



PRINCIPES SUR L'IDENTIFICATION

POUR UN DÉVELOPPEMENT DURABLE



PRINCIPES SUR L'IDENTIFICATION POUR UN DÉVELOPPEMENT DURABLE : VERS L'ÈRE NUMÉRIQUE

ORGANISATIONS SOUTENANT LES PRINCIPES

Agence norvégienne de coopération
pour le développement (Norad)

Banque africaine de développement

Banque asiatique de développement

Bill & Melinda Gates Foundation (BMGF)

Bureau des institutions démocratiques et des droits
de l'homme de l'OSCE (BIDDH)

Center for Global Development (CGD)

Commission économique des Nations Unies pour l'Afrique (CEA)

Digital Impact Alliance (DIAL)

Digital Nations — Canada, Denmark, Estonia, Israel, Mexico,
New Zealand, Portugal, Republic of Korea, United Kingdom,
Uruguay

FHI 360

Fonds des Nations Unies pour l'enfance (UNICEF)

Groupe de la Banque mondiale

Haut-Commissariat des Nations Unies pour les réfugiés (HCR)

ID4AfricaMastercard

Nations numériques

Norwegian Agency for Development Cooperation (Norad)

Omidyar Network

Open Identity Exchange UK/Europe

Organisation des États américains

Organisation internationale pour les migrations (OIM)

Plan international

Privacy and Consumer Advisory Group to the Government
Digital Service and GOV.UK

Programme alimentaire mondial des Nations Unies

Programme des Nations Unies pour le développement (PNUD)

Secure Identity Alliance (SIA)

Smart Africa

The GSMA

Union internationale des télécommunications (UIT)

Union internationale du Notariat

United Nations Capital Development Fund (UNCDF)

Women in Identity

PRINCIPES

INCLUSION

- 1 Garantir un accès universel à toutes les personnes, sans discrimination
- 2 Éliminer les obstacles à l'accès et à l'utilisation

CONCEPTION

- 3 Établir une identité fiable, unique, sécurisée et précise
- 4 Créer une plateforme adaptable et interopérable
- 5 Utiliser des normes ouvertes et éviter la dépendance vis-à-vis des fournisseurs et des technologies
- 6 Protéger la vie privée et permettre le contrôle individuel, grâce à la conception du système
- 7 Planifier la pérennité financière et opérationnelle

GOUVERNANCE

- 8 Protéger les données personnelles, assurer la cybersécurité et protéger les droits des personnes, grâce à un cadre juridique et réglementaire complet
- 9 Définir clairement les mandats institutionnels et le principe de responsabilité
- 10 Faire respecter les cadres juridiques et de confiance, grâce à une supervision indépendante et à l'arbitrage des griefs



OBJECTIF

Toute personne a le droit de participer pleinement à la vie de la société et à son économie et d'être reconnue comme une personne devant la loi¹. Pourtant, près de 1 milliard de personnes dans le monde n'ont pas de preuve d'identité élémentaire, ce qui est essentiel pour protéger leurs droits et leur permettre d'avoir accès égalitaire aux services et aux opportunités². Beaucoup d'autres ont des formes d'identification non sécurisées ou non reconnues et acceptées par les fournisseurs de services, ou vivent dans des pays où les systèmes d'identification sont faibles et inadaptés à l'ère numérique ou qui ne protègent pas les droits et les données des personnes. Combler ce « déficit d'identification » — en améliorant la couverture, la qualité et la gouvernance de systèmes d'identification, qui protègent les droits et facilitent l'accès aux services — est donc essentiel pour l'agenda du développement.

Les organisations qui soutiennent ces Principes sont attachées à un ensemble de valeurs partagées, le but étant de garantir que les systèmes d'identification soient inclusifs, protègent les données et les droits des individus et soient conçus pour contribuer à la réalisation des objectifs de développement.

S'appuyant sur les normes internationales existantes³, les Principes ont été élaborés et publiés pour la première fois en 2017 par un groupe d'organisations, qui se sont engagées à promouvoir le développement de systèmes d'identification inclusifs, fiables, responsables et servant à améliorer la vie des gens et à atteindre les objectifs de développement durable (ODD). Compte tenu de l'évolution rapide du secteur de l'identification, les signataires originaux des Principes se sont engagés à les revoir en vue d'y incorporer de nouveaux points de vue et les enseignements de l'expérience tirés. Cette deuxième édition reflète les contributions issues de ce processus et de consultations publiques élargies.

Les organisations qui soutiennent ces Principes — conformément à leurs mandats, leurs politiques opérationnelles et règles respectifs — les utilisent pour promouvoir une compréhension commune des questions clés et des bonnes pratiques ; susciter une meilleure adhésion des parties prenantes ; orienter les décisions de soutien et de financement ; faciliter les discussions aux niveaux national, régional et/ou mondial ; et œuvrer ensemble pour soutenir les systèmes d'identification qui font progresser le développement économique et social, protègent les droits individuels et humains et ne laissent personne de côté. Nous espérons qu'un éventail de plus en plus large de parties prenantes — y compris les gouvernements, les organisations intergouvernementales, les partenaires de développement, la société civile et les organisations non gouvernementales locales et internationales et les acteurs du secteur privé — se joindront à nous pour appuyer les Principes et les mettre en pratique.

1 Le droit à la reconnaissance devant la loi est inscrit à l'article 6 de la Déclaration universelle des droits de l'homme et à l'article 16 du Pacte international relatif aux droits civils et politiques. Le droit à l'enregistrement des naissances est inscrit dans plusieurs conventions internationales, dont l'article 7 de la Convention relative aux droits de l'enfant.

2 Les estimations de l'ensemble de données ID4D mondial 2018 de la Banque mondiale sont disponibles à : <http://id4d.worldbank.org/global-dataset>

3 Il s'agit notamment des Principes et recommandations des Nations Unies sur l'enregistrement des faits d'état civil et les statistiques de l'état civil, des normes internationales sur la protection des données (telles que le règlement général de protection des données de l'Union européenne et la Convention 108+ du Conseil de l'Europe), des normes mondiales et régionales et cadres de confiance et des Principes de développement numérique.

