Lignes directrices sur l'identité nationale numérique

Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Convention 108

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Lignes directrices sur l'identité nationale numérique

Adoptées par le Comité de la Convention
pour la protection des personnes
à l'égard du traitement automatisé
des données à caractère personnel
(Convention 108)

Conseil de l'Europe

Édition anglaise :
Guidelines on National Digital Identity

Photo: Shutterstock

Conception de la couverture et mise en page : Division de la production des documents et des publications (DPDP), Conseil de l'Europe

Cette publication n'a pas fait l'objet d'une relecture typographique et grammaticale de l'Unité éditoriale du SPDP.

Imprimé dans les ateliers du Conseil de l'Europe

Table des matières

Introduction

De nombreux pays ont adopté des « schémas d'identité nationale » qui traitent une série de données personnelles, y compris des données appartenant aux catégories spéciales de données sur les individus, dans le but principal de certifier l'authenticité de l'identité juridique d'une personne au regard de la loi et de l'État. Le concept d' « identité juridique » a été développé à partir de l'article 6 de la Déclaration universelle des droits de l'homme qui stipule que « *Chacun a le **droit** à la reconnaissance en tous lieux de sa personnalité juridique.* »

Historiquement, cela a commencé par des schémas d'identité « analogiques » basés sur une quantité limitée d'informations contenue dans les dispositifs d'enregistrement civils (enregistrements des naissances, des mariages, des décès). Ces schémas étaient fondés – et le sont peut-être encore – sur l'émission de « documents » d'identification (tels qu'une carte d'identité) qui permettent à une personne de prouver son identité au regard de la loi et de l'État. Ces documents peuvent permettre d'accéder à des services publics (par exemple, une couverture sociale) ou d'affirmer ses droits civiques.

De plus en plus, les systèmes d'identité « analogiques » sont numérisés afin d'y inclure le traitement électronique de données personnelles souvent accompagné d'une authentification au moyen de données biométriques telles qu'empreintes digitales et balayages d'iris. Ces schémas numériques nationaux peuvent en plus absorber ou établir des liens vers des données démographiques et biométriques collectées dans d'autres systèmes spécifiques à d'autres secteurs comme les soins de santé, la protection sociale ou même l'enregistrement d'une carte SIM mobile ou les bases de données d'identité d'appareils sans fil. Les schémas nationaux d'identité numérique visent à représenter le statut juridique d'un individu et peuvent avoir des effets et des influences sur de nombreux aspects de la vie privée des personnes, y compris sur la sphère privée de leurs activités numériques. Par exemple, une identité nationale numérique peut être utilisée par le secteur commercial pour offrir des services de vérification de l'identité ou dans le cas où elle est liée à un numéro ou à l'identifiant d'un appareil sans fil du secteur privé.

L'une des principales justifications de la numérisation de l'« identité juridique » et de la création de schémas et de systèmes d'identité numérique (SNID) est qu'ils assurent et garantissent une sécurité et une certitude juridiques mais peuvent aussi faciliter l'accès aux droits sociaux et économiques, et fournissent des protections sociétales plus larges, telles que la sécurité personnelle et sociétale. Il est aussi avancé qu'ils offrent des avantages comme l'interopérabilité à l'intérieur des frontières et par-delà, qu'ils améliorent l'exactitude et la disponibilité des données, les prises de décision des gouvernements et la fourniture des services publics et des mesures de protection sociale.

Si les SNID peuvent comporter des protections et des avantages significatifs dans de multiples contextes et permettre aux individus d'obtenir et de faire valoir des droits importants, ils peuvent aussi avoir des conséquences négatives pour les individus **ainsi que** pour des communautés et des groupes de personnes. Ces conséquences peuvent aller de la discrimination et de l'exclusion à la marginalisation, au profilage et à la surveillance injustifiés, en passant par la perte de contrôle par une personne sur son identité ou même un usage frauduleux ou une usurpation de son identité.

D'autres risques pour la vie privée des personnes découlent de la multitude d'acteurs impliqués dans la gestion de l'identité numérique, notamment les fournisseurs d'identité, les prestataires de services et les tiers autorisés à développer ou à utiliser les systèmes nationaux d'identification numérique, et proviennent aussi du fait que l'utilisation des identités numériques par les personnes peut être tracée, ce qui permet des formes intrusives de surveillance et de profilage.

Les politiques, le droit et la pratique définissent de manière inadéquate l'« identité numérique nationale » de sorte que les systèmes nationaux d'identité numérique peuvent ne pas prendre en compte les risques pour les droits et libertés fondamentaux des individus (et des groupes et communautés) de manière appropriée, les prévoir ou les protéger. Les évolutions ont également conduit à lier ou à intégrer des systèmes d'identité tels que les bases de données biométriques obligatoires des cartes SIM dans les politiques et systèmes nationaux numériques d'identité, ainsi qu'à la possibilité de relier et d'intégrer ces systèmes à d'autres systèmes comme ceux qui assurent la surveillance des véhicules, la reconnaissance faciale ou vérification des visages.

Le préambule du Rapport explicatif du Protocole STCE No.223 amendant la Convention STE No. 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ('Convention 108+') stipule

que « ***la dignité humaine*** *exige que des garanties soient mises en place* ***lors du traitement des données à caractère personnel****, afin que les individus* ***ne soient pas traités comme de simples objets*** ».[1] L'inclusion croissante de la biométrie dans les SNID, qui rend les personnes « lisibles par des machines », porte en elle le risque de réduire les individus à de simples objets, sans considération de dignité humaine, ainsi que le risque d'autres conséquences néfastes sur les droits et les libertés.

Les SNID peuvent interférer avec les droits de l'homme et les libertés fondamentales, et particulièrement les droits à la vie privée et à la protection des données à caractère personnel, et avoir sur eux des conséquences significatives qui peuvent être encore plus importantes lorsque des données biométriques sont traitées. En conséquence, il est fortement recommandé qu'une loi nationale sur la protection des données conforme à la Convention 108+ soit d'abord mise en place pour fournir les fondements d'une base légitime aux règles et aux sauvegardes. Une telle loi devrait apporter les informations nécessaires et être un prérequis à l'introduction des SNID.

En outre, devant le potentiel de risques pour les droits de l'homme, les SNID devraient adopter une approche fondée sur ces droits et intégrer explicitement les considérations relatives aux droits de l'homme telles quelles sont ancrées dans le droit international correspondant, dans la politique, la conception, la mise en œuvre et le fonctionnement des systèmes et schémas nationaux d'identité numérique. Par conséquent, les présentes lignes directrices soutiennent une approche de la vie privée et des droits de l'homme dès la conception (*by design*) qui comprend la nécessité d'engager les parties prenantes dans l'identification et l'évaluation des impacts négatifs possibles des SNID sur les intérêts et les droits et libertés fondamentales des individus et des groupes. Cette approche suppose que les parties tiennent compte de manière appropriée des besoins, des problèmes et des risques posés par les SNID tels qu'identifiés par les communautés et/ou leurs représentants. Une telle approche est aussi en accord avec la déclaration de l'ancien rapporteur spécial des Nations Unies qui, en 2007, déclarait que « *L'évaluation d'impacts sur les droits de l'homme est le processus qui permet de prédire les conséquences potentielles d'une proposition de politique, de programme ou de projet sur la jouissance des droits de l'homme* ».[2]

1. Convention 108+, Rapport explicatif, préambule et paragraphe 9, https://rm.coe.int/16808ac91b
2. Rapport du Rapporteur spécial sur le droit de toute personne de jouir du meilleur état de santé physique et mentale, https://undocs.org/A/62/214

Les contestations juridiques et de la société civile, que ce soit au Royaume-Uni, au Kenya ou à la Jamaïque, révèlent l'importance pour les titulaires de droits de comprendre l'impact et les conséquences des SNID, ainsi que la nécessité de définir et de garantir les modalités de la responsabilisation en matière de droits de l'homme, pour que les SNID réussissent et inspirent confiance.

Une évaluation d'impact fondée sur les droits de l'homme, qui reflète les articles 1 et 10 de la Convention 108+, incite les titulaires de droits non seulement à promouvoir la transparence des politiques et des pratiques en matière de SNID, mais aussi à identifier leurs propres intérêts, ainsi qu'à percevoir les risques potentiels et réels qu'ils courent et les éventuelles conséquences négatives des SNID pour les personnes et les groupes, risques et conséquences qui, sans cela, resteraient invisibles. Impliquer les titulaires de droits dans une telle approche peut permettre de garantir que le traitement des données à caractère personnel respecte de manière adéquate les droits individuels et autres droits applicables, et qu'il est réellement équitable et transparent, tout en renforçant la conscience des droits existants. Impliquer les parties prenantes peut être considéré comme un élément approprié et nécessaire de protection contre les risques posés aux intérêts, aux droits et aux libertés fondamentaux des personnes.

Portée et objectif

Ces lignes directrices ont une portée générale et s'appliquent aux secteurs public et privé et à l'identité juridique visés par les schémas nationaux d'identité numérique. Rien dans ce document ne devrait être interprété comme excluant ou limitant les dispositions de la Convention européenne des droits de l'homme ni de la Convention STE 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108). D'autres instruments spécifiques peuvent être aussi pertinents dans le contexte des systèmes nationaux d'identité numérique, comme la Recommandation CM/Rec(2021)8 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage ou les Lignes directrices sur la reconnaissance faciale.[3] Ces lignes directrices prennent en compte les principes, autres dispositions et garanties clés de la Convention 108+[4] et visent à les appliquer à l'élaboration et à la mise en œuvre des SNID.

S'appuyant notamment sur l'article 10 de la Convention 108+, ces lignes directrices établissent un ensemble de mesures de référence que les décideurs politiques et autres parties prenantes peuvent appliquer aux systèmes nationaux d'identité numérique, afin de contribuer à garantir que ces systèmes ne portent pas atteinte aux droits de l'homme et aux libertés fondamentales consacrés par les instruments internationaux pertinents, mais qu'ils examinent, prennent en considération et réduisent les effets néfastes potentiels. Il s'agit de contribuer à veiller à ce que les SNID respectent et protègent les droits de l'homme et les libertés fondamentales, depuis leur élaboration politique au travers de leur conception et dans tous les aspects du traitement des données.

Ces lignes directrices encouragent une évaluation objective de tous les intérêts en jeu, y compris des avantages de tels systèmes par rapport à l'interférence qu'ils représentent avec les droits et les libertés fondamentales des personnes, en soutenant les objectifs de politiques légitimes, tout en limitant les risques pour les individus, les groupes et les communautés de personnes.

3. Lignes directrices sur la reconnaissance faciale
4. Protocole STCE n°223 amendant la Convention 108, (« Convention 108+ »)

Principes de protection des données à caractère personnel et des droits de l'homme et libertés fondamentales – la dignité humaine

Lorsque l'on envisage le traitement de données à caractère personnel pour atteindre les objectifs des SNID, il est crucial de réfléchir à ce que disent le préambule et l'article 1 de la Convention 108+ et à la nécessité de sécuriser la dignité humaine et de respecter et protéger les droits de l'homme et les libertés fondamentales de chacun.

