'assurer une base légitime adéquate, l'« intérêt pratique » du traitement déterminera si celui-ci nécessite ou non le consentement des personnes concernées. Cela étant, et dans une contradiction apparente, elles indiquent en outre que « *compte tenu de la vulnérabilité de la plupart des bénéficiaires et de la nature des urgences humanitaires, bon nombre d'organisations humanitaires ne pourront compter sur le consentement au traitement de la plupart des données personnelles* »[144]. La question suivante se pose alors : sur quelle base « légitime » le HCR et le Gouvernement du Bangladesh se sont-ils appuyés et quelle était la base légitime selon les réfugiés rohingyas ? Ce point est tout particulièrement important d'une part, car le Bangladesh n'a pas de loi sur la protection des données à caractère personnel et la vie privée et d'autre part, car le HCR en tant qu'organisation internationale n'est pas soumis notamment au Règlement général sur la protection des données.

Le présent rapport n'a pas vocation à commenter en détail chaque constat de l'étude citée concernant le système d'identification numérique déployé au Bangladesh par le HCR et le

[140] Il convient de noter que le Bangladesh n'a pas de loi sur la protection des données qui pourrait s'appliquer au traitement des données personnelles ; il est difficile par conséquent de savoir comment les réfugiés rohingyas pourraient exercer leurs droits et faire entendre leurs préoccupations en matière de protection des données.
[141] Groupe de travail sur l'article 29, (2018), *Guidelines on Transparency under Regulation 2016/679* www.ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227
[142] L'article 5(2) de la Convention 108+ exige des organisations qu'elles veillent à ce que le traitement des données personnelles soit effectué sur la base du consentement libre, spécifique, éclairé et non équivoque de la personne concernée ou en vertu d'autres fondements légitimes prévus par la loi. L'article 5(4) exige aussi que les données à caractère personnel soient traitées loyalement et de manière transparente, collectée pour des finalités explicites et déterminées, adéquates, pertinentes et non excessives et ne soient pas conservées plus que nécessaire.
[143] Note de bas de page 109.
[144] Note de bas de page 109.

Gouvernement bangladais. Il convient toutefois de noter l'importance de développer un langage commun sur l'identité numérique et sur la participation de la collectivité à l'élaboration de politiques et à la conception et mise en œuvre de systèmes d'identification numérique. L'étude souligne comment ne pas faire participer les personnes concernées peut conduire à des perceptions négatives et à une résistance à l'aide humanitaire et donc déterminer la réussite ou l'échec de l'action menée. L'étude insiste en outre sur les multiples répercussions négatives des programmes d'identification numérique sur la dignité humaine et l'autonomie pour ne citer que celles-ci. Elle devrait être utilement lue par tous les décideurs politiques et toutes les parties à l'écosystème d'« identification numérique pour l'action humanitaire. Elle devrait d'ailleurs servir à éclairer l'élaboration de normes adéquates en matière de protection des données personnelles et de la vie privée ainsi que des droits de l'homme et des libertés connexes, afin de mieux tenir compte du vécu de chacun et de le préserver.

Il est plus que jamais nécessaire d'intégrer le point de vue des communautés et de les faire participer afin que soit mis au point une approche de l'identification numérique centrée sur les droits de l'homme dès la conception et de protéger les droits et libertés, car, comme l'a affirmé le HCR : « *beaucoup d'États, en particulier africains, envisagent […] de plus en plus d'inclure les réfugiés dans les plateformes [nationales] d'identité fondamentale* ». Le HCR suggère en outre que ces efforts d'identification fondamentale déterminent comment faciliter la satisfaction des exigences de connaissance du client lors de l'enregistrement obligatoire des données d'utilisateurs de cartes SIM au niveau national et d'autres services, notamment d'argent mobile[145]. Alors que, dans son rapport sur les personnes déplacées et déconnectées, le HCR ne remet pas en cause directement la justification de l'identité lors de l'enregistrement obligatoire des données liées aux cartes SIM, le rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression a déclaré pour sa part que « *les États devaient s'abstenir de faire de l'identification des utilisateurs une condition d'accès aux communications numériques et aux services en ligne et d'exiger l'enregistrement de données liées à la carte SIM pour les utilisateurs mobiles* »[146].

Dans le résumé général du rapport sur les personnes déplacées et déconnectées, le HCR exprime sa volonté de dialoguer avec un large éventail d'acteurs tels que les gouvernements, les opérateurs de téléphonie mobile, les prestataires de services financiers et les agences humanitaires et de développement. Il ne fait aucune référence en revanche aux représentants des communautés bénéficiaires ni aux organisations non gouvernementales et de la société civile. Il est à espérer que ce n'est là qu'un oubli, car ces groupes sont essentiels pour élaborer des approches inclusives et pour répondre aux préoccupations soulevées dans ce rapport concernant l'enregistrement obligatoire des données d'utilisateurs de cartes SIM et les services d'argent mobile, par exemple.

PROJET

[145] HCR, (2020) *Connectivity for refugess - Displaced and Disconnected*, https://www.unhcr.org/innovation/wp-content/uploads/2019/04/Displaced-Disconnected-WEB.pdf
[146] Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye, A/HRC/29/32, 22 mai 2015. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc

4. Conclusions et éléments de réflexion pour les responsables politiques

Comme nous l'avons vu dans ce rapport, les systèmes d'identification numérique, qu'il s'agisse de systèmes nationaux ou de systèmes fonctionnels, y compris de systèmes hybrides d'identification avec enregistrement des données d'utilisateurs de cartes SIM, peuvent présenter des risques importants pour les droits et les libertés des personnes. Les actions en justice à cet égard ne cessent de mettre en évidence le caractère inconstitutionnel de tels dispositifs et le manque de cadres juridiques et de gouvernance adéquats pour protéger la vie privée et prémunir contre les risques de surveillance, de marginalisation et de discrimination. Le danger existe que l~~L~~es politiques, les lois et la conception de ces systèmes ne soient~~semblent~~ pas ~~être~~ axée~~e~~s sur les personnes qu'ils sont censés servir, mais soient plutôt destinés à créer une seule et unique source de vérité sur les citoyens dans un objectif général de sécurité nationale.

Alors que la jurisprudence dans le domaine porte essentiellement sur les dispositifs d'identification nationaux sous l'angle des droits constitutionnels et fondamentaux des citoyens, nous assistons au développement de systèmes d'identification numérique à l'initiative d'organisations internationales telles que le HCR. Une organisation internationale comme les Nations Unies doit bien souvent traiter et transférer des volumes considérables de données personnelles, y compris des catégories spéciales de données relatives à l'ethnicité ou à la biométrie des bénéficiaires. Compte tenu de leur influence au niveau mondial en faveur d'une identité juridique pour tous (au titre de l'Objectif de développement durable 16.9) et de leur rôle crucial dans la fourniture de l'aide humanitaire et que certains cadres de protection des données tels que le RGPD ne s'appliquent pas aux organisations internationales[147], les Nations Unies devraient envisager d'adopter la Convention 108+ du Conseil de l'Europe et d'y adhérer.[148] S'il est possible que les cadres internationaux de protection des données inspirent les politiques et pratiques de protection des données des organisations internationales, il importe que les obligations des organisations et les droits des personnes soient encadrés de manière claire par la législation et que des droits, protections et voies de recours soient aussi prévus clairement par la loi.

Les systèmes d'identification numérique recouvrent différents secteurs réglementés et nécessitent une approche stratégique, juridique et de gouvernance harmonisée pour garantir une cohérence de l'application des droits de l'homme à l'identité numérique. Il semble nécessaire pour cela de renforcer les capacités des décideurs politiques, des organismes de réglementation, des agences gouvernementles, des organisations humanitaires et de développement et de la société civile en matière de droits de l'homme et d'identification numérique pour éviter la chosification de l'identité numérique en tant qu'un droit de l'homme et pour~~Le but est d'~~ éviter que ~~l'identification numérique ne soit présentée et « venduc » comme un droit de l'homme, mais aussi que notre qualité d'~~ « être humain » ne signifie plus que des humains ~~soit~~ réduit~~se~~ à un ensemble de données corporelles, lisibles par des machines pour définir un profil et entreprendre des actions portant sur les individus et « traités comme de simples objets »[149].

[147] Kuner, C, (2020), *American Journal of International Law*, « The GDPR and International Organizations » *https://www.cambridge.org/core/journals/american-journal-of-international-law/article/gdpr-and-international-organizations/5EDB2AA87AB6BAF9C3731FF3CD0080A9/core-reader*

[148] Greenleaf, G, (2017) « The UN should adopt Data Protection Convention 108 as a global treaty: submission on the 'right to privacy in a digital age' to the UN High Commission for Human Rights » *https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/GrahamGreenleafAMProfessorLawUNSWAustralia.pdf*

[149] Rapport explicatif de la Convention 108+ du Conseil de l'Europe, page 17, Préambule, paragraphe 10 « le préambule mentionne expressément le droit à l'autonomie personnelle, le droit de chacun de contrôler ses propres données à caractère personnel, lequel découle en particulier du droit au respect de la vie privée, ainsi que la dignité de la personne. La dignité humaine requiert la mise en place de garanties lors du traitement des données à caractère personnel, afin que les individus ne soient pas traits comme de simples objets »

Comme l'a souligné la Cour suprême de la Jamaïque dans l'un de ses arrêts, « *toute personne, du simple fait que ce soit un être humain, est sujet de droits* ». Les dispositifs d'identification numérique ne doivent pas négliger l'incidence qu'ils peuvent avoir sur le fait d'« être humain » et le vécu qu'ils sont susceptibles de causer. Pour s'en assurer, il faut élaborer de bonnes pratiques en matière de conception de l'identification numérique respectant les droits de l'homme. Nous recommandons que le Conseil de l'Europe envisage l'élaboration :

- d'une méthodologie d'évaluation de l'impact sur les droits de l'homme pour les systèmes d'identité numérique qui comprenne des critères sur la nécessité et la proportionnalité des systèmes nationaux d'identité numérique ;

- de lignes directrices reflétant les dispositions de la Convention 108+ destinées à aider les décideurs, l'industrie, les développeurs d'applications et les régulateurs à garantir que les systèmes d'identité numérique ne portent pas atteinte aux droits de l'homme et aux libertés fondamentales, et en particulier au droit à la protection des données et à la vie privée, et qu'ils suivent des approches de respect des droits de l'homme dès la conception. De telles lignes directrices pourraient exclure l'usage d'identifiants mondiaux permanents uniques, par exemple, et traiter de la question des choix de systèmes d'identité de base fonctionnels par rapport aux nationaux. Cette orientation devra prendre en compte aussi refléter les développements mobiles ci-dessous.

Il y aurait encore beaucoup à écrire sur le sujet à l'heure où les appels en faveur d'identifiants numériques et de passeports d'immunité internationale sont de plus en plus pressants face à la pandémie de covid-19[150]. Compte-tenu du rôle central que jouent les appareils mobiles dans la vie des personnes et qu'ils sont davantage appelés à jouer dans le cadre de la mise en place de politique de « passeport d'immunité », dans le contexte de la pandémie de covid-19, il convient de prendre note du dépôt de brevet par Apple pour l'utilisation d'un appareil pour « l'émission de documents d'identité contrôlée » (*controlled identity credential release*). Ce dépôt de brevet porte sur un contrôle sur un appareil mobile de documents d'identité tels que permis de conduire, passeport, avec comme argument que « collecter/partager [des documents] devrait être fait seulement après avoir reçu le consentement de l'utilisateur ou sur une base légitime spécifiée par la législation en vigueur »[151]

Il est aussi important de noter que le Bureau fédéral allemand pour la sécurité de l'information (BSI) a récemment annoncé que ses documents d'identité nationaux numériques (eID) pourraient bientôt être enregistrés sur une puce électronique sécurisée sur les téléphones mobiles Samsung.[152] Ces développements et les normes adoptées peuvent aider à renseigner les solutions mobiles d'identités numériques (notamment dans la mesure où l'eID est conçu pour ne pas utiliser un identifiant mondial unique permanent mais un pseudonyme et pour éviter un profilage par les partenaires impliqués).[153]

[150] *The Guardian* (2020) « Surveillance a price worth paying to beat coronavirus, says Blair thinktank ». https://www.theguardian.com/world/2020/apr/24/surveillance-a-price-worth-paying-to-beat-coronavirus-says-blair-thinktank

[151] United States Patent Application 20200320188 (October 8 2020), controlled identity credential release' http://appft1.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=%2Fnetahtml%2FPTO%2Fsrchnum.html&r=1&f=G&l=50&s1=%22020032018 8%22.PGNR.&OS=DN/20200320188&RS=DN/20200320188

[152] SecureIDNews, 07 October 2020, German national digital ID is going mobile https://www.secureidnews.com/news-item/german-national-digital-id-is-going-mobile/ and Samsung Newsroom, 23 July 2020, Samsung, BSI, Bundesdruckerei and Telekom Security Partner to Bring National ID to Your Smartphone https://news.samsung.com/global/samsung-bsi-bundesdruckerei-and-telekom-security-partner-to-bring-national-id-to-your-smartphone

[153] Federal Office for Information Security, (2017) Overview of the German eID system https://ec.europa.eu/cefdigital/wiki/download/attachments/48762401/2017_02_20_German%20eID_01_Whitepaper_final.pdf?version=1&modificationDate=1499172188962&api=v2