Définitions et champ d'application

Ces Principes sont destinés à s'appliquer généralement à la création et à l'utilisation de systèmes d'identification⁴ pour faire progresser les objectifs de développement. En raison de leur rôle central dans l'exercice des droits individuels et dans la facilitation de l'accès aux services et prestations de base dans les mondes physique et numérique, **les Principes se concentrent sur les systèmes d'identification « officiels » offerts par les gouvernements ou en leur nom, ou reconnus par eux⁵.**

Bien que chaque pays dispose communément d'une variété unique de systèmes d'identification officiels, qui peuvent différer considérablement quant à leur objectif, leur fournisseur, leur technologie, leur architecture, leur utilisation et leurs modalités de gouvernance, ces systèmes peuvent généralement être catégorisés comme des systèmes d'identification « juridique » ou « fonctionnelle ». Les **systèmes d'identification juridique** constituent une reconnaissance devant la loi et une preuve d'identité juridique. Le nom et la nature des systèmes d'identification juridique varient selon la législation nationale, mais incluent généralement les systèmes de registre d'état civil, les systèmes nationaux d'identification, les registres de population et d'autres systèmes d'identification de base⁶. Les **systèmes d'identification fonctionnelle** fournissent une preuve officielle d'identité et d'autorisation à des fins ou dans des secteurs particuliers. Il s'agit communément des systèmes d'identification qui établissent l'identité des électeurs, les cartes de rationnement, les numéros de sécurité sociale, les cartes de santé, les numéros d'identité fiscale, etc. ; dans certains cas, ces justificatifs peuvent également être reconnus comme preuve d'identité à d'autres fins ou dans d'autres secteurs⁷.

Étant donné la tendance généralisée à la numérisation des économies et des sociétés, les Principes reflètent la nature de plus en plus numérique des systèmes d'identification officiels. Par exemple, beaucoup fournissent des **justificatifs et des services numériques** officiels (tels que des identifiants mobiles, des certificats numériques, des signatures électroniques, etc.) qui permettent une authentification automatisée et à distance pour l'accès aux services et aux prestations, en personne et en ligne. Dans certains cas, les gouvernements ont eux-mêmes construit ces systèmes. Dans d'autres, des pays ont développé des écosystèmes de fournisseurs d'identité numérique qui s'appuient sur les systèmes d'identification officiels existants pour la vérification de l'identité et l'inscription. Dans le cadre d'un modèle d'écosystème fédéré, par exemple, plusieurs entités publiques et/ou privées opérant dans un cadre de confiance peuvent émettre des justificatifs d'identité numériques officiellement reconnus. De plus, les nouvelles architectures et normes d'identité décentralisées créent des possibilités de stockage et de vérification des justificatifs numériques officiels sur les appareils personnels.

Dans le reste du présent document, le terme « système d'identification » est utilisé pour désigner les versions analogiques et numériques des systèmes d'identification officiels décrits ci-dessus.

4 De manière générale, les systèmes d'identification collectent et valident les données d'identité au moyen d'un processus d'enregistrement, puis fournissent aux personnes des identifiants (tels que des certificats, des cartes ou d'autres documents d'identité) qu'elles peuvent utiliser pour s'authentifier ou vérifier des attributs d'identité spécifiques à l'intention d'un tiers qui doit s'appuyer sur leurs revendications d'identité ou d'attribut.

5 Les systèmes d'identification reconnus par le gouvernement sont activés par le cadre juridique d'un pays, auquel ils adhèrent, et sont basés sur un processus de preuve d'identité qui consiste à valider le titulaire, compte tenu des justificatifs émis par le gouvernement et/ou aux registres de source faisant autorité, tels que les systèmes d'enregistrement des faits d'état civil, les systèmes nationaux d'identification ou les registres de population.

6 Les gouvernements conservent la responsabilité ultime de l'identification juridique (voir, par exemple, la Définition opérationnelle officielle de l'identité juridique des Nations Unies, résolution E/CN.3/2020/15 de l'ECOSOC). Bien que la preuve de l'identité juridique — en particulier l'enregistrement de la naissance ou du mariage — soit souvent une exigence pour acquérir la nationalité, l'identification juridique n'a pas besoin d'être liée à la nationalité et ne doit pas être assimilée à un statut juridique ou national. Alors que certains systèmes d'identification juridique (par exemple les systèmes d'identification nationaux) exigent ou constituent une preuve de nationalité, ce n'est pas le cas pour d'autres.

7 Dans le cas des demandeurs d'asile et des réfugiés, bien que les États d'accueil soient principalement chargés de fournir la preuve de l'identité juridique des réfugiés qui n'ont pas de documents de voyage valides, les pièces d'identité délivrées par le Haut-Commissariat des Nations Unies pour les réfugiés dans le cadre de son mandat au nom de l'État d'accueil peuvent être reconnues comme preuve d'identité juridique ou officielle (Convention de 1951 sur le statut des réfugiés, articles 25 et 27 ; Statut de 1950 du Haut-Commissariat des Nations Unies pour les réfugiés).

Pourquoi l'identification est importante pour le développement

Pour les populations, l'identification est un droit, un instrument de protection et une passerelle pour accéder aux services, aux allocations et aux opportunités.

L'importance de l'identification pour les droits des personnes et pour le développement a été reconnue par la communauté internationale grâce à l'adoption de la cible 16.9 des Objectifs de développement durable (ODD) : « d'ici à 2030, garantir à tous une identité juridique, notamment grâce à l'enregistrement des naissances ». Le droit à une identité dès la naissance — garanti par les articles 7 et 8 de la Convention relative aux droits de l'enfant — et à être reconnu comme une personne devant la loi constitue la première étape essentielle pour assurer une protection à vie et est une condition préalable à l'exercice d'autres droits. Une identité juridique est la base sur laquelle les enfants peuvent établir une nationalité, éviter le risque d'apatridie et rechercher une protection contre la violence et l'exploitation. Par exemple, une preuve d'âge est nécessaire pour prévenir le travail des enfants, le mariage des enfants et le recrutement de mineurs dans les forces armées.