En adoptant une approche de précaution et en s'appuyant sur les articles 5 et 6 de la Convention 108+, ces lignes directrices insistent sur les principes de proportionnalité et de nécessité aux stades de l'élaboration des politiques, de la conception, de la mise en œuvre et de l'exécution des systèmes nationaux d'identité numérique. Elles soulignent notamment le besoin de traitements de données personnelles équitables et transparents, y compris grâce à une protection renforcée des catégories spéciales de données comme les données biométriques.

Les politiques ainsi que la conception, la mise en œuvre et le fonctionnement des systèmes nationaux d'identité numérique devraient par conséquent garantir que les SNID ne nuisent pas à la dignité humaine ni aux autres droits humains et libertés fondamentales et que les personnes ne soient pas réduites à de « simples objets ».

Légitimité du traitement

Conformément à l'article 5 de la Convention 108+, le traitement des données à caractère personnel ne peut être réalisé que sur la base du consentement ou d'une autre base légitime établie par le droit national. En outre, l'article 6 de la Convention 108+ exige que le traitement des catégories particulières de données, telles que les données révélant l'origine ethnique d'une personne (souvent utilisées dans les SNID) ou les données biométriques permettant d'identifier de façon précise une personne, fasse l'objet de garanties appropriées inscrites dans le droit national, en complément de celles de la Convention.

Compte tenu de la relation entre l'État, les citoyens et autres personnes concernées, il faut garder à l'esprit qu'en raison du déséquilibre des pouvoirs entre le responsable du traitement et la personne concernée, le consentement ne peut être considéré, en principe, comme une base juridique appropriée pour le traitement des données à caractère personnel par les autorités publiques. Toutefois, lorsque dans des cas individuels, le traitement des données est fondé sur le consentement prévu à l'article 5, paragraphe 2, de la Convention 108+, ce consentement doit être donné librement, être éclairé, explicite et limité à une finalité spécifique. Le consentement doit représenter la libre expression d'un choix intentionnel d'une personne. Il faut tenir compte du fait qu'un déséquilibre de pouvoir entre le responsable du traitement et la personne concernée peut également se produire dans les relations dans le secteur privé (par exemple, la relation employeur-employé). Ainsi, dans les relations entre les citoyens et les tiers autorisés à développer ou à utiliser des systèmes nationaux d'identification numérique, il faut veiller à garantir des normes élevées afin de préserver la libre volonté des individus d'exprimer leur consentement.

Le traitement des données à caractère personnel dans les SNID doit être nécessaire et proportionné, et doit avoir une base juridique spécifique prévue par le droit national, et sa mise en œuvre doit être précédée d'une analyse d'impact. Les SNID doivent servir des objectifs légitimes tels que l'authentification de l'identité d'une personne physique, en conformité avec la constitution du pays et la législation internationale applicable, plutôt que des raisons d'opportunité ou d'être justifiés comme «souhaitables». La loi doit définir, sous une forme aisément accessible et compréhensible, leur champ d'application et les objectifs spécifiques du traitement des données personnelles, y compris les catégories spéciales de données proposées dans le cadre des SNID. Il est recommandé que la loi soit accompagnée d'une évaluation d'impact couvrant les impacts

potentiels sur les droits de l'homme et les libertés des individus et des groupes, préalablement à tout traitement de données. Cela doit inclure une évaluation des garanties appropriées pour limiter et atténuer les risques pour les droits à la vie privée et à la protection des données personnelles.

En raison de leur caractère intrusif et de leur potentiel en termes de surveillance des activités menées par les personnes concernées, l'utilisation des systèmes d'identité numérique qui servent à certifier l'authenticité de l'« identité juridique » d'un individu devant la loi et vis-à-vis de l'État ne devrait pas être rendue obligatoire, et des alternatives moins intrusives devraient être garanties aux personnes pour qu'elles aient accès aux services.

Équité et transparence

La transparence est un principe central de la protection des données comme le décrit le paragraphe 2*(a)* de l'article 5 de la Convention 108+. Elle est particulièrement importante lorsqu'il s'agit de permettre aux personnes de comprendre non seulement quelles sont leurs données traitées et pourquoi, mais aussi les conséquences de leur utilisation et les risques potentiels sur leur vie privée et plus largement sur leurs droits humains et leurs libertés. La transparence est aussi cruciale pour garantir que les individus connaissent leurs droits et sachent comment les exercer. Sur la base du principe d'équité et parce que les individus auront des attentes particulièrement élevées en matière de sécurité de leurs informations, des garanties importantes doivent être mises en place pour protéger les données personnelles contre les menaces extérieures et pour empêcher la violation des actifs et des informations.

Afin que ce principe soit appliqué, les SNID doivent respecter l'article 8 de la Convention 108+ tel qu'explicité par les paragraphes 67 à 70 de son rapport explicatif qui définissent les informations qui doivent être fournies aux personnes pour garantir des niveaux de transparence appropriés. Les informations peuvent être mises à disposition à différents niveaux ou par étapes (c'est-à-dire des informations générales sur le site web, des informations plus détaillées dans le formulaire d'inscription, etc.) à condition que cela contribue à l'efficacité de l'information appropriée et à la compréhensibilité globale du traitement des données prévu dans le SNID. Elles doivent avoir une forme facilement accessible, de préférence par le biais du dispositif numérique qui permet de tracer les données personnelles des individus respectifs au sein du SNID, et être lisibles, compréhensibles et adaptées à des groupes spécifiques

de personnes (par exemple les personnes aveugles ou avec un faible niveau d'alphabétisation). Les informations doivent :

- fournir aux personnes l'identité et le lieu d'établissement ou la résidence habituel du responsable du traitement et la manière de le contacter (les personnes doivent savoir qui est responsable de la collecte et du traitement ultérieur de leurs données et du respect de leurs droits, par exemple) ;
- communiquer quelles catégories de données à caractère personnel seront traitées et pour quelles finalités explicites et spécifiques, y compris si leurs données seront traitées ou pourraient être traitées dans le cadre d'un profilage ;[5]
- indiquer la base juridique invoquée pour traiter les données, conformément aux articles 5 et 6 de la Convention 108+ ;
- renseigner sur les destinataires auxquels les données seront divulguées ou mises à disposition (par exemple, d'autres autorités ou agences publiques) ;
- indiquer l'existence des droits à la protection des données garantis par la Convention 108+ et la manière de les exercer tels que le moyen de faire corriger facilement les données enregistrées inexactes et comment mettre à jour leur enregistrement (ce qui devrait être gratuit) ;
- indiquer comment obtenir réparation.

Des informations supplémentaires sont recommandées :

- indiquer si la communication des données en vue de l'établissement d'une identité numérique nationale est volontaire ou obligatoire – si aucune exemption n'est applicable (et dans ce cas, quelle loi est invoquée) – et indiquer les conséquences de ne pas fournir de données en vue d'établir une identité numérique (NID) ;
- préciser les contextes dans lesquels la présentation ultérieure de la preuve d'une NID est une exigence obligatoire ou volontaire et les conséquences du refus de fournir une NID (par exemple, le refus d'accès à des services ou l'obtention d'un téléphone mobile) ;
- indiquer si les données de l'identité numérique nationale (NID), telles que le numéro national d'identification (NNI), seront partagées avec d'autres

5. Recommandation CM/Rec(2021)8 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement des données à caractère personnel dans le cadre du profilage (adoptée par le Comité des Ministres le 3 novembre 2021, lors de la 1416e réunion des Délégués des Ministres)

systèmes dépendant de l'identité nationale ou accessibles à ces derniers, ou si elles seront requises pour ces systèmes et pourquoi. Par exemple, est-ce que l'identité nationale sera exigée pour obtenir une carte SIM, pour accéder à l'instruction ou aux services de santé et quelles données en seront ensuite collectées ;

- préciser si un NNI sera lié à d'autres identifiants uniques (et quelle sera la base légale pour cela), tels qu'un numéro de téléphone portable, le numéro d'identifiant électronique d'une carte SIM ou le numéro d'équipement électronique d'un téléphone portable, et qui pourraient faciliter l'ingérence de l'État dans les droits de l'homme tels que le droit à la liberté de mouvement et d'association ou le droit à la liberté d'expression ;
- préciser la base d'une exclusion du SNID (par exemple l'absence de preuve de la naissance) ;
- fournir les informations relatives à la conception et la mise en œuvre des systèmes et des opérations appliquées pour le traitement des données à caractère personnel, en particulier lorsque des systèmes automatisés sont utilisés.

L'équité exige également que les communications relatives au SNID et au traitement des données personnelles soient appropriées et intelligibles pour les diverses communautés que le SNID est censé servir.[6]

Objectif(s) spécifique(s) et légitime(s) et limitation des finalités

Avant la mise en œuvre des SNID, il est important que la politique et la législation nationales sur les SNID précisent explicitement les finalités légitimes et autorisées pour lesquelles les traitements des données personnelles, y compris des catégories spéciales de données (telles que les données biométriques identifiant une personne de façon précise) sont jugés licites. Il convient de rappeler que les cas de traitements de données à caractère personnel prévus devraient également être nécessaires et proportionnés pour atteindre les finalités, conformément au point 3. Cela permet de remplir les conditions d'un traitement légitime et de la limitation des finalités prévues par l'article 5, paragraphe 4, point *b*), de la Convention 108+ et d'éviter que les données

6. Voir par exemple le paragraphe 68 du Rapport explicatif sur l'article 8 de la Convention 108+ https://rm.coe.int/16808ac91b

soient traitées pour des finalités imprécises, vagues ou incompatibles. Il est aussi demandé de respecter les obligations concernant la conception contenues par l'article 10 de la Convention 108+.[7]

Les responsables du traitement et les autres entités qui fournissent du matériel, des logiciels et des services permettant la mise en œuvre du SNID doivent veiller à ce que, dès sa conception et les phases suivantes, seules soient traitées les données nécessaires à une finalité spécifiée par la loi sur le SNID ou toute autre législation appropriée. Si le traitement devient incompatible avec les finalités spécifiées et légitimes, les données ne devraient plus être traitées et devraient être détruites. En outre, il convient de noter que, même si le traitement des données à caractère personnel est effectué à des fins légitimes, les données relatives aux SNID ne devraient pas être conservées plus longtemps que nécessaire et devraient être soumises aux politiques et aux procédures applicables de conservation et de suppression.

L'utilisation ultérieure des numéros d'identification nationaux, ainsi que d'autres données collectées aux fins de l'identité nationale numérique, devrait être interdite, sauf pour des finalités clairement prévues par la loi et si des garanties appropriées ont été mises en place.

Étant donné que différentes caractéristiques (tels que l'identité civile, la date de naissance, l'adresse et d'autres éléments plus précis encore) peuvent fournir une image détaillée de la sphère intime d'un individu, elles ne peuvent être introduites dans les systèmes d'identité numérique que si elles sont nécessaires et proportionnées à l'objectif légitime poursuivi.

Qualité des données – exactes, adéquates, pertinentes et non excessives

Données exactes

Il est crucial que des mesures soient adoptées pour garantir l'exactitude de toute donnée personnelle traitée, et que les données personnelles inexactes puissent être corrigées ou supprimées de manière efficace et rapide, notamment afin d'éviter des dommages significatifs sur les droits de l'homme et

7. Le paragraphe 89 du Rapport explicatif de la Convention 108+ sur l'article 10 – Obligations supplémentaires, spécifie « *que les exigences en matière de protection des données soient intégrées dès que possible, c'est-à-dire idéalement au stade de la conception du système et de l'architecture, par des mesures techniques et organisationnelles (protection des données dès la phase de conception).* »

les libertés fondamentales, tels qu'une exclusion de services et de mesures de protection sociale, une discrimination, de fausses accusations d'activités criminelles ou des arrestations et emprisonnements injustifiés.

Lorsque les SNID nécessitent l'enregistrement de données biométriques et que ces dernières peuvent relier à d'autres systèmes basés sur l'identité telle que la reconnaissance faciale, il est important de souligner que, selon les Lignes directrices sur la reconnaissance faciale,[8] « *L'utilisation de la reconnaissance faciale dans le seul but de déterminer la couleur de la peau, les convictions religieuses ou autres convictions, le sexe, l'origine raciale ou ethnique, l'âge, l'état de santé, ou la condition sociale d'une personne, devrait être interdite à moins que des garanties appropriées soient prévues par la loi afin de prévenir tout risque de discrimination* ». Il convient de noter que la simple présence de garanties ne justifie pas à elle seule l'utilisation des technologies de reconnaissance faciale pour la finalité décrite. D'autres considérations devraient entrer en ligne de compte pour procéder à ce type d'utilisation, notamment la nécessité de la technologie, la proportionnalité du déploiement compte tenu des besoins et des objectifs de l'utilisateur, et la mesure dans laquelle la technologie présente un risque de préjudice ou d'autre impact négatif (par exemple, identifié par les évaluations de l'impact sur les droits de l'homme – EIDH).

L'utilisation de données biométriques dans les SNID exige des mesures supplémentaires pour garantir l'exactitude des données biométriques acquises, enregistrées et jumelées. Cela est également vrai lorsque les SNID sont utilisés pour les données biométriques d'une personne afin de prouver son identité ou pour son authentification.[9] Ces mesures sont également exigées afin de réduire la subjectivité et les inexactitudes des techniques et technologies d'identité biométrique et renforcer l'équité.[10] La « vérification de l'exactitude » est une exigence fondamentale de l'approche fondée sur les droits de l'homme dès la conception (*human rights by design*) ainsi qu'une condition à remplir avant l'acquisition et la mise en œuvre des technologies d'identité biométrique.

8. Lignes directrices sur la reconnaissance faciale
9. Voir, par exemple, les Lignes directrices du Conseil de l'Europe sur la reconnaissance faciale, (2021) et les conseils sur la *Biometric recognition and authentication systems* du UK National Cyber Security Centre
10. Bureau des sciences du gouvernement britannique, (2018) *Biometrics : a guide* https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715925/biometrics_final.pdf

Données adéquates, pertinentes et non excessives (minimisation des données)

Seules les données minimales nécessaires doivent être traitées pour atteindre une ou plusieurs finalités spécifiques identifiées et légitimes. Il convient de noter ici aussi que les caractéristiques qui ne sont pas strictement nécessaires à de telles finalités (à savoir, identifier la personne et permettre l'accès aux services) devraient être évitées. Pour ce faire, il faut d'abord définir la finalité et s'assurer de l'existence d'une base légitime appropriée – laquelle, pour les SNID, doit être spécifiée dans la loi.

Les données doivent être proportionnées et suffisantes pour répondre aux finalités identifiées et spécifiques et ne pas être excessives. Les données personnelles ne devraient pas être partagées de manière injustifiée. Le traitement de données à caractère personnel qui pourrait entraîner une ingérence disproportionnée dans le droit à la vie privée et de ce fait dans d'autres droits humains et libertés fondamentales des personnes et des groupes, serait considéré comme excessif au regard de la Convention 108+ et constituerait un traitement illicite de données personnelles.[11]

Des mesures doivent être prises pour garantir que les données biométriques recueillies auprès des personnes pour créer un modèle biométrique à des fins d'identification et d'authentification (si cela est autorisé par la loi sur le SNID) ne contiennent que les informations suffisantes pour répondre à une finalité précise, et ce afin d'empêcher une utilisation abusive ou incompatible des modèles biométriques.

La qualité des données doit faire partie d'un cycle continu d'évaluation et d'adaptation aux résultats et aux événements.

Les bonnes pratiques de gestion de la qualité des données favorisent l'interopérabilité entre systèmes/institutions/juridictions et contribuent à prévenir les effets néfastes sur les droits et libertés des individus et des groupes, à prévenir et/ou supprimer les doublons dans les identités enregistrées et contribuent à une gestion efficace des services dépendant de ces identités. [12]

---

11. Article 5 – Légitimité du traitement des données et qualité des données du Rapport explicatif de la Convention 108+ paragraphe 52
12. Programme alimentaire mondial des Nations Unies, (2021) Rapport du commissaire aux comptes sur la gestion des informations relatives aux bénéficiaires, projet de décision, paragraphe 52

Conservation des données

La conservation des données personnelles doit être proportionnée et nécessaire à la finalité spécifique justifiée et légitime. Une attention particulière doit être portée à la conservation des catégories particulières de données comme les données biométriques.

Les données devraient être supprimées ou ne pas être conservées sous une forme qui permet l'identification d'une personne au-delà de la durée nécessaire à la finalité spécifique pour laquelle elles sont traitées. Cela doit inclure la prise en compte des données traitées dans des systèmes intégrés dans les SNID ou dont les SNID tirent des données - par exemple, les systèmes de reconnaissance faciale, les systèmes d'enregistrement obligatoire des cartes SIM ou les systèmes de contrôle aux frontières. Il convient de noter que des normes communes de suppression pourraient être très utiles au stade de l'élaboration dans laquelle les autorités de contrôle pourraient jouer un rôle moteur.

En outre, un modèle biométrique devrait être supprimé s'il n'est plus lisible en raison d'une telle dégradation des données biométriques de la personne à partir de laquelle il a été créé que cela le rend inutilisable. Un autre exemple est le réenregistrement de données biométriques telles que les empreintes digitales, les balayages de visage et d'iris à intervalles réguliers. Dans ces cas, les anciens modèles biométriques devraient être détruits à moins que leur conservation puisse être justifiée et soit accompagnée des garanties appropriées.

Sécurité du traitement

Les SNID impliquent le traitement de données personnelles (souvent sensibles) à l'échelle d'une population et peuvent même contenir des données sur des groupes spécifiques vulnérables et à risque. Une incapacité à assurer la sécurité des données et des systèmes peut entraîner des conséquences négatives graves pour les droits humains et les libertés fondamentales de personnes, de groupes et de communautés de personnes.

Il est très important que des mesures techniques et organisationnelles appropriées pour protéger les données et les droits et libertés fondamentaux des personnes soient mises en œuvre. Un défaut de sécurité constitue un traitement illicite de données et peut, par exemple, entraîner un vol et/ou une divulgation non autorisée de données, ce qui peut résulter en des dommages tels que le harcèlement, la persécution, la fraude ou l'usurpation d'identité. Il est également important de considérer qu'une fois corrompues – volées

par exemple – les données biométriques ne peuvent pas être remplacées, ou que les modèles biométriques volés peuvent être réutilisés à d'autres fins.

La protection contre le traçage par des tiers d'informations relatives aux appareils à l'aide d'un système SNID doit également être évitée.

Les « mesures appropriées » incluent :

- d'assurer que dans la conception et le fonctionnement des systèmes seules soient traitées les données personnelles nécessaires pour chaque finalité spécifique par défaut ;
- d'évaluer le caractère sensible des données impliquées et les dommages potentiels pour des personnes ou des groupes, et d'adopter des mesures permettant de réduire les risques pour eux ;
- d'adopter et de mettre en œuvre des politiques et des procédures de recherche et de gestion des incidents de sécurité susceptibles de nuire à des personnes, ainsi que des procédures de signalement de ces incidents aux personnes et aux autorités de contrôle ;
- d'adopter et de mettre en œuvre des politiques, des procédures et des mesures physiques et techniques pour contrôler l'accès aux systèmes et aux données qu'ils contiennent ou auxquelles ils donnent accès ;
- de crypter les données fixes et celles en transit et de garantir que seuls des dispositifs fiables puissent accéder aux SNID ;
- d'adopter et de mettre en œuvre des procédures pour rechercher les faiblesses de sécurité et assurer une vérification régulière des mesures de « sécurité » ;
- de fournir des procédures internes et externes pour un signalement confidentiel des failles de sécurité ;[13]
- de tester régulièrement l'efficacité des mesures de sécurité existantes et de tenir un registre des tests effectués ainsi que des mesures prises pour remédier aux défaillances susceptibles de corrompre les données et d'affecter les droits et libertés des personnes ;
- d'envisager les moyens de prévenir une mauvaise utilisation des données des SNID et des systèmes qui ont été corrompus et peuvent être utilisés pour nuire intentionnellement à des personnes, des groupes et des communautés de personnes. Des plans d'urgence devraient être mis en

13. Voir, par exemple, le UK National Cyber Security Centre, Vulnerability Reporting, https://www.ncsc.gov.uk/information/vulnerability-reporting

place pour éviter toute perturbation d'un service essentiel ou d'autres services reposant sur des systèmes liés à l'identité nationale en cas de compromission. Ces plans devraient identifier les systèmes et les processus de sauvegardes qui pourront être activés pour soutenir les opérations des services touchés ;

- de fournir à la personne concernée des outils spécifiques pour prévenir l'usurpation d'identité (par exemple, la vérification des accès et de l'utilisation de l'identité) ;
- que le traçage par des tiers puisse être atténué concrètement par des barrières de sécurité supplémentaires afin d'empêcher la fuite d'informations. À titre de précaution supplémentaire, une information plus approfondie sur des questions comme des dispenses de responsabilité applicables sera mise à disposition des personnes lors de l'accès, afin qu'elles soient informées du régime juridique ou des dispositions contractuelles relatifs à la responsabilité juridique du responsable du traitement des données en cas de violation de la sécurité par des tiers.

Une autre question à prendre en compte par les autorités nationales de contrôle qui fournissent ou valident des applications mobiles pour l'accès au SNID et aux services qui y sont liés n'est pas seulement la sécurité de ces applications mais aussi la possibilité qu'elles contiennent un code de traçage par des tiers intégré qui collecte, entre autres, les identifiants de dispositifs ou des données comportementales, ce qui peut affecter la vie privée et les droits des personnes.