En outre, il peut être nécessaire de disposer d'un moyen officiel de prouver son identité pour bon nombre d'interactions, de transactions et de services officiels dans les secteurs public et privé. Par exemple, la vérification de l'identité d'une personne à partir d'une pièce d'identité officielle ou d'un registre officiel est souvent nécessaire pour ouvrir un compte bancaire, voter lors d'une élection, obtenir un emploi dans l'économie formelle, acquérir une nationalité, s'inscrire à l'école, s'inscrire à l'assurance maladie, recevoir une allocation sociale, acheter une carte SIM, enregistrer une propriété, traverser les frontières ou demander un recours judiciaire. L'accélération du mouvement vers les services en ligne et la transformation numérique au niveau des gouvernements et des entreprises signifie que les gens ont également de plus en plus besoin d'un moyen sécurisé et accessible pour prouver leur identité à distance, par exemple sur Internet⁸.

Pour les gouvernements, les acteurs du secteur privé et les autres parties prenantes, il est essentiel d'être en mesure d'identifier de manière fiable les personnes ou de vérifier certains attributs pour offrir des programmes et des services de manière efficace, efficiente et responsable.

Être en mesure de savoir qui sont les gens est essentiel pour un certain nombre de responsabilités gouvernementales, et notamment pour cibler les programmes sociaux et garantir que les personnes appropriées reçoivent des prestations ; intervenir en cas d'urgences, de catastrophes et d'épidémies nécessitant une assistance directe rapide ; procéder au recouvrement des impôts ; réduire la fraude sur les salaires publics ; faciliter une migration sûre et ordonnée ; et, en ce qui concerne l'état civil, produire des statistiques d'état civil pour la planification et le suivi des progrès en matière de développement. Pour certaines entités privées, la vérification de l'identité des clients à

8 Pour ces raisons, l'identification est un catalyseur clé de nombreuses cibles des objectifs de développement durable en plus de la cible 16.9, notamment les cibles 1.3 (mettre en place des systèmes de protection sociale pour tous), 1.4 (faire en sorte que les pauvres et les personnes vulnérables aient le contrôle des terres, des biens et des actifs financiers), 5a (donner aux femmes pauvres l'égalité d'accès aux ressources économiques, y compris le financement), 5b (renforcer l'utilisation de la technologie, en particulier les TIC, pour promouvoir l'autonomisation des femmes), 8.10 (favoriser l'accès universel aux services bancaires et financiers et aux services d'assurance), 10.7 (faciliter la migration et la mobilité de façon ordonnée et responsable), 10c (réduire le coût des transferts de fonds), 12c (éliminer progressivement les subventions carburants nuisibles), 16a (renforcer les moyens de lutte contre le terrorisme et la criminalité), 16.5 (réduire la corruption), et bien d'autres.



un niveau d'assurance donné pour certains services (comme l'ouverture ou l'autorisation d'accès à un compte) est nécessaire pour atténuer les risques, se conformer aux exigences de diligence raisonnable ou de connaissance de son client ou autres réglementations, et pour protéger les clients contre la fraude et le vol d'identité. Lorsque les systèmes d'identification offrent des mécanismes numériques permettant aux individus de s'authentifier à distance dans des contextes en ligne, ils sont également des catalyseurs importants d'une économie numérique inclusive et sous-tendent les plateformes numériques dans tous les secteurs, y compris pour les services en ligne et les systèmes de paiement numérique⁹.

Lorsqu'ils sont conçus et utilisés de manière appropriée, les systèmes d'identification peuvent aider les pays à accélérer le développement inclusif.

Il s'agit notamment d'améliorer la gouvernance et la prestation de services, d'augmenter l'inclusion financière, de réduire les inégalités entre les sexes par l'autonomisation des femmes et des filles et d'améliorer l'accès aux services de santé et aux filets de sécurité sociale pour les personnes vivant dans la pauvreté. Par rapport aux registres papier, l'adoption des technologies numériques peut contribuer à accroître l'exactitude et la fiabilité des données d'identité et des justificatifs, d'automatiser les processus pour réaliser des économies et accroître la commodité, et de fournir de nouvelles plates-formes permettant l'innovation dans la qualité de service. Bien que la technologie numérique présente des risques, la numérisation offre également la possibilité de concevoir de façon intentionnelle des systèmes d'identification plus inclusifs, plus conviviaux et plus protecteurs des droits individuels et des données personnelles, grâce au développement de nouveaux modèles, normes et outils de supervision et de contrôle individuels de la façon dont les données sont utilisées.

⁹ Voir, par exemple, GAFI 2020, Guide sur l'identité numérique, Groupe d'action financière (GAFI), Paris ; Banque mondiale, 2018. "Private Sector Economic Impacts from Identification Systems", Washington; Gelb, A., et Metz, A. 2018. *Identification Revolution: Can Digital ID Be Harnessed for Development?* Washington, Center for Global Development; Gelb, A., et Clark, J. 2013. "Identification for Development: The Biometrics Revolution," Center for Global Development Working Paper 315.

Pourquoi la création de « bons » systèmes d'identification est essentielle pour atténuer les risques

Malgré les possibilités offertes par l'amélioration de l'identification, les systèmes d'identification mal mis en œuvre ou mal utilisés peuvent créer des risques. Ces risques, qui touchent de manière disproportionnée les groupes déjà défavorisés, peuvent être amplifiés par la technologie numérique.

Parmi les principaux risques figurent ceux liés à l'exclusion ou à la discrimination, au manque de protection des données et de la vie privée, ainsi qu'au gaspillage de ressources résultant de systèmes d'identification mal conçus et mal mis en œuvre qui présentent peu d'avantages. Les groupes vulnérables et marginalisés sont souvent les moins susceptibles d'avoir un moyen de prouver leur identité, mais aussi ceux qui ont le plus besoin de la protection et des services liés à l'identification¹⁰. Les personnes qui ne peuvent pas obtenir ou utiliser facilement une pièce d'identité courent donc un plus grand risque d'être laissées pour compte lorsque des exigences d'identification strictes doivent être remplies pour accéder aux services. Sans mesures d'atténuation volontaristes, les systèmes d'identification récemment mis en place ou améliorés peuvent renforcer ou perpétuer les inégalités existantes, les pratiques discriminatoires et les partis pris structurels. Comme d'autres systèmes qui traitent des données personnelles, les systèmes d'identification peuvent également porter atteinte à la protection des données individuelles et aux droits à la vie privée en l'absence de lois et réglementations appropriées, de surveillance et de contrôles et garanties techniques. Les violations de données, l'utilisation ou la surveillance non autorisée, la fraude à l'identité et le détournement de fonction peuvent exposer les individus — en particulier les groupes vulnérables — à de graves risques de préjudice. De plus, les systèmes d'identification sont souvent mis en place selon l'approche « du haut vers le bas » et avec peu de transparence. Associé à de mauvaises pratiques d'achat et à des choix de conception qui gonflent les coûts et conduisent à une dépendance vis-à-vis des fournisseurs et des technologies. Cela peut aboutir à des systèmes qui ne sont pas viables sur le plan opérationnel ou financier et qui ne répondent ni aux besoins des populations ni aux objectifs de développement.