Profilage et prise de décision automatisée

S'ils sont mal utilisés, les systèmes nationaux d'identité peuvent faciliter le profilage et la surveillance électronique des personnes, avec d'importantes conséquences négatives pour les droits de l'homme.[14] Le profilage peut « *exposer les individus à des risques particulièrement élevés de discrimination et d'atteinte à leurs droits personnels et à leur dignité* » et peut conduire à la violation des droits de l'homme. [15]

14. Comme l'a décidé, de façon éloquente, la Cour suprême de la Jamaïque : Cour suprême de la Jamaïque ; Julian J. Robinson c le Procureur général de la Jamaïque
15. Recommandation CM/Rec(2021)8 du Comité des Ministres aux États membres relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage

La mise en place et l'attribution d'un NNI unique, permanent et général devrait être évité pour empêcher le profilage et les risques qui y sont associés, tels que la surveillance des activités sur internet/ou des activités numériques des personnes concernées. Ainsi faut-il privilégier des NNI spécifiques à un service ou à une application et étayés par des garanties appropriées.

Le profilage (tel que décrit dans la Recommandation sur le profilage[16]) devrait être évité au sein des SNID et des systèmes associés, sauf si la loi le prévoit expressément. Toute mesure visant à permettre le profilage devrait être soumise à l'obligation de réaliser une évaluation préalable de l'impact sur les droits de l'homme des personnes et les risques collectifs que cela peut représenter. Les personnes devraient également avoir accès à des mesures basées sur les droits conformément à l'article 9 de la Convention 108+ (par exemple, l'*opt-out* [non-participation/retrait], la possibilité de recours, la possibilité de demander des explications), lorsque le profilage et la prise de décision automatisée sont utilisés. Toute exception à ces droits doit être clairement déterminée conformément à l'article 11 de la Convention108+.

Droits de l'homme et vie privée dès la conception (*human rights and privacy by design*) et évaluations d'impact fondées sur les droits de l'homme

Les choix politiques et conceptuels portant sur les systèmes nationaux d'identité numérique peuvent avoir un impact négatif sur la vie privée et d'autres droits et libertés fondamentales d'individus, de groupes et de communautés. L'article 10 de la Convention 108+ exige que les responsables du traitement et, le cas échéant, les sous-traitants, « *préalablement au commencement de tout traitement [des données], procèdent à l'examen de l'impact potentiel du traitement de données envisagé sur les droits et libertés fondamentales des personnes concernées* » et qu' « *ils doivent concevoir le traitement des données de manière à prévenir ou à minimiser les risques d'atteinte à ces droits et libertés fondamentales* ».

Dans la même veine, le Comité des Ministres du Conseil de l'Europe recommande que « *Les États membres devraient appliquer toutes mesures jugées nécessaires pour encourager et, le cas échéant, exiger que : – les entreprises domiciliées dans leur juridiction montrent une diligence raisonnable en matière de droits de l'homme dans l'ensemble de leurs activités ; – les entreprises réalisant*

16. idem

des activités commerciales significatives dans leur juridiction montrent une diligence raisonnable en matière de droits de l'homme à l'égard de ces activités ».[17] Comme les SNID peuvent constituer une combinaison de dispositifs **et de technologies** publics et privés, l'obligation de montrer une diligence raisonnable et de procéder à des évaluations d'impact sur les droits de l'homme devrait s'appliquer de la même manière aux secteurs public et privé lorsque l'adoption de SNID est envisagée.

Il convient également de prendre en compte la Recommandation du Comité des Ministres sur les impacts des systèmes algorithmiques sur les droits de l'homme[18] par laquelle il préconise l'obligation d'évaluations d'impact sur les droits de l'homme pour tout système algorithmique qui présente un tel risque élevé. Le Comité recommande aussi que « *Les États, ainsi que tous les acteurs privés amenés à collaborer avec eux ou à travailler en leur nom,* ***devraient mener régulièrement et à titre consultatif, des études d'impact des systèmes algorithmiques sur les droits de l'homme avant*** *toute passation de marchés publics, pendant le développement, à des étapes régulières et tout au long du déploiement spécifique au contexte pour identifier les risques de résultats préjudiciables pour les droits.* » Il est très important que des mesures d'atténuation correspondant aux risques identifiés soient également mises en place. L'utilisation d'une catégorisation du risque d'un système algorithmique basée sur des critères de réversibilité et de durée prévue (c'est-à-dire que les décisions automatisées ayant peu ou pas d'impact sont réversibles et brèves, tandis que celles ayant un impact très élevé sont irréversibles et permanentes), telle qu'elle est déjà appliquée dans certaines juridictions, pourrait également être envisagée pour renforcer la confiance et améliorer la transparence.

Sur la base de ce qui précède, et du fait que les systèmes nationaux d'identité numérique peuvent contenir des systèmes de prises de décisions algorithmiques, les présentes lignes directrices visent à assurer une approche de l'identité nationale numérique fondée sur le respect de la vie privée et les droits de l'homme.

Une telle approche fondée sur les droits de l'homme exige aussi d'identifier et d'impliquer des parties prenantes (engagement des parties prenantes) et en

17. Conseil de l'Europe. Recommandation du Comité des Ministres aux États membres sur les droits de l'homme et les entreprises
18. Recommandation Rec(2020)1 du Comité des Ministres sur les impacts des systèmes algorithmiques sur les droits de l'homme

particulier les titulaires des droits concernés. Cela permettra d'identifier non seulement les risques pour les SNID, mais aussi pour les droits de l'homme, les libertés fondamentales et les intérêts des personnes qui seront concernées par eux. Les SNID ne peuvent être conçus de manière à éviter ou limiter les impacts négatifs sur les droits de l'homme que si ces impacts sont identifiés et pris en compte.

Engagement des parties prenantes

L'engagement des parties prenantes est indispensable pour identifier, examiner et atténuer les risques que les SNID peuvent entraîner. Cela facilitera le dialogue sur les problèmes que les SNID cherchent à résoudre et permettra de faire apparaître les intérêts, les attentes, les besoins et les préoccupations des titulaires de droits concernés, ainsi que les avantages et les risques tels qu'ils les perçoivent.[19] Un tel engagement donne une voix nécessaire aux titulaires de droits concernés et les aide à renforcer leurs pouvoirs en reflétant leurs expériences vécues et leurs besoins, et peut aider à établir une confiance dans les propositions.

Une telle obligation d'impliquer les parties prenantes est conforme à l'article 10 et notamment au paragraphe 90 du Rapport explicatif de la Convention 108+ qui permet des obligations supplémentaires pour tenir compte des risques pour les intérêts, les droits et les libertés fondamentaux des « personnes concernées ». De tels risques peuvent rester invisibles sans un engagement efficace des parties prenantes. C'est pourquoi il est recommandé comme garantie appropriée et nécessaire contre ces risques pour les intérêts, les droits et les libertés fondamentaux des personnes.

L'annexe A de ces lignes directrices suggère une liste de parties prenantes clés à consulter dans le contexte de SNID. L'annexe B présente un exemple pour l'engagement de parties prenantes.

Les présentes lignes directrices suggèrent d'adopter une évaluation d'impact fondée sur les droits de l'homme qui reflète l'article 1 ainsi que l'article 10 de la Convention 108+. Cette approche vise à intégrer les considérations des

19. Voir par exemple, the Engine Room, 2019, *What to look for in digital identity systems : A typology of stages* https://www.theengineroom.org/wp-content/uploads/2019/10/Digital-ID-Typology-The-Engine-Room-2019.pdf et *Caribou Digital, Identities : New practices in a connected age* (2017) https://www.identitiesproject.com/wp-content/uploads/2017/11/Identities-Report.pdf

droits de l'homme dans les politiques, la conception, la mise en œuvre et le fonctionnement des SNID. Elle assure aussi que les outils et les instruments de la protection des données contribuent à une prise en compte et à une protection plus large des droits humains et des libertés fondamentales des personnes. Elle aide à identifier et à aborder activement et explicitement les impacts négatifs potentiels du traitement de données dans le cadre des SNID sur un large éventail de droits humains au-delà du droit à la vie privée et conformément à l'article 1 de la Convention 108+.

Une telle approche exige expressément des responsables du traitement qu'ils examinent l'impact probable du traitement envisagé sur les droits et les libertés fondamentales des personnes, préalablement à son début. De plus, ils doivent concevoir le traitement de manière à ce qu'il évite ou réduise le risque d'interférence avec ces droits et libertés fondamentales.

Cette approche intègre aussi la nécessité de prendre en considération les valeurs morales, éthiques et sociales[20] des droits de l'homme énoncées par les instruments internationaux tels que la Convention européenne des droits de l'homme (CEDH)[21] et la Déclaration universelle des droits de l'homme.[22] Elle oblige les décideurs et les responsables du traitement à examiner si un programme risque d'exclure des catégories de personnes ou d'entraîner une discrimination, par exemple. Rien qu'au niveau des politiques, cette approche peut permettre d'évaluer la proportionnalité d'une proposition et même de prévenir des effets néfastes tels que lorsque l'avantage perçu est dépassé par la gravité du préjudice subi par les personnes et, par conséquent, d'évaluer la légitimité du traitement.[23]

Les décideurs, régulateurs, responsables du traitement et fournisseurs de technologies d'identité sont très fortement invités à se familiariser avec les éléments-clé d'une approche de l'analyse d'impact fondée sur les droits de

20. Mantelero, A (2018) *AI and Big Data : A blueprint for a human rights, social and ethical impact assessment* https://www.sciencedirect.com/science/article/pii/S0267364918302012
21. Convention européenne des droits de l'homme (CEDH)
22. Déclaration universelle des droits de l'homme
23. Voir par exemple, les considérations relatives aux avantages et aux inconvénients examinées par la Cour suprême de la Jamaïque dans l'affaire Robinson contre le procureur général de la Jamaïque et le programme Jamaica Digital ID, ainsi que le test de proportionnalité et de légitimité du traitement. https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

l'homme.[24] Bien qu'elles ne traitent pas explicitement des droits de l'homme, les normes internationales sur les schémas d'enregistrement de l'identité peuvent aider à établir une approche méthodique pour créer un cadre pour la gestion de l'identité qui peut être adopté pour inclure des droits de l'homme plus larges.[25]

Responsabilité

L'une des principales exigences de la Convention 108+[26] et de la nouvelle génération de lois en matière de protection des données est que les responsables du traitement, et le cas échéant les sous-traitants, doivent pouvoir démontrer que le traitement des données sous leur contrôle est conforme aux principes et aux obligations énoncés dans ces instruments.

En outre, la responsabilité (telle que décrite dans cette section), ainsi que la garantie des droits des personnes (section 3.10), sont primordiales pour assurer la protection des données personnelles et des droits de l'homme. La prise en compte permanente de ces lignes directrices ainsi que la garantie d'une transparence permanente et d'une évaluation régulière des menaces et des risques, sont essentiels pour la légitimation des SNID.

À cet égard, il est suggéré que les organisations concernées appliquent le principe de responsabilité tout au long des étapes clé des SNID et notamment qu'elles :

- documentent et publient leur engagement en faveur d'une approche fondée sur les droits de l'homme ;
- documentent et publient un plan pour assurer que les impacts sur les droits de l'homme soient pris en compte à chaque étape des SNID – depuis

24. Voir en particulier l'Institut danois des droits de l'homme, et les orientations (2020) sur l'évaluation de l'impact des activités numériques sur les droits de l'homme https://www.humanrights.dk/publications/human-rights-impact-assessment-digital-activities et notamment les comparaisons entre une DPIA et une HRI https://www.humanrights.dk/sites/humanrights.dk/files/media/document/A%20HRIA%20of%20Digital%20Activities%20-%20Introduction_ENG_accessible.pdf. Voir également (2020) *The Tech Sector and National Action Plans on Business and Human Rights* (Le secteur de la technologie et les plans d'action nationaux sur les entreprises et les droits de l'homme) et les conseils sur l'évaluation de l'impact sur les droits de l'homme de l'autorité française de protection des données, la CNIL
25. Par exemple, l'organisation internationale de normalisation a développé des cadres et des normes sur la gestion de l'identité, la preuve d'identité, l'assurance de l'identité biométrique. Voir https://www.iso.org/home.html
26. Article 10

les politiques jusqu'à l'engagement des parties prenantes, la loi, les EIDH, la conception et le fonctionnement des SNID ;

- documentent et publient les résultats de l'engagement des parties prenantes et les résultats des EIDH, ainsi que la manière dont ils seront pris en compte et la suite qui leur sera donnée ;
- élaborent des politiques, des procédures et des pratiques qui montrent comment les incidences sur les droits de l'homme sont prises en compte (depuis la protection des données jusqu'au respect de la vie privée, en passant par la garantie de la non-discrimination, par exemple) ;
- élaborent et mettent en œuvre des programmes de sensibilisation et de formation, notamment aux droits de l'homme et à la protection des données et de la vie privée ;
- mettent en place des procédures d'audit, non seulement pour garantir le respect des obligations énoncées par la législation sur la protection des données et les SNID, mais aussi pour éviter et minimiser les effets négatifs sur les droits de l'homme, en évaluant les cas de traitement des données existants ou antérieurs, et en exploitant la documentation et les autres preuves pertinentes concernant un SNID ;
- veillent à ce que tous les intervenants dans la fourniture et l'exploitation du SNID respectent les principales exigences applicables, notamment les principes clés de la protection des données ;
- établissent des politiques et des procédures pour le respect des droits des personnes et les publient ;
- éditent un processus clair de plaintes individuelles ou collectives et des mécanismes de recours ;
- veillent à ce que l'impact sur les droits de l'homme et la nécessité de prendre les droits de l'homme en compte dès la conception des projets fassent partie des exigences des processus de passation des marchés. Les organisations fournissant du matériel, des logiciels ou des services de maintenance, par exemple, doivent être tenues de certifier leur manière de prendre en compte les droits de l'homme, notamment par la réalisation d'EIDH à l'appui des contrats de soutien aux SNID ;
- mettent en place des structures de gouvernance claires, y compris des comités d'éthique, afin de garantir non seulement le respect de la loi, mais aussi l'exercice d'une diligence raisonnable en matière de droits de l'homme ;

- envisagent des examens indépendants du point de vue de l'évaluation de l'impact sur les droits de l'homme en impliquant toutes les parties prenantes (par exemple les chercheurs, les ONG, les organisations gouvernementales, les experts de l'industrie).

Droit des personnes

L'article 9 de la Convention 108+ confère aux individus un certain nombre de droits sur le traitement de leurs données personnelles. Ces droits doivent être établis par la loi et appliqués aux SNID et à tout service interconnecté ou interdépendant qui demande une preuve d'identité légale ou NID, ou NNI, etc.

Les droits conférés par la Convention 108+ et par la législation internationale en matière de droits de l'homme, telle que la Convention européenne des droits de l'homme, ne peuvent être restreints[27] que lorsque cela est prévu par la loi, que cela constitue une mesure nécessaire et proportionnée dans une société démocratique à des fins spécifiques et légitimes en droit, tout en respectant toujours l'essence des droits et des libertés fondamentaux.

Les personnes doivent être informées de leurs droits et de toute éventuelle restriction ainsi que des contextes dans lesquels ces restrictions peuvent s'appliquer. Ces droits s'appliquent indépendamment de la citoyenneté, de la nationalité ou du statut de résidence des personnes. Il est essentiel que les SNID soient conçus de manière à permettre l'exercice des droits individuels.

Sous réserve des restrictions prévues par la loi, les droits des personnes comprennent :

- le droit d'être informé des raisons pour lesquelles leurs données sont requises, de l'usage qui en sera fait (finalités), de la base légale invoquée (par exemple, le consentement ou le respect d'une obligation légale), de la durée de conservation de leurs données et des destinataires auxquels leurs données seront communiquées ou par lesquels elles seront accessibles, de l'utilisation de systèmes automatisés pour traiter leurs données, en particulier dans les cas impliquant des décisions juridiquement importantes ; il est important que les personnes soient informées d'une façon claire, simple et culturellement appropriée, et de manière suffisante pour leur garantir que le traitement est équitable ;

27. Article 11 de la convention 108+

- le droit d'accéder à leurs données personnelles et d'obtenir, gratuitement, copie des données personnelles traitées ;
- le droit de faire corriger les données inexactes, gratuitement et sans délai excessif ;
- le droit d'obtenir l'effacement de leurs données (gratuitement) lorsque leur traitement est contraire aux dispositions de la loi applicable (telle que la loi sur la protection des données / la loi nationale sur l'identité numérique) ;
- le droit de restreindre le traitement de leurs données ;
- le droit de s'opposer au traitement de leurs données ;
- le droit de ne pas être soumis à une décision les affectant d'une manière significative qui serait prise uniquement sur le fondement d'un traitement automatisé des données, sans que leur point de vue soit pris en compte ;
- le droit de déposer une plainte auprès d'une autorité de contrôle ;
- le droit à des recours juridictionnels et non juridictionnels (comme prévu par l'article 12 de la Convention 108+) ;
- le droit des personnes concernées par des décisions automatisées à des explications qui décrivent comment une décision a été prise et fournissent des informations pertinentes sur le système et les entrées et sorties de données connexes.

Recommandations pour les décideurs

Qu'ils soient parlementaires, législateurs, officiels gouvernementaux ou encore conseillers politiques, les décideurs ont un rôle crucial à jouer pour établir les valeurs sociétales et les approches juridiques ainsi que les normes qui doivent s'appliquer aux schémas nationaux d'identité.

Les politiques et les décideurs devraient :

- veiller à ce que les objectifs suivis par les SNID soient ancrés dans la constitution et la législation internationale applicable, bien définis, basés sur des preuves, proportionnés et nécessaires aux finalités poursuivies ;
- adopter une politique nationale fondée sur les droits de l'homme ;
- envisager d'incorporer dans les législations nationales une approche d'évaluation de l'impact sur les droits de l'homme (EIDH) qui dépasse l'évaluation de l'impact sur la protection des données (EIPD) et qui intègre de façon explicite d'autres considérations de droits de l'homme dans les politiques, la conception, le déploiement et le fonctionnement des schémas et des systèmes d'identité numérique (SNID) ;
- mettre en place des forums de régulation qui permettraient aux autorités de contrôle de la protection des données ainsi qu'à d'autres autorités de contrôle qui ont un rôle dans les SNID d'assurer ensemble une conformité effective, d'aborder les risques et de développer de bonnes pratiques ;
- garantir que les politiques et l'élaboration de la loi soient étayées par un engagement et une participation des parties prenantes qui aient une réelle possibilité d'y contribuer et de les examiner avant leur adoption ;
- publier les résultats de l'engagement des parties prenantes ;
- spécifier dans la loi que le traitement des données personnelles et des catégories particulières de données en particulier n'est permis que pour des finalités spécifiques et légitimes et sur une base juridique précise ;
- spécifier que le consentement au traitement des données ne doit servir de base légale que si toutes les conditions de ce consentement sont réunies, en particulier celles de garantir la liberté de décision des personnes ;

- veiller à ce que l'adoption de garanties appropriées soit une exigence de la politique et de la loi, y compris que des catégories spéciales de données exigent l'adoption de garanties supplémentaires ;
- exiger que les SNID soient soumis à des évaluations et à des obligations en matière de cybersécurité et de capacité d'adaptation compte tenu de leur rôle potentiel dans les infrastructures et services nationaux critiques ;
- exiger des évaluations d'impact fondées sur les droits de l'homme et un examen régulier continu des impacts des SNID sur les titulaires de droits – cela depuis l'élaboration des politiques de la loi et jusqu'à la conception, la mise en œuvre et le fonctionnement des SNID ;
- soutenir le développement d'une méthodologie et de lignes directrices en matière de vie privée et de droits de l'homme dès la conception qui reflètent l'article 10 de la Convention 108+ et les bonnes pratiques ;
- garantir que la loi nationale sur l'identification inclue une obligation de transparence quant au traitement des données et aux droits des personnes concernées (comme décrit ci-dessus). La loi doit prévoir que toute exception soit conforme aux normes prévues par l'article 11 de la Convention 108+ ;
- garantir la mise en place de mécanismes de recours civils et judiciaires permettant aux personnes de faire valoir leurs griefs et leurs droits ;
- mettre en place des fonctions indépendantes de contrôle dotées de pouvoirs d'audit et de correction ;
- prévoir la réparation des dommages qui pourraient survenir du fait d'une corruption du SNID comme le vol de données, des attaques entraînant un refus de service ou toute autre forme d'actes de cybercriminalité, comme les définissent la Convention STCE N°185 sur la cybercriminalité (Convention de Budapest) et ses protocoles additionnels,[28] l'appropriation de systèmes nationaux d'identité pour nuire intentionnellement à des personnes ou des catégories de personnes ;
- pénaliser d'éventuelles attaques contre et au moyen d'ordinateurs en relation avec le SNID, conformément à la Convention de Budapest ; par exemple, la vente ou l'utilisation frauduleuse des données pour des bénéfices financiers.

28. Convention STCE n° 185 sur la Cybercriminalité (Convention de Budapest)

Recommandations pour les responsables du traitement

Les responsables du traitement, aux termes de l'article 2 de la Convention 108+, qu'ils soient publics ou privés, devraient suivre les orientations contenues dans ce document. Toutefois, cela ne saurait remplacer les lois applicables en matière de protection des données auxquelles ils doivent se conformer dans le traitement de données personnelles et de données particulières telles que les données biométriques permettant d'identifier une personne de façon précise. Ils doivent dûment tenir compte des risques pour les droits et les libertés des personnes et être en mesure de démontrer que leur traitement est conforme aux lois applicables en matière de protection de la vie privée et des données personnelles.