Bien que ces risques soient présents dans tout système d'identification, ils peuvent être amplifiés par la numérisation. En effet, avec les technologies numériques, l'ampleur et les préjudices potentiels liés à la mauvaise gestion ou à l'utilisation abusive des données personnelles sont bien plus importants qu'avec les systèmes sur support papier. De même, l'adoption de technologies tributaires de la connectivité Internet et d'appareils coûteux peut aggraver la fracture numérique et créer de nouveaux obstacles propres à empêcher les groupes déjà marginalisés d'obtenir ou d'utiliser l'identification de manière fiable. Par ailleurs, la vitesse de l'innovation peut inciter à s'attacher à obtenir les dernières technologies plutôt qu'à construire des systèmes adaptés aux objectifs actuels et à même de s'adapter aux besoins futurs. En outre, même si les systèmes d'identification sont numérisés avec succès, il est peu probable qu'ils atteignent leur potentiel sans une

¹⁰ Les groupes particuliers qui risquent le plus d'être exclus par les systèmes d'identification varient selon le contexte, mais comprennent souvent les personnes vivant dans la pauvreté, les femmes et les enfants, les migrants, les réfugiés et les demandeurs d'asile, les résidents éloignés et ruraux, les minorités ethniques, linguistiques ou religieuses et les minorités de genre, les personnes handicapées, les personnes déplacées à l'intérieur du pays, les apatrides, les personnes touchées par un conflit, les travailleurs du secteur informel et d'autres groupes marginalisés ou minoritaires. Voir, par exemple, Banque mondiale, 2019, *Global ID Coverage, Barriers, and Use by the Numbers: An In-Depth Look at the 2017 ID4D-Index Survey*, Washington, Groupe de la Banque mondiale.



numérisation complète – à savoir transformer et repenser les processus pour les moyens numériques – et des investissements complémentaires dans la connectivité Internet, les services en ligne, les plateformes de paiement et autres systèmes numériques.

Pour tirer parti des avantages des systèmes d'identification à l'ère numérique, ces risques doivent être traités par les parties prenantes de manière proactive, généralisée et continue.

Pour mettre en place un système d'identification qui réponde aux objectifs de développement, il convient d'adopter une approche multiforme et multipartite. Pour cela, il convient de définir clairement les finalités et les utilisations prévues du système ; d'adopter, et de doter des ressources nécessaires, des cadres juridiques et réglementaires adéquats qui suppriment les obstacles à l'accès et offrent des garanties et un contrôle suffisants ; de mettre en œuvre des politiques et des pratiques inclusives pour l'enrôlement et l'utilisation du système d'identification ; de suivre une approche centrée sur les personnes et la protection de la confidentialité des données pour la conception et l'évaluation des risques ; et de sélectionner des technologies adaptées au contexte, équitables et accessibles qui garantissent la qualité, la sécurité et l'utilité du système maintenant et à l'avenir. Des échanges continus et transparents avec le public et un ensemble diversifié de parties prenantes tout au long de ces processus sont essentiels pour favoriser la confiance et la responsabilité, et pour garantir que les systèmes d'identification sont conçus pour être utiles aux personnes et contribuer aux réalisations en matière de développement durable.

Principales parties prenantes et leurs rôles

Dans la pratique, l'application des Principes nécessite un effort coordonné et soutenu de multiples parties prenantes qui jouent un rôle essentiel dans la fourniture, l'utilisation, la supervision et le financement des systèmes d'identification officiels :

- **Individus.** Les individus sont au centre des systèmes d'identification, à la fois en tant que personnes concernées par ces systèmes et en tant que bénéficiaires finaux, qui s'appuient sur l'identification pour protéger et revendiquer leurs droits et pour accéder aux services. Ils ont le droit de savoir et d'exercer une supervision et un contrôle appropriés sur la manière dont leurs données personnelles sont collectées, utilisées, stockées, partagées et traitées par des organismes publics et privés, et dans quel but. Il est essentiel de comprendre et de répondre aux besoins et préoccupations des personnes en matière d'identification, de protéger leurs données personnelles et leur vie privée, et d'assurer leur participation à la conception et à la mise en œuvre des systèmes d'identification qui affectent leur vie.
- **Administration publique.** Les services de l'administration nationale et locale sont généralement les fournisseurs d'identité pour les systèmes d'identification juridique (par exemple, l'enregistrement des faits d'état civil et les statistiques de l'état civil, les systèmes nationaux d'identification, les registres de population, les informations d'identification de base, etc.) ainsi que pour de nombreux systèmes fonctionnels, notamment les cartes d'électeur, les identifiants fiscaux et les permis de conduire. D'autres organismes publics et prestataires de services s'appuient sur ces systèmes, et les utilisent pour identifier ou authentifier les personnes avec lesquelles ils interagissent ou qu'ils servent. Les institutions gouvernementales, y compris les parlements et les organes de contrôle, jouent également un rôle essentiel dans la création et l'application de cadres juridiques et réglementaires pour permettre et protéger les systèmes d'identification fournis par les secteurs public et privé. Enfin, des organismes publics participent généralement à l'établissement de normes et à l'élaboration et la supervision de cadres de confiance et d'assurance pour les fournisseurs d'identité, les parties utilisatrices et d'autres parties prenantes dans les écosystèmes d'identité numérique centralisés, fédérés ou décentralisés.
- **Secteur privé.** Les entreprises privées sont des développeurs, des innovateurs et des fournisseurs fréquents de composants et d'infrastructures de systèmes d'identification, et peuvent également être des fournisseurs de services de vérification d'identité et d'authentification. De nombreuses entreprises privées sont également parties utilisatrices, qui dépendent de systèmes d'identification juridique ou autres pour vérifier ou authentifier l'identité de leurs clients (par exemple, pour ouvrir des comptes bancaires ou d'argent mobile). Dans certains cas, les entités du secteur privé sont des fournisseurs d'identité au sein d'un écosystème fédéré ou décentralisé utilisant des justificatifs délivrés par le gouvernement et des registres sources faisant autorité (par exemple, registres d'état civil et systèmes d'identification nationaux) pour créer des justificatifs numériques ou des services d'authentification qui sont acceptés pour accéder en ligne aux services publics (et aux services du secteur privé).