Les responsables du traitement devraient :

- envisager la nomination d'un délégué à la protection des données ayant les compétences et les connaissances appropriées en matière de législation sur la protection des données personnelles (et notamment son application aux SNID) ;
- garantir que leur personnel soit correctement formé en matière de protection des données et de la vie privée ainsi que sur l'impact que peuvent avoir la collecte et l'utilisation des données sur les droits de l'homme en général ;
- adopter des politiques effectives et des mesures pour garantir que les données ne sont traitées que sur une base légale appropriée et afin d'assurer la qualité des données, la transparence et les autres principes clés de la protection de données ; en particulier, veiller à ce que les personnes reçoivent toutes les informations pertinentes, y compris sur leurs droits afin qu'elles puissent les exercer facilement ;
- adopter des politiques et des mesures en matière de données soutenant la gestion du cycle de vie et la gouvernance des données dont l'évaluation et le maintien continus de la qualité des données font partie intégrante ;

- lorsque le consentement est la base légale du traitement, garantir qu'il soit donné librement par les personnes et qu'il leur permette de correctement garder le contrôle sur leurs données au long de toutes les activités de traitement ;
- développer et adopter une méthodologie d'évaluation d'impact fondée sur les droits de l'homme et la vie privée, et de droits de l'homme dès la conception (*privacy and human rights by design*), afin de protéger les personnes par exemple contre l'exclusion, la discrimination ou toute autre conséquence néfaste illégale ;
- prévoir un point de contact pour permettre aux personnes de signaler les problèmes rencontrés ou de poser des questions sur la collecte et la réutilisation de leurs données ;
- mettre en œuvre des mesures techniques et d'organisation effectives pour une protection contre les risques pour les personnes ;
- garantir que le partage des données entre responsables de traitement ne puisse être effectué que sur la base de justifications légales appropriées et qu'il soit soumis aux normes appropriées de protection des données décrites dans les présentes lignes directrices ;
- garantir que des contrôles d'accès appropriés soient assurés en ce qui concerne les données relatives aux SNID, spécialement les données personnelles et les catégories particulières de données, pour limiter l'accès aux systèmes nationaux d'identité et aux enregistrements spécifiques aux personnes et dispositifs autorisés, et conserver un registre des accès ;
- empêcher le profilage des personnes sauf s'il est expressément prévu par la loi et que des garanties appropriées sont en place ;
- aider à garantir l'équité et à prévenir l'exclusion lorsque les SNID exigent légalement le traitement de données biométriques à des fins d'authentification ; un autre moyen d'inclusion devrait être prévu pour les personnes qui ne sont pas en mesure de fournir des données biométriques ou dont les données biométriques sont illisibles ou deviennent illisibles.

Recommandations pour les fabricants, les prestataires de services et les développeurs

Les fabricants d'équipements, les prestataires de services et les développeurs de logiciels auxquels il est fait appel dans le cadre des SNID devraient adopter les principes clés de la Convention 108+ pour assurer le respect des droits humains et des libertés fondamentales des personnes. Ces entités commerciales peuvent être concernées par le fait que les responsables du traitement et leurs sous-traitants auxquels ils fournissent équipements et services ont eux-mêmes l'obligation de se conformer à la législation applicable en matière de protection des données ; elles ont alors l'obligation de concevoir le traitement des données de manière à prendre en compte, minimiser et prévenir les risques sur les intérêts, les droits de l'homme et les libertés fondamentales des personnes. Ces entités elles-mêmes traitent peut-être des données pour tester des matériels et des logiciels, par exemple.

Pour permettre aux responsables du traitement et aux sous-traitants de se conformer à la Convention 108+, ces entreprises devraient garantir que les matériels, les logiciels et les services qu'elles fournissent dans le cadre des SNID soient conçus de manière à assurer la qualité des données, la limitation des finalités, la limitation des données, que les données ne soient pas conservées plus longtemps que nécessaire pour une finalité précisée, qu'elles soient effacées de façons appropriées, que les données ne soient traitées que sur une base légale spécifiée et que les systèmes prévoient que les personnes concernées puissent exercer leurs droits (y compris le droit à la correction, l'accès et l'effacement).

L'article 5 de la Convention 108+ exige que les données soient :

- traitées de manière correcte et maintenues à jour. Cela implique que les SNID soient conçus pour permettre de modifier un nom – à la suite d'un acte notarié ou d'un mariage par exemple, ou pour corriger une erreur d'enregistrement – ou encore pour changer les données biométriques d'une personne quand elles rendent inutilisables les modèles biométriques en cours ;

- correctes, pertinentes et non excessives. Cela implique que les SNID soient conçus pour ne traiter que la quantité de données minimale nécessaire pour remplir la finalité spécifiée par la loi et que les données et les opérations de traitement doivent être adaptées à la finalité c'est-à-dire, adéquates et pertinentes au regard de la finalité légitime.

L'article 6 de la Convention 108+ s'applique au traitement des catégories particulières de données telles que les données biométriques qui identifient une personne de façon précise ou les données concernant les origines raciales ou ethniques d'une personne. Il exige que des mesures de sécurité appropriées soient prévues par la loi afin d'assurer une protection contre les risques pour les intérêts, les droits et les libertés des personnes. En outre, l'article 10 de la Convention 108+ prévoit que les exigences de protection des données (et les sauvegardes appropriées) soient prises en compte aussi tôt que possible « *…dans les opérations de traitement, idéalement au stade de la conception du système et de l'architecture…* ».[29]

Les fabricants d'équipements, les prestataires de services et les développeurs de logiciels utilisés pour les SNID devraient prendre les mesures nécessaires pour répondre aux exigences de ces lignes directrices, de la Convention 108+ et des lois nationales applicables en matière de protection des données.

29. Rapport explicatif de la Convention 108+, paragraphe 89.

Recommandations à l'intention des autorités de contrôle de la protection des données

Avant tout, les autorités de contrôle devraient jouer un rôle effectif et actif pour soutenir l'application des lois nationales et d'autres lois applicables en matière de protection des données, conformément au chapitre IV de la Convention 108+.

L'article 15 paragraphe 3 de la Convention 108+ impose aux États des obligations pour garantir que les autorités de contrôle soient consultées sur toute proposition pour toute mesure législative ou administrative impliquant le traitement de données à caractère personnel. Les décideurs et les législateurs devraient donc veiller à ce que ces autorités soient consultées en tant que parties prenantes clés, et ce dès le début de la formulation d'une politique nationale sur les SNID puis tout au long des processus législatifs.

Avec le droit d'être consultée sur des mesures telles que les SNID, une autorité de contrôle peut émettre une opinion sur les opérations de traitement de données qui présentent des risques que les SNID peuvent poser aux droits et aux libertés des personnes. Ainsi, une autorité de contrôle devrait envisager d'émettre de telles opinions lors des consultations réalisées en application de l'article 15 de la Convention 108+ sur tout aspect de propositions d'introduire ou de modifier un SNID lorsque le traitement proposé présente des risques pour les droits et les libertés fondamentales.

L'article 15 impose aussi aux autorités de contrôle de rendre leurs activités publiques – cela devrait inclure leur implication et leurs activités particulières en relation avec les SNID et comprendre des rapports périodiques. Cela répond au rôle crucial qu'elles jouent en tant que défenseurs de la protection de données et de la vie privée, veillant ici à ce que les schémas et systèmes nationaux d'identité numériques intègrent les dispositions de la Convention 108+ et des lois nationales applicables en matière de protection des données. Elles

sont en position d'autorité et ont une expertise que n'ont pas les titulaires de droits concernés et grâce à cela, elles peuvent aider à garantir que les intérêts de ces personnes soient pris en compte dans les SNID, depuis les politiques jusqu'à la pratique.

Les autorités de contrôle peuvent travailler avec les principaux groupes de parties prenantes pour les sensibiliser aux principales considérations de l'impact des SNID sur les droits de l'homme et les libertés et sur les mesures appropriées pour réduire les risques. Elles peuvent participer à l'élaboration des politiques, des lois et au développement d'orientations ou de codes de pratiques contraignants.

Les autorités de contrôle devraient être invitées à prendre part à toute décision envisageant une approche de l'évaluation d'impact sur les droits de l'homme qui étende l'évaluation d'impact à la protection des données et la vie privée, afin d'intégrer explicitement les considérations relatives aux droits de l'homme dans les politiques, la conception, la mise en œuvre et le fonctionnement des schémas et des SNID.

Les autorités de contrôle devraient envisager de participer à des forums de régulation par lesquels toutes les autorités qui jouent un rôle dans les SNID pourraient se rassembler pour veiller à un respect effectif des normes, aborder les risques et élaborer de bonnes pratiques.

Il est aussi recommandé que les autorités de contrôle exercent une surveillance sur les SNID ou qu'elles y soient impliquées d'une manière appropriée.

Glossaire

Authentification : processus consistant à vérifier l'identité d'une personne et à s'assurer qu'elle est bien celle qu'elle prétend être. Cela peut se faire en examinant les documents relatifs à la naissance ou le passeport d'une personne, par exemple.

Autorité de contrôle : une autorité établie pour assurer le respect des dispositions de la Convention 108+ sur la protection des données, conformément à son article 15, ou à la législation interne de référence.

Catégories particulières de données : les données génétiques, des données à caractère personnel relatives à des infractions, des procédures pénales et des condamnations, ainsi que des mesures de sécurité y afférentes, des données biométriques permettant d'identifier une personne de façon précise, et des données à caractère personnel pour les informations qu'elles révèlent concernant l'origine raciale ou ethnique, les opinions politiques, l'appartenance syndicale, les convictions religieuses ou autres, la santé ou la vie sexuelle, et qui nécessitent des garanties appropriées devant être inscrites dans la loi en complément de celles de la Convention 108+ conformément à son article 6.

Convention 108+ : le Protocole (STCE n°223) amendant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention STE N°108).

Données à caractère personnel : toute information relative à une personne identifiée ou identifiable (personne concernée). Cela inclut les informations qui peuvent être utilisées pour individualiser ou distinguer une personne d'une autre, par exemple, par référence à un NNI, un numéro de téléphone mobile ou l'identifiant d'un appareil.

Données biométriques : données résultant d'un traitement technique spécifique concernant les caractéristiques physiques ou physiologiques d'un individu qui permettent de l'identifier ou de l'authentifier de façon précise.

Droits de l'homme et vie privée dès la conception : (*anglais : Human Rights by Design - HRbD*) assurer le respect et la protection des droits de l'homme à toutes les étapes du développement technologique, depuis l'élaboration des politiques, la règlementation, la conception technologique jusqu'au traitement des données personnelles.

Identifiant : un numéro ou une séquence unique de caractères attribué à une personne afin qu'elle soit identifiable de manière unique dans un système de gestion de l'identité donné.

Identification – le processus visant à établir l'identité d'une personne sur la base d'attributs vérifiables.

Identité : un attribut ou une combinaison d'attributs qui identifie un individu de façon précise.

Identité nationale numérique (NID) : traitement des attributs d'un individu de manière à ce que celui-ci soit identifiable de façon précise dans des contextes donnés.

Numéro national d'identité (NNI) : un numéro unique attribué par un SNID qui relie une personne à une identité juridique et par lequel une personne peut être identifiée de façon précise par référence à la vérification des attributs liés à la saisie lors de la création d'un NID.

Profilage : désigne toute forme de traitement automatisé de données à caractère personnel, notamment au moyen de systèmes d'apprentissage automatique, consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne (ou à des groupes de personnes), notamment en ce qui concerne l'ethnie ou la religion, le comportement, la localisation ou les déplacements d'une personne.

Responsable du traitement : désigne la personne physique ou morale, l'autorité publique, le service, l'agence ou tout autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de décision en matière de traitement des données.

Système national d'identité centralisé : système dans lequel les données d'identité sont conservées et contrôlées par un seul système et qui fournit une preuve d'identité et une authentification de l'identité.

Systèmes nationaux d'identité numérique (SNID) : combinaison de politiques, de lois et de technologies permettant de saisir les données personnelles d'une personne afin d'établir et de représenter numériquement, de vérifier et de gérer l'identité juridique d'une personne dans les services publics (et privés) identifiés dans les politiques et lois nationales.

Annexe A
Exemples de listes de parties prenantes

Cette liste n'est pas exhaustive mais comprend les éléments suivants :

Gouvernement

- Les principaux départements, agences et ministères du gouvernement responsables :
  - des technologies de l'information et de communication (TIC)
  - des politiques numériques
  - de l'agenda et de l'économie numériques
  - des soins de santé
  - de l'éducation
  - de l'enregistrement des naissances/enregistrement de la population civile
  - de l'identité nationale
  - du contrôle des frontières
  - de la sécurité nationale/application de la loi
  - de la protection sociale
  - des affaires autochtones
  - des réfugiés
  - de l'approvisionnement
  - de la protection des données
  - des droits de l'homme
  - des questions de discrimination

Parlement

- Comités axés sur les droits de l'homme et la technologie, l'économie numérique et l'identité

Organismes nationaux de réglementation ayant un mandat et des responsabilités en matière de droits de l'homme :

- Autorités chargées de la protection des données (commissaires à la protection des données et de la vie privée et à l'information)
- Commissions ou commissaires chargés des droits de l'homme ou de l'égalité[30]
- Commissaires à la biométrie
- Commissaires au renseignement
- Commission nationale de l'identité
- Autorités chargées des télécommunications

Judiciaire / Réparation

- Médiateur avec des mandats et responsabilités en matière de droits de l'homme et de justice sociale[31]
- Associations des barreaux
- Organisations communautaires qui soutiennent la résolution des conflits en matière de droits de l'homme

Titulaires et représentants des droits

- Représentants associatifs
- Société civile / Organisations de défense des droits de l'homme[32]
- Conseils de citoyens

Secteur de l'entreprise

- Fournisseurs d'identification – matériel et logiciels
- Associations professionnelles
- Opérateurs mobiles[33]

---

30. Par exemple, le chancelier de la justice d'Estonie https://www.oiguskantsler.ee/en.
31. Voir, par exemple, Equinet – Réseau européen des organismes de promotion de l'égalité https://equineteurope.org/author/greece_ombudsman/ ou le Réseau européen des médiateurs https://www.ombudsman.europa.eu/en/european-network-of-ombudsmen/about/en Voir également la note de bas de page 4.
32. Par exemple, des organisations telles que Namati et le réseau d'autonomisation juridique https://namati.org/network/.
33. Les opérateurs de téléphonie mobile peuvent être tenus de collecter et/ou de vérifier les données personnelles et biométriques ainsi que les détails de l'identité nationale de toute personne cherchant à acheter une carte SIM mobile et de les enregistrer en fonction des identifiants de la carte SIM, des identifiants de l'appareil et des numéros de téléphone mobile. Voir par exemple GSMA, 2021, *Access to Mobile Services and Proof Identity* (2021)

- Services financiers/agents de monnaie mobile

Université / Recherche

- Universitaires/chercheurs spécialisés dans l'identité nationale numérique et les droits de l'homme
- Institutions axées sur l'identité nationale numérique et les droits de l'homme[34]

Acteurs internationaux

- Organisations humanitaires
- Banque mondiale
- Organisations des Nations Unies[35]
- Union internationale des télécommunications (UIT)
- Organisation de coopération et de développement économiques (OCDE)
- Union africaine
- Commission africaine des droits de l'homme
- Conseil de l'Europe
- UE[36]

34. Par exemple, l'université de Strathmore, au Kenya, et son Centre de droit de la propriété intellectuelle et des technologies de l'information et son programme de recherche sur l'identité numérique https://cipit.strathmore.edu/our-id-experience/ ou le projet de recherche sur les identités https://www.identitiesproject.com/ ou le Centre d'études Internet, en Inde, «*Digital Identities : Design and Uses'*
35. Voir par exemple l'Agence des Nations Unies pour les réfugiés, Enregistrement et gestion de l'identité ou le PNUD https://unstats.un.org/legal-identity-agenda/meetings/2021/UNLIA-FutureTech/docs/Agenda.pdf.
36. Voir, par exemple, le groupe de travail UE-UA sur l'économie numérique qui considère les services d'identité numérique comme un catalyseur de l'économie numérique https://digital-strategy.ec.europa.eu/fr/policies/africa ou le récent accord entre l'UE et les membres de l'Organisation des États d'Afrique, des Caraïbes et du Pacifique. L'article 70, paragraphe 3, de l'accord exige des parties qu'elles «développent des systèmes d'identification robustes, sûrs et inclusifs afin de garantir la fourniture d'une identité légale à chaque citoyen, notamment en renforçant le système d'enregistrement des faits d'état civil et des statistiques de l'état civil (CRVS). https://ec.europa.eu/international-partnerships/system/files/negotiated-agreement-text-initialled-by-eu-oacps-chief-negotiators-20210415_en.pdf

Annexe B

Exemples d'approches d'engagement des parties prenantes

Les tableaux suivants ont été adaptés directement du *Stakeholder Engagement Practitioner Supplement* de l'Institut danois des droits de l'homme,[37] élaboré dans le cadre de son guide et de sa boîte à outils pour l'évaluation de l'impact sur les droits de l'homme. Les tableaux et les suggestions sont conçus comme une aide à la prise en compte des éléments clés de l'approche des parties prenantes.

37. Stakeholder Engagement Practitioner Supplement

TABLEAU A: Identification des parties prenantes					
Groupe de parties prenantes	**Types spécifiques de parties prenantes**	**Entité et caractéristiques générales** *Exemples fournis*	**Relations avec le promoteur de l'identité nationale/ autres parties prenantes**	**Opinions/ influences sur les NID**	**Type d'engagement, c'est-à-dire** quand et comment (en personne, à distance).
Titulaires de droits/ représentants	**Catégories de groupes potentiellement affectés**	Il peut s'agir de personnes dépourvues de preuve de citoyenneté ou d'identité légale reconnue, de groupes ethniques, réfugiés, demandeurs d'asile et de personnes incapables de faire lire leurs données biométriques ou dont les données biométriques se dégradent avec le temps.			
	Citoyens / consommateurs	Services d'enregistrement des naissances/ CRVS. Patients/étudiants pour lesquels les services exigent une preuve de NID. Les abonnés au téléphone mobile qui ont besoin d'une preuve de NID.			
	Organisations de la société civile/ défenseurs des droits de l'homme	Organisations non gouvernementales locales/internationales et organisations communautaires telles que conseils communautaires, organisations de défense des droits de l'homme, réseaux juridiques, etc. qui représentent les groupes affectés et qui peuvent également faciliter les rôles de recours/médiateurs.			

TABLEAU A: Identification des parties prenantes					
Groupe de parties prenantes	**Types spécifiques de parties prenantes**	**Entité et caractéristiques générales** *Exemples fournis*	**Relations avec le promoteur de l'identité nationale/ autres parties prenantes**	**Opinions/ influences sur les NID**	**Type d'engagement, c'est-à-dire** quand et comment (en personne, à distance).
Les responsables	**Acteurs gouvernementaux**	Autorités nationales, agences ou départements gouvernementaux spécifiques, décideurs et régulateurs ayant une responsabilité directe au niveau politique, juridique, technique, sur la mise en œuvre et/ou réglementaire pour les systèmes nationaux d'identité numérique.			
	Représentants/ comités parlementaires	Comités axés sur les droits de l'homme, la technologie, l'économie numérique et l'identité.			
	Judiciaire/ recours	Associations de barreaux. Organisations communautaires qui soutiennent la résolution des recours en matière de droits de l'homme			
	Industrie/ secteur d'activité	Fournisseurs de matériel/logiciels pour SNID. Fournisseurs de SNID en coentreprise. Entreprises complémentaires pouvant être mandatées pour enregistrer et/ou vérifier les détails de l'identité nationale – par exemple l'enregistrement des cartes SIM. Associations industrielles engagées dans les SNID.			

TABLEAU A: Identification des parties prenantes					
Groupe de parties prenantes	**Types spécifiques de parties prenantes**	**Entité et caractéristiques générales** *Exemples fournis*	**Relations avec le promoteur de l'identité nationale/ autres parties prenantes**	**Opinions/ influences sur les NID**	**Type d'engagement, c'est-à-dire** *quand et comment (en personne, à distance).*
Les responsables	**Marchés publics**	Autorités chargées des achats qui devraient s'assurer que le matériel et les logiciels intégrent les droits de l'homme et les libertés fondamentales dans la conception et le fonctionnement des SNID, de la qualité des données à la conservation et à l'effacement des données en passant par l'exercice des droits individuels. Les processus de passation de marchés devraient exiger une garantie de respect des droits de l'homme dès la conception.			
	Organisations internationales	La Banque mondiale, le CICR, les agences des Nations Unies telles que le PNUD, le HCR, etc.			
	Institutions nationales des droits de l'homme (INDH)	Organes autonomes dotés d'un mandat constitutionnel ou législatif pour promouvoir et protéger les droits de l'homme, tels que les commissions des droits de l'homme ou les médiateurs.			
	Experts et chercheurs	Experts nationaux/juridiques en matière d'identité numérique, notamment universitaires et chercheurs spécialisés dans les droits de l'homme aux niveaux politique, juridique et technologique.			
	Médias/ journalistes	Médias/journalistes publics et privés/associatifs pour favoriser une plus grande sensibilisation et une meilleure connaissance des NID et des consultations publiques et encourager l'engagement communautaire, etc.			

TABLEAU B : Exemples d'étapes à suivre avant un engagement direct avec les parties prenantes		
Étapes	**Processus**	**Domaines nécessitant une attention et des considérations supplémentaires**
1. Créer une équipe d'évaluation de l'impact sur les droits de l'homme	Une **équipe d'évaluation de l'impact sur les droits de l'homme** doit être mise en place. Cette équipe doit avoir des objectifs clairs, et les rôles et responsabilités clés doivent être convenus. L'équipe d'EIDH doit préparer un briefing qui reflète les compétences, les connaissances, etc. des groupes d'intervenants ciblés et qui exprime clairement : – le problème qu'un SNID est censé résoudre, – la base juridique sur laquelle les NID sont établis, – les liens entre le SNID et d'autres services tels que les cartes SIM mobiles, les programmes de santé, d'éducation et de protection sociale, ainsi que l'objectif et la base juridique de ces liens, – les données que le SNID collectera, les objectifs et les personnes qui auront accès aux données (et à quelles fins) ou avec qui les données seront partagées (et à quelles fins), l'endroit où les données seront conservées et comment elles seront sécurisées et protégées contre les abus, – si le SNID est volontaire ou obligatoire et quelles données sont volontaires ou obligatoires. De même, les contextes dans lesquels la preuve du NID sera requise. – tout coût financier pour les individus, – l'objectif de la recherche des points de vue des parties prenantes et la manière dont ils seront pris en compte, – comment les droits et libertés fondamentaux seront protégés, – un point de contact clé par lequel les préoccupations des parties prenantes concernant le processus de consultation peuvent être communiquées.	Il peut être nécessaire de former le personnel existant ou d'engager des experts en engagement des parties prenantes qui peuvent garantir des techniques d'engagement culturellement appropriées et une participation inclusive. L'équipe doit également avoir une connaissance approfondie de la protection des données, des droits de l'homme et de l'identité nationale numérique.