- **Organisations non gouvernementales, organisations communautaires et société civile.** Les organisations non gouvernementales (ONG), la société civile et les organisations communautaires peuvent jouer un rôle essentiel dans la conception et la mise en œuvre des systèmes d'identification, notamment en menant des activités de plaidoyer, en fournissant une protection et une assistance juridique, en sensibilisant la population, en facilitant les consultations communautaires, en dotant les gens des moyens d'accéder aux mécanismes d'identification ou de règlement des plaintes, et en faisant en sorte que les fournisseurs d'identité répondent de leurs actes.
- **Organisations internationales, organismes régionaux et partenaires de développement.** Les organismes intergouvernementaux internationaux, les organismes humanitaires et de développement, les fondations et autres donateurs apportent souvent un soutien aux systèmes d'identification sous forme de financement et d'assistance technique, et soutiennent l'établissement de normes. D'autres organismes internationaux et régionaux participent également à l'établissement de normes liées à l'identification, notamment celles relatives à l'interopérabilité transfrontalière et à la reconnaissance mutuelle des justificatifs d'identité. Dans certains cas, les acteurs du développement et de l'action humanitaire peuvent également être des fournisseurs d'identité ou administrer des systèmes d'identification pour des programmes ou activités spécifiques. Dans le cas des réfugiés et des demandeurs d'asile, le HCR peut fournir une preuve d'identité juridique ou officielle au nom de l'État hôte dans le cadre de son mandat.



PRINCIPES

INCLUSION

1

Garantir un accès universel à toutes les personnes, sans discrimination.

- *Identité juridique pour tous.* Chacun doit pouvoir prouver son identité juridique. Les pays doivent remplir leurs obligations et engagements de fournir une identification juridique à tous les résidents¹¹ — et pas seulement aux citoyens¹² — de la naissance à la mort, conformément au droit international et aux législations nationales¹³. Il s'agit notamment de l'obligation d'assurer l'enregistrement universel des naissances pour tous les enfants¹⁴, ce qui est essentiel pour fournir une preuve d'identité juridique dès la naissance, et l'enregistrement en temps opportun des autres faits d'état civil, tels que les mariages et les décès. Il s'agit également de l'obligation et de l'engagement de fournir une preuve d'identité juridique aux réfugiés, aux apatrides et aux migrants qui n'ont pas de titre valide ou ne peuvent pas prouver autrement leur identité juridique.
- *Non-discrimination.* Tous les systèmes d'identification doivent être exempts de discrimination, dans les politiques publiques s'y référant, dans la pratique et de par leur conception. Il faut donc garantir que les cadres juridiques, les exigences et procédures pour enregistrer, obtenir ou utiliser une identification et les données collectées ou affichées sur les justificatifs d'identité ne permettent pas ou ne renforcent pas la discrimination contre des groupes particuliers, notamment ceux susceptibles de faire face à des risques accrus d'exclusion pour des raisons culturelles, politiques, économiques ou autres. Ces groupes comprennent notamment : les personnes vivant dans la pauvreté ; les femmes et les enfants ; les populations rurales ; les minorités raciales, ethniques, linguistiques et religieuses ; les personnes handicapées ; les minorités sexuelles et de genre ; les migrants ; les demandeurs d'asile, les réfugiés et les personnes déplacées de force ; et les apatrides. En outre, les systèmes d'identification et les données ne devraient jamais être utilisés comme un outil de discrimination ou pour enfreindre ou nier les droits individuels ou collectifs.

11 Si les États ont le droit souverain de déterminer l'éligibilité à la citoyenneté et de délivrer une preuve de citoyenneté, conformément au droit international, ils ont également l'obligation de fournir une preuve d'identité juridique — ou de reconnaître une identification légalement délivrée par un autre État ou une organisation internationale — à toutes les personnes résidant sur leur territoire, y compris l'enregistrement des naissances. Par exemple, l'article 27 de la Convention de 1951 relative au statut des réfugiés dispose que les « États Contractants délivreront des pièces d'identité à tout réfugié se trouvant sur leur territoire et qui ne possède pas un titre de voyage valable. » Et une disposition similaire pour les apatrides figure à l'article 27 de la Convention de 1954 sur le statut des apatrides. Fournir à tous une preuve d'identité juridique est essentiel pour prévenir l'apatridie (voir www.unhcr.org/ibelong).

12 Les États devraient fournir une preuve de citoyenneté à toutes les personnes qui y ont droit sans discrimination d'aucune sorte.

13 L'obligation qu'ont les États de fournir une preuve d'identité juridique ne signifie pas nécessairement que l'inscription dans les systèmes d'identification devrait être juridiquement obligatoire.

14 Par exemple, l'article 7 de la Convention relative aux droits de l'enfant dispose : « L'enfant est enregistré aussitôt à sa naissance et a dès celle-ci le droit à un nom, le droit d'acquérir une nationalité et, dans la mesure du possible, le droit de connaître ses parents et d'être élevé par eux. » La Convention a été ratifiée par tous les États membres de l'ONU à l'exception des États-Unis, qui l'ont signée, mais pas ratifiée. Dans la pratique, cependant, pratiquement toutes les naissances aux États-Unis sont enregistrées.

Éliminer les obstacles à l'accès et à l'utilisation.

- *Coûts directs et indirects.* Les coûts pour l'individu ne doivent jamais être un obstacle à l'obtention des documents d'identité nécessaires pour exercer ses droits ou accéder aux services ou prestations de base. Par exemple, l'enregistrement des faits d'état civil et la délivrance initiale de certificats de naissance et de décès et d'autres pièces d'identité juridique devraient être gratuits. Si des frais sont facturés pour certains services supplémentaires (tels que la redélivrance de justificatifs d'identité perdus), les tarifs doivent être raisonnables, proportionnels aux coûts encourus et transparents pour le public. En outre, les coûts indirects de la délivrance d'une pièce d'identité, y compris les frais relatifs aux pièces justificatives, les frais de voyage et les procédures administratives lourdes, doivent être réduits au minimum.
- *Asymétrie de l'information.* Les parties prenantes doivent s'efforcer de réduire les barrières et les disparités en matière d'information et de connaissances qui pourraient empêcher les individus, notamment les minorités linguistiques, les personnes à faible niveau d'alphabétisation, les personnes handicapées et autres, d'accéder à l'identification ou de l'utiliser et de favoriser une culture de confiance et de responsabilité par une alphabétisation et une sensibilisation accrues au sujet du système. Les campagnes d'information et d'éducation et autres soutiens doivent être inclusifs et accessibles pour garantir que *chacun* dispose des connaissances, des capacités et des outils dont il a besoin pour participer au système d'identification et exercer ses droits de supervision et de contrôle.
- *Lacunes technologiques.* Bien que la technologie soit un facteur essentiel des systèmes d'identification, personne ne devrait se voir refuser l'identification ou les services et droits associés, faute de connectivité mobile ou d'Internet, d'appareils électroniques, d'alphabétisation numérique ou de compétences numériques, de disposition ou d'aptitude à utiliser certaines technologies, ou en raison de biais ou d'échecs technologiques. Les parties prenantes doivent donc œuvrer ensemble pour garantir que les services d'identification et d'authentification soient disponibles et utilisables par tous, indépendamment des ressources numériques, des compétences ou de la connectivité. En outre, des procédures accessibles de traitement des exceptions et des mécanismes de règlement des plaintes sont nécessaires pour éviter le déni de services ou de droits et en cas de difficultés techniques.
- *Inclusion dès la conception.* Les systèmes d'identification doivent hiérarchiser les besoins et répondre aux préoccupations des groupes marginalisés et vulnérables qui risquent le plus d'être exclus et qui ont le plus besoin des protections et des avantages que l'identification peut offrir. Il s'agit donc de collaborer avec les communautés pour identifier proactivement les obstacles juridiques, procéduraux, sociaux et économiques auxquels sont confrontés des groupes particuliers, ainsi que les risques et les effets qu'ils encourrent, et d'adopter des technologies appropriées et des mesures d'atténuation pour faire en sorte que les systèmes d'identification nouveaux ou mis à jour ne renforcent ni n'approfondissent les inégalités existantes.



CONCEPTION

3

Établir une identité fiable, unique, sécurisée et précise.

- *Unicité.* Un système d'identification offre un mécanisme pour établir et authentifier une identité unique lorsque, dans ce système, chaque personne n'a qu'une seule identité et qu'aucune personne ne partage la même identité avec une autre personne. L'unicité est particulièrement importante pour les systèmes d'identification juridique et autres qui prennent en charge des cas d'utilisation nécessitant des niveaux élevés d'assurance¹⁵, tels que les paiements de gouvernement à personne et le vote. Par ailleurs, l'unicité dans un système donné n'implique pas qu'il doit y avoir un seul prestataire ou système d'identité ou un seul identifiant permanent (par exemple, un numéro d'identification unique) utilisé à toutes les fins dans un pays ou une juridiction.
- *Sécurité.* Les systèmes d'identification doivent disposer de garanties suffisantes et efficaces contre les accès non autorisés, la falsification (altération ou autres modifications non autorisées des données ou des justificatifs d'identité), le vol d'identité, l'utilisation abusive des données, la cybercriminalité et les autres menaces pouvant survenir tout au long du cycle de vie de l'identité. Les données doivent être protégées lorsqu'elles sont stockées et en transit, y compris lorsque les gens utilisent leurs identifiants, ou lors d'usage sur des appareils personnels. Les mesures de sécurité doivent comprendre des systèmes pour sensibiliser à l'utilisation sûre du système et pour informer les personnes concernées en cas de violation de données, ainsi que des recours en cas d'identités volées ou compromises et qui doivent être réémises.
- *Précision.* Garantir que les données relatives à l'identité sont exactes et adéquatement mises à jour est un élément central de la protection des données et est un droit des individus concernés ; c'est par ailleurs essentiel afin d'asseoir la confiance dans le systèmes. Les systèmes d'identification devraient être conçus pour assurer l'exactitude des données collectées et mettre à disposition des procédures simples et adaptées aux besoins des bénéficiaires pour leur permettre d'accéder à leurs données personnelles et les mettre à jour et corriger les erreurs afin d'en assurer l'exactitude au fil du temps.

¹⁵ De manière générale, un « niveau d'assurance » représente le degré de confiance qu'un système d'identification ou un identifiant donné assure à un tiers qu'une identité revendiquée par une personne ou une entité est effectivement la « vraie » identité. Ceci est fonction de plusieurs facteurs, notamment la solidité de la procédure de vérification de l'identité lors de l'enrôlement dans un système d'identification et de l'émission des identifiants (le niveau d'assurance de l'identité), la solidité du processus et de la technologie d'authentification (niveau d'assurance d'authentification) et – s'il s'agit d'un modèle fédéré – le protocole d'affirmation utilisé par la fédération pour communiquer les informations concernant l'authentification et les attributs (niveau d'assurance de la fédération) (adapté de NIST 800-63: 2017).

4

Créer une plateforme adaptable et interopérable.

- *Adaptabilité.* Les services d'identification et d'authentification doivent être conçus pour répondre aux besoins et préoccupations réels des gens. En outre, ils doivent être flexibles, évolutifs et utiles pour les organismes publics et les entités du secteur privé qui y ont recours pour l'identification ou l'authentification. Il faut donc une large consultation des parties prenantes et une approche participative centrée sur les personnes, y compris la société civile, le grand public, les prestataires de services et d'autres parties de confiance, depuis le processus de conception et tout au long de la mise en œuvre.
- *Interopérabilité.* Sous réserve des lois et réglementations sur le partage des données et des garanties techniques appropriées, dont les principes de « respect de la vie privée dès la conception », la capacité des systèmes d'identification à communiquer avec d'autres systèmes (par exemple, les systèmes d'état civil et les fournisseurs de services) et à échanger des requêtes ou des informations facilite les services, tels que la vérification ou l'attestation d'identité, eKYC, les autres partages de données autorisées et la reconnaissance mutuelle des systèmes d'identification aux frontières¹⁶.

5

Utiliser des normes ouvertes et éviter la dépendance vis-à-vis des fournisseurs et des technologies.

- *Normes ouvertes.* Les conceptions fondées sur des normes ouvertes permettent la libre concurrence et l'innovation¹⁷. Les normes ouvertes sont essentielles pour assurer une plus grande efficacité, une meilleure fonctionnalité et l'adaptabilité des systèmes d'identification, à la fois à l'intérieur des pays et au-delà des frontières.
- *Éviter la dépendance vis-à-vis des fournisseurs et de la technologie.* De bons processus de passation des marchés facilitent la concurrence, favorisent l'innovation et empêchent la dépendance vis-à-vis de la technologie et des fournisseurs, ce qui peut augmenter les coûts et réduire la souplesse nécessaire à la mise en place de changement au fil du temps. Les processus de passation des marchés devraient mettre l'accent sur l'optimisation des ressources, l'économie, l'intégrité, la réponse aux besoins définis, l'efficacité, la transparence et l'équité. Une gestion efficace des marchés garantira que ces avantages seront maintenus tout au long de la mise en œuvre.

¹⁶ L'interopérabilité transfrontalière peut faciliter la migration et le commerce, mais des contrôles doivent être mis en place pour protéger la sécurité des groupes vulnérables, notamment les réfugiés, dont les données personnelles doivent souvent être protégées de leur pays d'origine.

¹⁷ Par exemple, l'ISO/CEI a élaboré des normes couvrant de nombreux aspects des systèmes d'identification. Pour en savoir plus, voir Banque mondiale, 2016, "Technical Standards for Digital Identity Systems: Formulating a Strategic Approach."

6

Protéger la vie privée et permettre le contrôle individuel, grâce à la conception du système.

- *Approche de la protection de la vie privée dès la conception.* Les systèmes d'identification doivent être conçus avec comme priorité la protection de la vie privée et des données, laquelle protection devrait constituer un paramètre par défaut du système et ne requérir aucune action additionnelle particulière de la part des individus. Les données personnelles, y compris toutes les données liées ou pouvant être liées à un individu, doivent être proactivement protégées contre toute utilisation abusive et par défaut grâce à un cadre juridique et réglementaire solide, à la conception du système et à l'adoption de normes techniques et de contrôles opérationnels¹⁸.
- *Principes de protection des données dans la pratique.* La conception, les politiques et la technologie utilisées par les systèmes d'identification doivent être conformes aux normes mondiales de protection des données, y compris la minimisation et la proportionnalité des données, la spécification des finalités, le traitement légal, des limites strictes imposées pour la conservation des données, la précision des données, la sécurité, la responsabilité et la transparence, entre autres¹⁹. Par exemple, les systèmes d'identification devraient limiter la collecte et l'exposition des données, en particulier des informations personnelles sensibles²⁰, notamment les identifiants et la structure des numéros d'identification. Les protocoles d'authentification ne doivent divulguer que les données minimales nécessaires pour garantir des niveaux d'assurance appropriés et ne conserver les données que le temps nécessaire aux fins pour lesquelles les données peuvent être utilisées légalement ou pour lesquelles le consentement a été donné. Ces niveaux et la méthode d'authentification devraient refléter une évaluation du niveau de risque dans les transactions et être de préférence basés sur des normes internationales reconnues²¹. Les règles et politiques relatives aux données devraient être transparentes et mises à la disposition des personnes dans un format convivial, afin de leur permettre de connaître facilement leurs droits et les processus disponibles pour exercer le contrôle ou la supervision de leurs données.

18 Concernant l'approche « protection de la vie privée dès la conception », voir, par exemple, Cavoukian, A. 2011, "Privacy by Design : The 7 Foundational Principles. Implementation and Mapping of Fair Information Practices." https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf.

19 Les exemples de normes couramment mentionnées comprennent les *Fair Information Practices* (FIPs), les lignes directrices de l'OCDE sur la protection de la vie privée, le règlement général sur la protection des données de l'UE, les principes des Nations Unies sur la confidentialité et la protection des données et la Convention 108+, entre autres.

20 Les « informations personnelles sensibles » peuvent varier selon le contexte, mais elles incluent généralement les données qui pourraient être utilisées pour créer des identités frauduleuses ou pour profiler ou cibler des individus. Elles comprennent les données biométriques et les numéros d'identification, notamment les numéros d'identité permanents ou uniques, ainsi que des attributs tels que la religion, l'appartenance ethnique, la caste, l'affiliation politique, etc. La divulgation d'informations d'identification peut comporter des risques particulièrement graves pour certaines personnes, dont les demandeurs d'asile et les réfugiés. Par conséquent, des considérations spécifiques s'appliquent aux systèmes d'identification utilisés principalement ou exclusivement à des fins humanitaires, en particulier dans les situations de conflit, de violence et de fragilité. Voir, par exemple, Comité international de la Croix-Rouge, "Policy on the Processing of Biometric Data by the ICRC." 2019, disponible à l'adresse : https://www.icrc.org/en/download/file/106620/icrc_biometrics_policy_adopted_29_august_2019_.pdf, et ICRC/Brussels Privacy Hub Handbook on Data Protection in Humanitarian Action, 2nd edition, 2020.

21 Ces évaluations de l'impact des risques devraient être effectuées par l'entité en charge de créer, collecter, partager, ou utiliser des données à des fins d'authentification et d'identification liées au cas d'utilisation spécifique. Des exemples de normes existantes pour les niveaux d'assurance pour la preuve d'identité comprennent l'ISO / CEI 29115 et celles publiées par eIDAS, le *Cabinet Office* du Royaume-Uni, le *National Institute of Standards and Technology* (NIST) des États-Unis et d'autres.

7

Planifier la pérennité financière et opérationnelle.

- *Viabilité.* Les systèmes d'identification doivent être conçus de manière à assurer une viabilité budgétaire et opérationnelle à long terme. Il faut donc un mode de conception transparent et axé sur les résultats, afin de garantir que le système soit adapté aux besoins et fasse des choix techniques et de gestion durables, ainsi que l'adoption de modèles opérationnels qui garantissent la longévité du système sans compromettre les autres Principes. Les frais pour les services d'identification peuvent créer des obstacles à l'accès, à l'inclusion pour les individus et à l'adoption pour les prestataires de services. En outre, les efforts visant à récupérer les coûts, grâce à des gains d'efficacité et à la réduction des fuites, doivent mettre en balance les objectifs d'économies budgétaires et la possibilité d'erreurs d'exclusion accrues. Les systèmes d'identification devraient être conçus de façon à encourager l'adoption de normes de performance élevées par toutes les parties concernées.



GOUVERNANCE

8

Protéger les données personnelles, assurer la cybersécurité et protéger les droits des personnes, grâce à un cadre juridique et réglementaire complet.

- *Cadres juridiques et réglementaires.* Les systèmes d'identification doivent être étayés par des cadres juridiques et réglementaires légitimes, complets et applicables et des politiques solides qui favorisent la confiance dans le système ; garantir la protection des données et la confidentialité (y compris la cybersécurité) ; atténuer les abus tels que la surveillance non autorisée en violation de la procédure régulière ; être exempts de discrimination et favoriser l'inclusion, en particulier des groupes vulnérables ou marginalisés ; et assurer la responsabilité. Les cadres juridiques doivent clairement définir la responsabilité et les recours des particuliers et être supervisés par des organismes de réglementation indépendants dotés de pouvoirs appropriés et d'un financement adéquat et régulier. Ils devraient également protéger les personnes contre l'accès et l'utilisation inappropriés de leurs données à des fins de surveillance indue ou de profilage illégal. Les cadres exigent un équilibre entre les modèles de réglementation et d'autorégulation qui ne freine pas la concurrence, l'innovation ou l'investissement. Des cadres juridiques et réglementaires appropriés sont également nécessaires pour l'interopérabilité transfrontalière ou la reconnaissance mutuelle²².
- *Droits des personnes concernées.* Les services d'identification devraient offrir aux usagers un véritable choix et un contrôle sur la collecte et l'utilisation de leurs données, y compris la possibilité de ne divulguer de manière sélective que les attributs requis pour une transaction particulière. Les gens devraient avoir un moyen simple de faire corriger gratuitement des données inexactes et d'obtenir une copie de leurs données personnelles. Les données personnelles ne doivent pas être utilisées à des fins secondaires et non liées sans le consentement éclairé de la personne concernée, sauf disposition contraire ou autorisation légale (par exemple, si cela est nécessaire et proportionné)²³. Les fournisseurs d'identité et les autres parties prenantes doivent faire preuve de transparence dans la gestion des identités, mettre en place des ressources appropriées pour sensibiliser les gens à la manière dont leurs données seront utilisées, et leur fournir des outils accessibles et conviviaux pour gérer leurs données, fournir un consentement éclairé et traiter les plaintes. Les fournisseurs d'identité devraient veiller à ce que le processus initial de correction des erreurs soit administratif plutôt que judiciaire afin d'accélérer le règlement des cas et de réduire les coûts. Les modalités de partage des données doivent également être transparentes et entièrement documentées.

²² Par exemple, les demandeurs d'asile et les réfugiés doivent faire l'objet d'une attention particulière ; voir *UNHCR Advisory Opinion on the Rules of Confidentiality Regarding Asylum Information* à <https://www.refworld.org/docid/42b9190e4.html>

²³ Voir, par exemple, Convention 108+, articles 5, 10 et 11.

9

Définir clairement les mandats institutionnels et le principe de responsabilité.

- *Mandats institutionnels.* La législation, la réglementation et les cadres de confiance doivent établir et réglementer des dispositifs de gouvernance complets pour les systèmes d'identification et les fournisseurs au niveau national et, le cas échéant, au niveau international. Il s'agit notamment de préciser les termes et conditions régissant les relations institutionnelles entre les parties participantes, afin que les droits et responsabilités de chacun soient clairs pour tous.
- *Principe de responsabilité.* Il devrait y avoir une reddition de comptes et une transparence claires concernant les rôles et les responsabilités de toutes les entités impliquées dans la mise en place, l'exploitation, la gestion et la supervision des systèmes d'identification.



10

Faire respecter les cadres juridiques et de confiance, grâce à une supervision indépendante et à l'arbitrage des griefs.

- *Supervision.* L'utilisation des systèmes d'identification doit être supervisée par un organisme de contrôle indépendant (à des fins d'efficacité, de transparence, d'exclusion, d'utilisation abusive, etc.) afin de garantir que toutes les parties prenantes se conforment aux lois et réglementations applicables, utilisent de manière appropriée les systèmes d'identification pour atteindre leurs objectifs définis, surveillent et répondent aux potentielles violations de données et reçoivent les plaintes ou préoccupations individuelles concernant le traitement des données personnelles. Les régulateurs devraient disposer de suffisamment de ressources et de pouvoirs pour s'acquitter de leurs responsabilités statutaires.
- *Règlement des plaintes.* Les litiges concernant l'identification et l'utilisation des données personnelles — par exemple, le refus d'enregistrer une personne ou de corriger des données, ou une détermination défavorable du statut juridique d'une personne — qui ne sont pas réglés de manière satisfaisante par les fournisseurs d'identité devraient faire l'objet d'une procédure rapide et peu onéreuse d'examen par des autorités administratives et judiciaires indépendantes, habilitées à fournir une réparation appropriée sans créer d'autres obstacles pour l'individu.

06/06

REPUBLIQUE DE COTE D'IVOIRE
ETAT CIVIL
DESCRIPTION D'ETAT CIVIL
TEAPLEU

CENTRE
ESALE

24 DU 16/2/2001

NAISSANCE DE
DIOMANDE
NOEL
BEROLE

Le QUATORZE FEVRIER DEUX MIL UN /.
est né DIOMANDE NOEL BEROLE /.

à BOFLEU
Fil^{le} de DIOMANDE NIHOUA GERARD /.
Nationalité
et de DIOMANDE CLINGE CHANTAL /.
Nationalité

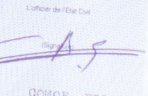
MENTIONS (éventuellement) : NEANT

Marie le à /
Avec
Mariage dissous par décision de divorce en date du
Décédé le à /

Certifié le présent extrait conforme aux indications portées au registre.

Delivré à TEAPLEU le 23 NOVEMBRE 2009

 D 05 597 551

 
GOMBE ESSON
Administrateur Civil

ORGANISATIONS SOUTENANT LES PRINCIPES



Nous invitons d'autres organisations à se joindre à nous pour soutenir ces Principes.

Février 2021