TABLEAU B : Exemples d'étapes à suivre avant un engagement direct avec les parties prenantes		
Étapes	**Processus**	**Domaines nécessitant une attention et des considérations supplémentaires**
2. Contacter les titulaires de droits	Identifier les représentants locaux et évaluer leur expérience des questions liées à l'identité numérique, à la protection des données, aux droits de l'homme et à la facilitation de l'engagement des parties prenantes de la communauté. Identifier les modes de communication et de participation préférés. S'assurer que les parties prenantes identifiées sont suffisamment représentatives. Évaluer si des individus ou des groupes au sein des communautés sont indirectement ou directement exclus par le processus (en raison de leur sexe, de leur statut socio-économique, de leur appartenance ethnique, de leur statut de citoyen, etc.)	Réfléchir au nombre d'individus à engager, à leur position au sein des communautés et à ce qui constituerait un échantillon représentatif des opinions. Quels sont la forme et le lieu préférés pour les réunions, en face à face ou virtuelles. Examiner si les coûts de participation peuvent constituer un obstacle à l'engagement ou si le manque d'équipement TIC et de connectivité peut empêcher la participation. Y a-t-il d'autres obstacles à l'engagement ? Linguistique ? Culturels ? Politiques ? La peur ? Réfléchir à la meilleure façon de garantir un engagement sûr et inclusif.
3. Déterminer le format, le lieu et l'heure des entretiens/ réunions et les facteurs qui peuvent constituer un obstacle à la participation + la confidentialité	Envisager des consultations individuelles ou en groupe, ainsi que des techniques d'engagement culturellement appropriées pour faciliter la collecte d'informations. Comment se déroulera l'engagement – face à face ou virtuel ? Tenir compte de ceux qui, pour une raison ou une autre, se sentent incapables de participer aux réunions proposées – par exemple, les personnes ou les groupes marginalisés ou des groupes uniquement constitués de femmes Tenir compte des paramètres et des horaires culturellement appropriés. Réfléchir à la fourniture de nourriture et de rafraîchissements appropriés, et à la nécessité éventuelle d'une assistance pour se rendre sur un lieu de réunion.	Ne pas prendre de photos sans le consentement explicite des personnes concernées et les informer au préalable si des photos seront publiées (presse écrite ou en ligne, sites web, médias sociaux). Examiner si le fait de fournir des données personnelles peut constituer un obstacle et s'il convient de ne pas enregistrer, ou d'expurger ultérieurement, les données personnelles – en assurant la transparence avec les participants.

TABLEAU B : Exemples d'étapes à suivre avant un engagement direct avec les parties prenantes		
Étapes	**Processus**	**Domaines nécessitant une attention et des considérations supplémentaires**
	Le lieu dispose-t-il d'installations appropriées et est-il un endroit où les parties prenantes se sentiront à l'aise ? Examiner s'il est nécessaire de collecter des données à caractère personnel et, dans l'affirmative, obtenir le consentement des intéressés et expliquer comment ils peuvent changer d'avis et quels sont leurs droits en matière de données.	
4. Évaluer le contexte de sécurité	**Effectuer des recherches approfondies sur la situation locale en matière de sécurité.** Tenir compte des risques, tant pour l'équipe d'évaluation que pour les personnes interrogées, en effectuant une analyse des risques portant sur les menaces, les vulnérabilités et les capacités. **Prendre en compte les risques liés à la participation –** en particulier des groupes marginalisés / vulnérables, des défenseurs des droits de l'homme.	Consulter les représentants des parties prenantes au sujet des préoccupations réelles ou perçues en matière de sécurité pour un lieu choisi. Examiner si la nécessité de prendre les transports publics est considérée comme sûre par les participants. Se demander si se rendre au lieu de rencontre proposé est considérée comme sûr par des groupes spécifiques ? S'assurer que les réponses des participants sont sécurisées de manière approprié – qu'elles soient informatisées ou sur papier. Ne pas prendre de photos sans le consentement explicite des personnes concernées et les informer au préalable si les photos seront publiées (presse écrite ou en ligne, sites web, médias sociaux).

TABLEAU C: Exemples d'étapes à suivre pendant l'entretien ou la réunion avec les parties prenantes		
Étapes	**Processus**	**Domaines nécessitant une attention et des considérations supplémentaires**
1. Information des participants et renforcement des capacités	Un facilitateur convenu doit clairement exprimer : – le processus pour les parties prenantes et son objectif – le problème qu'un SNID est censé résoudre – le souhait de comprendre et de réfléchir dûment aux points de vue, intérêts, besoins et préoccupations des participants – comment les données collectées seront utilisées – être transparent – les droits relatifs à l'utilisation des données personnelles Éviter le langage technique et le jargon juridique, à moins qu'ils ne soient appropriés au groupe de parties prenantes (par exemple, l'industrie, le comité scientifique parlementaire, l'autorité chargée des TIC, etc.) Rester respectueux et sensible aux participants. Rester attentif aux personnes qui peuvent être marginalisées/vulnérables. Rester attentif aux relations de pouvoir et s'efforcer d'inclure avec tact ceux qui peuvent sembler réticents à participer, mais ne pas exercer de pression sur ces individus ou groupes.	**Renforcer les capacités des titulaires de droits** en expliquant la relation entre l'identité nationale numérique, la protection des données et les droits de l'homme et les garanties pour les droits et libertés. Expliquer également le rôle que l'identité nationale et les données d'identification joueront dans d'autres domaines de la vie des citoyens/consommateurs. Par exemple, si une preuve d'identité nationale est requise pour obtenir une carte SIM mobile, ou pour accéder aux soins de santé, à l'éducation ou à la protection sociale, et quelles en seront les implications. Faire une brève présentation sur la protection des données, les NID et les droits de l'homme.

TABLEAU C: Exemples d'étapes à suivre pendant l'entretien ou la réunion avec les parties prenantes		
Étapes	**Processus**	**Domaines nécessitant une attention et des considérations supplémentaires**
2. Assurer une participation volontaire	Veiller à ce que la participation soit informée et volontaire – fondée sur le consentement des personnes. Fournir des avis de transparence culturellement appropriés qui tiennent compte des capacités de lecture et d'écriture et des langues des groupes/individus invités à participer. Veiller à ce que les personnes sachent comment retirer leur consentement à la participation. Informer les personnes de leurs droits sur leurs données – pour les faire détruire par exemple si elles le souhaitent. Valider la compréhension de la discussion avec les personnes interrogées à la fin d'un entretien. Permettre aux personnes de poser des questions.	
3. Respecter la vie privée des participants	**Ne pas recueillir le nom et les coordonnées des personnes, sauf si elles ont donné leur consentement éclairé.** – Veiller à ce que les personnes sachent comment ces données seront enregistrées, pendant combien de temps, où elles seront conservées, qui y aura accès et pourquoi, etc. Examiner s'il est possible d'autoriser une participation anonyme ou une participation en privé. Examiner les risques éventuels pour les individus ou les groupes de voir leurs données personnelles enregistrées et/ou leur participation rendue publique (certains peuvent craindre d'être rendus visibles).	Réfléchir, pendant la phase de planification des parties prenantes, à la manière de répondre/d'assister les individus ou les groupes en cas de connaissance de graves **violations des droits de l'homme** pendant les consultations.

TABLEAU C: Exemples d'étapes à suivre pendant l'entretien ou la réunion avec les parties prenantes		
Étapes	**Processus**	**Domaines nécessitant une attention et des considérations supplémentaires**
4. Assurer la sécurité et la sûreté – ne pas nuire	Tenir compte de tout développement immédiatement avant la date des réunions proposées et le jour même, qui pourrait avoir un impact sur la sécurité de l'équipe de facilitation et des participants des parties prenantes. Être prêt à interrompre l'événement si un groupe ou un individu ne se sent pas en sécurité.	
5. Rester respectueux – communiquer d'une manière culturellement appropriée.	Faciliter les discussions, ne pas les dominer. Écouter et faire preuve d'ouverture d'esprit pour permettre aux expériences vécues des individus et des communautés de faire surface. Faites preuve de respect lorsque vous envisagez d'interrompre ou d'aborder des comportements ou des interventions inappropriés. Rester attentif aux relations de pouvoir et à l'inclusion. S'efforcer d'inclure ceux qui sont moins désireux de s'exprimer dans les entretiens. Prévoir des pauses appropriées pour les rafraîchissements, etc.	

Outre ce qui précède, l'équipe chargée de l'analyse d'impact doit également réfléchir à la manière et au moment de rendre compte aux parties prenantes, partager les résultats et faire un suivi des prochaines étapes, et communiquer un plan.

Si les systèmes nationaux d'identité numérique (SNID) offrent des avantages significatifs, notamment en facilitant l'accès des personnes à des droits importants, ils portent aussi potentiellement des conséquences négatives pour les droits humains des individus, des communautés et des groupes de personnes. Cela peut aller de la discrimination et l'exclusion à la marginalisation, au profilage et à la surveillance injustifiés ainsi qu'à la perte de contrôle d'une personne sur son identité, un usage frauduleux ou une usurpation de son identité.

Pour pallier ce potentiel de risques pour les droits de l'homme, les SNID devraient adopter une approche centrée sur les droits de l'homme tels qu'ils sont ancrés dans le droit international, et ce dès la politique, la conception, la mise en œuvre et jusqu'au fonctionnement des systèmes et schémas nationaux d'identité numérique.

Fondées sur les principes et dispositions de la Convention 108+, ces lignes directrices encouragent une évaluation objective de tous les intérêts en jeu lors de la mise en place de SNID, y compris de leurs avantages par rapport aux risques qu'ils représentent pour les droits et les libertés fondamentaux des personnes. Elles proposent des recommandations pour chaque type d'intervenants dans le développement et la mise en place de tels systèmes et un guide concret pour un engagement des parties prenantes lors d'une évaluation d'impact.

www.coe.int/dataprotection

PREMS 010723

FRA

www.coe.int

Le Conseil de l'Europe est la principale organisation de défense des droits de l'homme du continent. Il comprend 46 États membres, dont l'ensemble des membres de l'Union européenne. Tous les États membres du Conseil de l'Europe ont signé la Convention européenne des droits de l'homme, un traité visant à protéger les droits de l'homme, la démocratie et l'État de droit. La Cour européenne des droits de l'homme contrôle la mise en œuvre de la Convention dans les États membres.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE