20 septembre 2021 T-PD-BUR(2021)2rev2

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

CONVENTION 108

Identité numérique

Projet de lignes directrices

Direction générale des droits de l'homme et de l'État de droit

TABLE DES MATIÈRES

1. Introduction

De nombreux pays disposent de 'systèmes d'identité nationale' qui collectent et enregistrent une série de données démographiques sur une personne afin de lui établir une 'identité légale' au regard de l'État[1]. Historiquement, cela a commencé par un système d'identité 'analogique' basé sur les informations des dispositifs d'enregistrement civils et l'émission de 'documents' établissant l'identification (comme une carte d'identité), qui permet à une personne de prouver son identité au regard de l'État. Ce document peut permettre d'accéder à quelque chose (par exemple, une protection sociale) ou d'affirmer ses droits civiques.

De plus en plus, ces systèmes d'identité 'analogiques' sont numérisés afin de leur inclure non seulement la collecte d'informations démographiques mais aussi des données biométriques tels que les empreintes digitales et des scans d'iris. Ces systèmes numériques nationaux peuvent en plus absorber des données démographiques et biométriques collectées dans d'autres systèmes spécifiques à d'autres secteurs comme l'enregistrement d'une carte SIM mobile ou les bases de données d'identité de dispositifs mobiles. Ils peuvent aussi leur être liés.

~~Les programmes et initiatives politiques des gouvernements, des organisations internationales et du secteur privé dans de nombreuses régions du monde conduisent à la reconceptualisation de « l'identité légale d'une personne »[2] de facto en « identité numérique nationale ». Pour renforcer ces évolutions, on assiste également à la promotion commerciale et à la marchandisation d'une "identité légale [numérique]" en tant que "droit humain fondamental" par les acteurs de l'identité du secteur privé.[3] Cette reconceptualisation d'une identité légale en "identité numérique nationale" a stimulé le développement de systèmes nationaux d'identité numérique (NIDS) qui, dans de nombreux cas, sont devenus une condition préalable à l'accès aux services et aux droits fondamentaux dans de nombreux pays.~~

L'une des principales justifications de la numérisation des systèmes d'identité juridique est que cela facilite ~~des systèmes d'identité nationale est qu'ils répondent à un droit humain fondamental, celui d'avoir une "identité légale".[4] Les NID facilitent~~ l'accès aux droits sociaux et économiques et fournissent des protections sociétales plus larges, telles que la sécurité personnelle et sociétale. Il est aussi argué que cela offre des avantages comme l'interopérabilité à l'intérieur et des frontières et à travers elles, que cela améliore l'exactitude

[1] Le concept d'identité juridique s'est développé à partir de l'article 6 de la Déclaration universelle des droits de l'homme, selon laquelle « Chacun a le droit à la reconnaissance en tous lieux de sa personnalité juridique ». L'Objectif de développement durable des Nations Unies (UN-SDG) 16.9 qui appelle à « garantir à tous une identité juridique, notamment grâce à l'enregistrement des naissances » lui a donné une impulsion. www.un.org/sustainabledevelopment/fr

~~[2] Le concept d'"identité légale" s'est développé à partir de l'article 6 de la Déclaration universelle des droits de l'homme, selon lequel "tout individu a **droit** à la reconnaissance en tous lieux de sa personnalité juridique". "Ce concept a été stimulé par la volonté d'atteindre l'objectif 16.9 des Nations unies pour le développement durable (UN-SDG), qui appelle à fournir "une *identité légale pour tous, y compris l'enregistrement des naissances*" d'ici 2030. https://www.un.org/sustainabledevelopment/fr/peace-justice/Voir également Manby, B (2020) *The Sustainable Development Goals and 'legal identity for all' : First, Do Not Harm* " https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3783299~~

~~[3] *Mastercard joins ID2020 Alliance* https://mastercardcontentexchange.com/newsroom/press-releases/2020/may/mastercard-joins-id2020-alliance/~~

~~[4] Selon la jurisprudence de la Cour européenne des droits de l'homme, l'identité d'une personne peut inclure l'origine ethnique d'une personne en tant qu'"*élément important de [sa] vie privée*" https://rm.coe.int/6608946-v6-case-law-guide-tt-protection-des-donnees-new-french-1st-ed-/1680a20aef l'identité peut "*englober de multiples aspects de l'identité d'une personne, tels que l'identification du genre et l'orientation sexuelle, le nom ou des éléments relatifs au droit d'une personne à son image*" et peut également inclure le droit à un nom et le droit à des documents d'identité. La CEDH a également estimé que l'utilisation de données biométriques et de profils ADN pour déduire l'origine ethnique peut violer le droit à l'identité ethnique d'une personne en vertu de l'article 8 de la CEDH - voir https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.~~

et la disponibilité des données, les prises de décisions des gouvernements et la fourniture des services publics et des mesures de protection sociales.

Si les~~un~~ système~~s~~ national~~ux~~ d'identité numérique (NIDS) [accronyme en français ?] peuvent comporter des avantages et des protections significatifs dans de multiples contextes et permettre aux individus d'obtenir et de faire valoir des droits importants, il~~s~~ peuvent aussi~~également~~ avoir des conséquences négatives pour les individus *et les* groupes. 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 d'une personne sur son identité ou la présentation de son identité par d'autres. ~~–~~Il s'ensuit donc que les « NIDS » devraient suivre une approche fondée sur les droits de l'homme, basée sur les droits de l'homme dès la conception (*human rights by design*) et intégrer~~ant~~ des évaluations de l'impact sur les droits de l'homme qui incluent ~~au-delà de~~ la protection des données et de la vie privée mais aillent aussi au-delà. Les valeurs des droits de l'homme devraient sous-tendre les NIDS.

~~Il est important de noter qu'il n'existe pas de définition universellement acceptée de l'"identité légale" ou de l'"identité numérique", et qu'il n'existe pas non plus de définition acceptée de l'"identité numérique nationale".~~ La définition d'''identité numérique nationale" apparait sous des définitions inadéquates dans les politiques, le droit et la pratique, de sorte que les systèmes d'identité numérique nationale peuvent ne pas prendre en compte de manière appropriée les risques pour les droits et libertés fondamentaux des individus (et des groupes), les prévoir ou les protéger. [5]

~~Les systèmes nationaux d'identité numérique impliquent la saisie électronique d'une série d'attributs concernant une personne, afin qu'elle soit identifiable de manière unique au sein d'une population et dans des contextes donnés. Les systèmes nationaux d'identité numérique évoluent rapidement et cherchent de plus en plus à intégrer des éléments biométriques tels que les empreintes digitales et les scans de l'iris, des identifiants d'appareils numériques ou même des attributs comportementaux numériques comme moyen de créer et de vérifier une "identité numérique".[6]~~ En 2011, le Conseil de l'Europe a adopté la résolution 1797 dans laquelle il s'inquiétait du fait que ces technologies puissent mettre en péril des droits de l'homme essentiels et appelait à une évaluation de ces risques et à l'adoption de mesures pour y faire face. [7] Les évolutions ont également conduit à lier ou à intégrer des systèmes d'identité tels que l'enregistrement obligatoire des cartes SIM mobiles sur la base de données biométriques dans les politiques et systèmes nationaux d'identité numérique, ainsi qu'à la possibilité de les relier et de les intégrer à d'autres systèmes comme les systèmes de

[5] Voir par exemple, *Robinson v The Attorney General of Jamaica* https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf ou Namati, (2019) *Case Filed to Stop New Digital ID Register in Kenya* https://namati.org/news-stories/case-filed-stop-new-digital-id-system-kenya/

~~[6] Voir Access Now, (2018) *National Digital Identity Programmes: What's Next* https://www.accessnow.org/cms/assets/uploads/2018/03/Digital-Identity-Paper-digital-version-Mar20.pdf et Digital Identity Trends - 5 forces that are shaping 2021 https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/digital-identity-services/trends et Kloppenburg et Ploeg, (2018) *Securing Identities : Biométric Technologies and the Enactment of Human Bodily Differences* https://www.tandfonline.com/doi/full/10.1080/09505431.2018.1519534.~~

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

surveillance des véhicules[8] ou de reconnaissance[9] ou de vérification des visages.[10] Ces développements ajoutent aux risques et préjudices potentiels qui peuvent découler de systèmes d'"identité numérique nationale" qui ne prennent pas en compte de manière appropriée leur impact sur les droits de l'homme et les libertés fondamentales d'une personne.

Ceux qui sont censés bénéficier des systèmes nationaux d'identité numérique sont en droit d'attendre que ces systèmes respectent et sauvegardent leurs droits de l'homme et leurs libertés fondamentales, et en particulier le droit à la vie privée conformément à l'article 8 de la Convention européenne des droits de l'homme et à la jurisprudence.[11] Et comme le juge Sykes l'a soutenu dans l'affaire *Robinson c. Le procureur général de la Jamaique*, des droits tels que la vie privée "*sont la propriété de toutes les personnes du simple fait d'être humain*"[12], et par conséquent, les systèmes nationaux d'identité numérique devraient prendre en compte les droits qui découlent de "l'être humain", en particulier pour ceux qui luttent pour affirmer ou qui sont autrement privés d'une identité légale.

Compte tenu de ce qui précède, ces lignes directrices soutiennent une approche des droits de l'homme dès la conception qui inclut la nécessité d'un engagement des parties prenantes dans l'identification et l'évaluation des impacts négatifs possibles des NIDS sur les droits et libertés fondamentaux des individus *et des* groupes. Cette approche exige que les parties prennent en compte de manière appropriée les besoins, les problèmes et les risques des NIDS tels qu'identifiés par les communautés et/ou leurs représentants. Comme l'affirme Beduschi, "les *plateformes d'identité numérique ne contribueront efficacement à la protection des droits de l'homme que si elles sont conformes au [droit international des droits de l'homme], si elles limitent les risques de manière adéquate… et si elles encouragent des normes élevées en matière de protection de la vie privée et des données*"[13], conformément à la jurisprudence de la Convention européenne des droits de l'homme, par exemple.[14]

2. Portée et objectif

2.1 Ces lignes directrices ont une portée générale, s'appliquent aux secteurs public et privé et visent à appliquer les principes et autres dispositions clés de la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement des données à caractère personnel ("Convention 108+")[15] à l'élaboration et à la mise en œuvre des systèmes nationaux d'identité numérique (NIDS).

2.2 S'appuyant notamment sur l'article 10(2) de la Convention 108+, ~~c~~les lignes directrices établissent un ensemble de mesures de référence que les décideurs politiques et autres

[8] Des dispositifs qui peuvent également inclure la reconnaissance faciale. Voir Harper, J (2018) *The new National ID Systems,* disponible à l'adresse : https://www.cato.org/policy-analysis/new-national-id-systems#real-id-and-e-verify

[9] Voir Unwanted Witnesses: Uganda's facial recognition technology threatens Privacy, disponible à l'adresse : https://www.unwantedwitness.org/ugandas-facial-recognition-technology-threatens-privacy/

[10] Voir BBC News: Singapore in world first for facial verification, disponible à l'adresse : https://www.bbc.co.uk/news/business-54266602

[11] Cour européenne des droits de l'homme, (2019) Guide sur l'article de la Convention européenne des droits de l'homme https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf.

[12] Para. 175. *Robinson c. Le procureur général de Jamaïque* https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

[13] Beduschi, A (2019) *Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights,* disponible à l'adresse *:* https://journals.sagepub.com/doi/pdf/10.1177/2053951719855091

[14] Voir, par exemple, les références à l'identité dans ce *Guide sur l'article 8 de la Convention européenne des droits de l'homme*, publié par la Cour européenne des droits de l'homme (2020) https://www.echr.coe.int/Documents/Guide_Art_8_ENG.pdf et dans ce Guide de la jurisprudence de la Cour européenne des droits de l'homme, Protection des données (2020) https://rm.coe.int/guide-data-protection-eng-1-2789-7576-0899-v-1/1680a20af0.

[15] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=090000168007c65bf

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 mais les prennent correctement en compte. Il est prévu que ~~l~~ces lignes directrices contribuent à encourager à ce que les NIDS ~~une approche centrée sur les droits de l'homme afin de garantir que les systèmes nationaux d'identité numérique soient conçus dès le début pour~~ respectent~~r~~ et protègentéger~~r~~ les droits et libertés fondamentaux, non seulement des individus mais aussi des groupes.

2.3 Adoptant une approche de précaution fondée sur les articles 5 et 6 de la Convention 108+, les lignes directrices soulignent la nécessité d'appliquer les principes de proportionnalité et de nécessité aux politiques, à la conception, à la mise en œuvre et au fonctionnement des systèmes nationaux d'identité numérique. ~~et, e~~En particulier, elles insistent sur la nécessité de renforcer la protection de l'utilisation de catégories spéciales de données que sont les données biométriques. Elles demandent ~~Cela nécessite~~ une évaluation objective des avantages par rapport à l'interférence avec les droits et les libertés ~~de l'homme~~ fondamentaux, en soutenant les objectifs de politiques justifiés tout en minimisant les risques pour les individus *comme pour les* groupes.

2.4 Les lignes directrices ne remplacent pas les mesures requises par la loi pour prévenir les risques d'atteinte aux intérêts, aux droits et aux libertés fondamentales des personnes et rien dans ces lignes directrices ne doit être interprété comme excluant ou limitant les dispositions de la Convention européenne des droits de l'homme et de la Convention 108+.[16]

3. Principes de protection des données à caractère personnel et des droits et libertés fondamentaux

Lorsque l'on envisage le traitement de données à caractère personnel pour atteindre les objectifs des NIDS, il est crucial de ~~commencer par l'article 1 de la Convention 108+ qui exige le **respect** des **droits de l'homme** et des **libertés fondamentales** d'un individu, et en particulier de son **droit à la vie privée**~~ **réfléchir** à ce que dit le ~~. Tout aussi important est le~~ préambule de la Convention 108+ et à la nécessité de « *garantir la dignité humaine ainsi que la protection des droits de l'homme et des libertés fondamentales de toute personne* ». Le préambule du Rapport explicatif de la Convention 108+~~, qui~~ stipule également 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"***.~~"~~[17] L'inclusion croissante de la biométrie dans les NIDS, qui rendent les personnes~~"~~ lisibles par des machines, porte en elle le risque de réduire les individus à des objets, sans considérations de dignité humaine ainsi que le risque d'autres conséquences négatives sur les droits et les libertés.

La Convention 108+ établit les principes, obligations et droits clés qui doivent s'appliquer lors du traitement des données personnelles et des catégories spéciales de données telles

[16] Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, STE 108, disponible sur https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108

[17] Convention 108+, Rapport explicatif sur le préambule, paragraphe 10, https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f

que les données biométriques, et qu'il est essentiel d'intégrer dans les politiques gouvernementales ainsi que dans la conception, la mise en œuvre et le fonctionnement des systèmes nationaux d'identité numérique. Les personnes ne doivent pas devenir de simples objets représentés par ~~leurs~~ des identités numérisées que d'autres leur affectent.

3.1 Légitimité du traitement

Comme le prévoit l'article 5 de la Convention 108+, le traitement des données à caractère personnel (et des catégories particulières de données) doit avoir une base légitime établie par la loi, telle qu'une loi nationale sur la protection des données ou toute autre loi ou réglementation.[18] L'article 6 de la Convention 108+ exige en outre que le traitement de catégories particulières de données, telles que les données biométriques ou les données révélant l'origine ethnique d'une personne (souvent utilisées dans les NIDS), soit soumis à des garanties appropriées inscrites dans le droit interne.

Les NIDS interfèrent ~~et ont des implications significatives~~ sur les droits et libertés fondamentaux, en particulier le droit à la vie privée et à la protection des données et ont sur eux des implications significatives. Par conséquent, une loi nationale omnibus sur la protection des données, alignée sur la Convention 108+, devrait *être ~~établie~~ mise en place en priorité* pour fournir une base légitime fondamentale, des règles et des garanties. Une loi nationale sur la protection des données devrait ~~informer~~ prendre en compte ~~et être une condition préalable à~~ l'introduction d'un NIDS et en être une condition préalable.

Un NIDS doit avoir une base ~~légitime~~ juridique spécifique séparée, établie dans le droit national et seulement après qu'une évaluation appropriée ait été menée.[19] Les NIDS doivent servir de véritables objectifs répondant à un besoin social pressant, considérés comme nécessaires *et* proportionnés dans une société démocratique, plutôt que d'être utilisés pour des raisons de commodité ou d'être justifiés comme "souhaitables". Cela exige que leur champ d'application ~~des NIDS~~ et les objectifs spécifiques du traitement des données personnelles et des catégories spéciales de données proposés dans le cadre des NIDS fassent l'objet d'une évaluation de leur impact sur les droits de l'homme et les libertés des individus (et des groupes), y compris une évaluation des garanties appropriées pour limiter et atténuer les risques pour les droits et libertés.

3.2 Équité et transparence

L'article 5, paragraphe 4, point *a*) et *b)* et l'article 8 de la Convention 108+ exigent ~~que le traitement d~~les données d'une personne soit ~~effectué~~ traitées de manière loyale et transparente pour elle. ~~La loyauté et la transparence sont également nécessaires pour garantir la légitimité du traitement.~~

~~La légitimité du traitement des données à caractère personnel et des catégories particulières de données personnelles dépend non seulement du fait que les NIDS soient inscrits dans la loi,~~ Cela suppose non seulement de~~mais aussi de la~~ garanti~~e~~r que la portée et l'objectif de la~~cette~~ loi sur les NIDS sont prévisibles et accessibles mais aussi que ~~. Elle~~

[18] https://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-FR-HRFILES-15(1997).pdf
[19] Ibid.

~~dépend également de la garantie que le traitement des données soit transparent et équitable pour~~ les individus et les groupes soient en position ~~auxquels ils peuvent appartenir et que des garanties appropriées sont établies pour assurer le respect et la protection des droits et libertés des personnes *et des* groupes touchés par les NIDS.~~

~~Les personnes et les groupes doivent être capables~~ de comprendre clairement :

- quelles données personnelles et catégories particulières de données personnelles, comme les données biométriques, seront traitées et à quelles fins spécifiques et explicites ;
    - ~~Il s'agit notamment de savoir si les données d'identité numérique nationale telles que le numéro national d'identification (NIN en anglais) seront partagées avec d'autres systèmes dépendant de l'identité nationale ou accessibles à ceux-ci, ou si elles seront requises pour ces systèmes, et pourquoi. Par exemple, si l'identité nationale sera requise pour obtenir une carte SIM mobile ou pour accéder à l'éducation ou aux soins de santé et quelles données d'identité nationale seront enregistrées en conséquence ;~~
    - ~~si un numéro national d'identification sera lié à d'autres identificateurs uniques (et la base légale pour cela) tels qu'un numéro de téléphone mobile, un numéro d'identité électronique de carte SIM mobile,[20] ou un numéro d'équipement électronique d'un téléphone mobile,[21] par exemple et qui peuvent 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.~~
- si la fourniture de données pour établir une identité numérique nationale est volontaire ou obligatoire, et quelles sont les conséquences de ne pas fournir de données pour établir une identité numérique ;
- les contextes dans lesquels la présentation ultérieure de la preuve d'une identité numérique nationale est une exigence obligatoire ou volontaire et les conséquences du refus de la fournir (par exemple le refus d'accès aux services ou l'obtention d'un téléphone mobile) ;
- si les données de l'identité numérique nationale, comme un numéro national d'identification (NIN), seront partagées avec d'autres systèmes d'identité nationales dépendant ou accessibles ou encore demandés par eux 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 ?
- si un NIN sera lié à d'autres identifiants uniques (et quelle sera la base juridique pour cela), par exemple un numéro de téléphone mobile, le numéro d'identifiant d'une carte SIM électronique[22] ou le numéro d'équipement électronique d'un téléphone portable[23], 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 ;

~~[20] Par exemple, l'identité internationale de l'abonné mobile (IMSI) qui identifie de manière unique chaque carte SIM sur un réseau mobile https://fr.wikipedia.org/wiki/Carte_SIM~~
~~[21] Par exemple, le numéro d'identité international d'équipement mobile (IMEI) qui identifie de manière unique un téléphone mobile sur un réseau mobile https://fr.wikipedia.org/wiki/International_Mobile_Equipment_Identity~~

[22] Par exemple, l'identifiant international des abonnés mobiles (IMSI) qui identifie de manière unique chaque carte SIM d'un réseau mobile https://en.wikipedia.org/wiki/International_mobile_subscriber_identity https://fr.wikipedia.org/wiki/International_Mobile_Subscriber_Identity
23 Par exemple, l'identité internationale d'équipement mobile (IMEI) qui identifie de façon unique u téléphone portable sur un réseau de téléphonie mobile https://fr.wikipedia.org/wiki/International_Mobile_Equipment_Identity

- l'existence des~~les~~ droits et la manière de les exercer ;
- comment faire corriger facilement les données enregistrées inexactes et comment mettre à jour leur enregistrement (ce qui devrait être gratuit~~ement))~~ ;
- la base d'une exclusion du NIDS (par exemple l'absence de preuve de la naissance) ;
- comment obtenir réparation.

Il est important que, lorsque les NIDS requièrent le traitement de données biométriques, un autre moyen d'inclusion soit prévu pour les personnes qui ne sont pas en mesure de fournir des données biométriques[24] ou dont les données biométriques sont illisibles[25] ou deviennent illisibles. [26] Cela contribuera à garantir l'*équité* et à *prévenir l'exclusion*.

L'équité exige également que les communications relatives au NIDS et au traitement des données personnelles et des catégories spéciales de données soient appropriées et intelligibles pour les diverses communautés que le NIDS est censé servir.[27]

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

Avant la mise en œuvre des NIDS, il est important que les politiques et la législation nationales sur les NIDS ~~définissent~~ précisent explicitement les objectifs légitimes et autorisés pour lesquels les données personnelles et les catégories spéciales de données (telles que les données biométriques) sont *nécessaires* et quelles données précises sont jugées *nécessaires* pour atteindre ces objectifs. Cela permettra de remplir les conditions d'un traitement légitime et de la limitation des finalités prévues par ~~e répondre à l'exigence de l'a~~l'article 5, paragraphe 4, point *b*), de la Convention 108+ et d'éviter que les données soient traitées dans des finalités imprécises, vagues ou incompatibles. Il est aussi nécessaire de respecter les~~ainsi qu'aux~~ obligations de conception contenues dans l'article 10 de la Convention 108+.[28]

Les responsables du traitement et les autres entités qui fournissent du matériel, des logiciels et des services permettant la mise en œuvre du NIDS doivent veiller à ce que, de la conception à la mise en œuvre et à l'exploitation, en passant par le traitement des données, seules soient traitées les données nécessaires à une finalité spécifiée par la loi NIDS ou toute autre législation appropriée. Les données ne doivent pas être utilisées à des fins incompatibles avec les objectifs spécifiés (par le NIDS).

Conformément aux principes de légitimité, de loyauté et de transparence, les données personnelles et les catégories particulières de données personnelles traitées dans le cadre du NIDS ne doivent pas être traitées d'une manière qui serait inattendue, inappropriée ou

[24] Voir, The Wire (2017) *Incapable de vérifier les empreintes digitales ou l'iris, Aadhaar refuse aux patients lépreux des services de base* https://thewire.in/government/unable-verify-fingerprints-iris-aadhaar-denies-leprosy-patients-basic-services.
[25] Voir par exemple, Drahansky et al, (2012) *Influence of Skin Diseases on Fingerprint Recognition* https://www.hindawi.com/journals/bmri/2012/626148/.
[26] L'association mondiale du commerce mobile, la GSMA, rapporte qu'au Kenya, dans le cadre d'un programme de protection sociale, les personnes âgées et celles qui effectuent un travail manuel, n'ont pas pu fournir de preuve d'identité (appelée " preuve de vie " dans le programme) car leurs empreintes digitales n'étaient plus lisibles par le scanner biométrique. GSMA, (2020) *Opportunités d'amélioration de l'identification numérique dans les transferts sociaux en espèces* https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/04/SCT_Report_R_WebSingles.pdf
[27] Voir par exemple le paragraphe 68 du rapport explicatif sur l'article 8 de la Convention 108+
[28] Le paragraphe 89 du Rapport explicatif de la Convention 108+ Article 10 - Obligations supplémentaires, exige « 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). »

auxquelles les personnes concernées pourraient s'opposer. Tout traitement qui aurait de telles conséquences doit être clairement établi par la loi et soumis à une évaluation de tout impact négatif potentiel sur les droits de l'homme des personnes et des groupes.

L'utilisation secondaire des numéros d'identification nationaux et des autres données collectées aux fins de l'identité numérique nationale devrait être interdite, sauf à des fins clairement prévues par la loi.

3.4 Qualité des données - Exactes, adéquates, pertinentes et non excessives

Exactes

Des données inexactes peuvent avoir des conséquences négatives importantes sur les droits de l'homme des personnes. Elles peuvent, par exemple, conduire à des soupçons erronés d'activités criminelles ou d'autres infractions à la loi et/ou à des arrestations et des emprisonnements injustifiés. Elles peuvent conduire à l'exclusion de services ou de mesures de protection sociale. Elles peuvent aussi entraîner une discrimination. Pour toutes ces raisons, il est crucial que des mesures soient adoptées pour garantir l'exactitude de toute donnée personnelle ou de catégorie spéciale de données traitée et que les données personnelles inexactes puissent être corrigées ou supprimées rapidement.

Il est crucial de garantir l'exactitude des données traitées dans les NIDS. Cela est particulièrement vrai lorsque les NIDS nécessitent l'enregistrement de données biométriques et que ces dernières peuvent être liées à d'autres systèmes basés sur l'identité, comme la reconnaissance faciale, ou lorsque les NIDS peuvent refuser à des personnes l'accès à des services essentiels tels que la connectivité mobile, les soins de santé, l'éducation ou la migration en raison de données inexactes.

L'utilisation de données biométriques dans les NIDS exige des mesures supplémentaires pour garantir l'exactitude des données biométriques acquises, enregistrées et appariées et pendant l'exécution des aspects des NIDS qui exigent qu'une personne présente ses données biométriques pour prouver son identité ou son authentification.[29] Elle exige également des mesures visant à réduire les biais et les inexactitudes des techniques et technologies d'identité biométrique et à renforcer l'équité.[30] Il est impératif que la vérification de l'"exactitude" soit une exigence fondamentale de l'approche des droits de l'homme dès la conception (*human rights by design*) et avant l'acquisition et la mise en œuvre des technologies d'identité biométrique.

Il est fondamental d'établir et de maintenir la capacité à mettre à jour les données. Les personnes doivent disposer d'un moyen simple et gratuit pour mettre à jour leurs informations, par exemple en cas de changement de nom, d'adresse ou de coordonnées.

Les obligations en matière de protection des données visant à garantir l'exactitude des NIDS requièrent également la possibilité de dissocier les identités. Par exemple, un

[29] Voir, par exemple, les lignes directrices du Conseil de l'Europe sur la reconnaissance faciale, (2021) https://rm.coe.int/lignes-direectrices-sur-la-reconnaissance-faciale/1680a134f4 et les conseils sur la *reconnaissance biométrique et les systèmes d'authentification* du UK National Cyber Security Centre, https://www.ncsc.gov.uk/collection/biometrics/measuring-performance.
[30] Bureau des sciences du gouvernement britannique, (2018) Biométrie : un guide https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/715925/biometrics_final.pdf

gouvernement peut imposer aux personnes l'obligation légale d'enregistrer leur numéro national d'identification et/ou leurs données biométriques auprès des opérateurs de téléphonie mobile afin d'obtenir une carte SIM prépayée pour téléphone portable (ce que l'on appelle "enregistrement obligatoire de la carte SIM"[31]). Les opérateurs mobiles peuvent être tenus par la loi de vérifier ces données par rapport à une base de données d'identités numériques nationales ou de capturer ces données et de les enregistrer dans une base de données d'identités numériques nationales. Le numéro d'identité national et/ou les données biométriques d'une personne seront liés à une série d'identifiants uniques tels que le numéro de téléphone mobile ou les identifiants uniques de ses appareils.[32] Lorsqu'une personne se défait de son numéro de téléphone mobile ou lorsqu'un opérateur de téléphonie mobile annule le service d'un numéro, ce dernier peut être recyclé pour une autre personne. De même, une personne peut se débarrasser de son téléphone portable - en le transmettant à un membre de sa famille ou en le revendant. Les identifiants uniques ne seront donc plus en possession ni utilisés par la personne à laquelle ils étaient initialement liés. Il est important de considérer également que les NIDS et les identités mobiles associées peuvent également être liés aux identifiants des services financiers par le biais de la réglementation relative à la lutte contre le blanchiment d'argent ou à la connaissance du client (KYC). Étant donné que la justification de l'enregistrement obligatoire des cartes SIM, voire de la lutte contre le blanchiment d'argent et de la connaissance du client, est la "nécessité" d'assurer la sécurité nationale et de réduire la criminalité, l'absence d'exactitude des données dans la liaison entre identifiants mobiles et identité nationale d'une personne peut aggraver les conséquences négatives existantes et potentielles pour ses droits de l'homme.

Adéquates, pertinentes et non excessives (minimisation des données)

Seules les données minimales nécessaires doivent être traitées pour atteindre un ou plusieurs objectifs spécifiques identifié et légitime. Pour ce faire, ~~comme pour ce qui précède,~~ il faut d'abord définir la finalité et s'assurer de l'existence d'une base légitime appropriée - qui, pour les NIDS, doit être spécifiée dans la loi.

Les données doivent être proportionnées et suffisantes pour répondre aux objectifs identifiés et spécifiques et ne pas être excessives pour ces objectifs. Le traitement de données à caractère personnel ou de catégories particulières de données qui entraînerait une ingérence disproportionnée dans les droits et libertés fondamentaux des personnes et des groupes serait considéré comme excessif au regard de la Convention 108+.[33]

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 (comme l'autorise la loi sur le NIDS) ne contiennent que les informations suffisantes pour répondre à un objectif précis afin d'empêcher une utilisation abusive ou incompatible des modèles biométriques.

[31] GSMA, Accès aux services mobiles et preuve d'identité 2021 : Revisiting SIM Registration and Know Your Customer (KYC) Contexts during COVID-19 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf
[32] Voir les notes de bas de page 19 et 20.
[33] Article 5 - Légitimité du traitement des données et qualité des données du Rapport explicatif de la Convention 108+ paragraphe 52

Le traitement des données aux fins d'un NIDS doit toujours être justifié et nécessaire pour atteindre un objectif spécifique défini par la loi. Déterminer quelles données sont nécessaires et quelle est la qualité des données nécessaires pour atteindre une finalité spécifique légitime pour le NIDS doit être précédé d'une évaluation commençant par les politiques, examinant ensuite la loi, la conception et la pratique, et doit en partie recueillir des informations auprès des parties prenantes engagées, comme indiqué ci-dessous. La qualité des données doit faire partie d'un cycle continu d'évaluation et d'adaptation aux résultats et aux événements. Ces obligations et exigences doivent également inclure d'autres systèmes qui dépendent du NIDS, tels que l'enregistrement obligatoire des cartes SIM, des programmes d'identification des réfugiés, des programmes de surveillance par reconnaissance faciale, etc.

De bonnes pratiques de gestion de la qualité des données peuvent contribuer 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 ainsi qu'à la gestion efficace des services dépendant de ces identités. [34]

3.5 Conservation des données

La conservation d~~l~~es données personnelles et ~~l~~des catégories particulières de données doit être proportionnée et nécessaire ~~ne doivent être conservées que le temps nécessaire~~ à la réalisation de l'~~un~~ objectif spécifique justifié et légitime. Une attention particulière doit être portée à la conservation de catégories de données comme les données biométriques.

Les données~~et~~ doivent être supprimées ou rendues anonymes lorsque la finalité spécifique du traitement a été atteinte ou lorsqu'elles ne sont plus nécessaires. Cela doit inclure la prise en compte des données traitées dans des systèmes qui sont intégrés dans les NIDS ou dont les NIDS tirent des données~~dépendent ou qui dépendent autrement des NIDS~~. Par exemple, les systèmes de reconnaissance faciale, les systèmes d'enregistrement obligatoire des cartes SIM ou les systèmes de contrôle des frontières.

Par exemple, un modèle biométrique doit être supprimé s'il n'est plus lisible en raison de la dégradation des données biométriques de la personne à partir de laquelle il a été créé à l'origine, de sorte que ce modèle est inutilisable. Un autre exemple est le re-enregistrement de données biométriques telles que les empreintes digitales, les scans de visages 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 mesures de sécurités appropriées.

3.6 Sécurité du traitement

Les NIDS impliquent le traitement de données (souvent sensibles) à l'*échelle d'une population* et peuvent même contenir des données sur des groupes spécifiques vulnérables

[34] 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, http://www.fao.org/3/nf601en/nf601en.pdf.

et à risque. Manquer à assurer la sécurité des données et des systèmes peut entraîner des conséquences négatives graves pour les personnes et les groupes. ~~Les NIDS peuvent s'interconnecter ou inclure d'autres systèmes basés sur l'identité qu'il est important de prendre en considération, tels que les bases de données de migration et d'application de la loi, ou les bases de données d'enregistrement obligatoire des cartes SIM~~

~~.~~[35] ~~–~~Il est essentiel que les responsables du traitement mettent en œuvre des ~~s'assurent que des~~ mesures *techniques* et *organisationnelles* qui protègent les données et les droits et libertés fondamentaux de personnes. Un défaut de sécurité peut entraîner un vol et/ou une divulgation non autorisée de données ce qui peut entraîner des dommages tels que harcèlement, persécution, fraude, usurpation d'identité. ~~appropriées sont mises en œuvre pour protéger les données détenues dans les systèmes nationaux d'identité et les autres systèmes liés à l'identité auxquels ils sont interconnectés. La corruption d'un système peut en corrompre d'autres.~~

~~Une sécurité "appropriée" nécessite une évaluation de la sensibilité des données concernées et des conséquences négatives potentielles pour les individus et les groupes ainsi que pour leurs droits et libertés fondamentaux. Une absence de sécurité appropriée peut entraîner un vol et/ou une divulgation non autorisée de données ce qui peut entraîner des dommages tels que harcèlement, persécution, fraude, usurpation d'identité.~~

Il est également important de considérer qu'une fois corrompues - volées par exemple - les données biométriques ne peuvent être remplacées ~~facilement~~, ou qu'une fois volés, les modèles biométriques peuvent être réutilisés.

~~Le principe de minimisation des données est une considération importante dans le contexte de la sécurité. Si on ne collecte pas de données, elles ne peuvent pas être compromises.~~

Les mesures appropriées peuvent inclure :

- d'assurer la minimisation des données dans la conception et le fonctionnement des systèmes – seules les données minimales nécessaires à une finalité spécifique et légitimes devraient être traitées. Il faut garder à l'esprit que si on ne collecte pas de données, elles ne peuvent pas être compromises ou être utilisées pour porter atteinte aux droits et libertés fondamentaux d'une personne ;
- d'évaluer le caractère sensible des données impliquées et les conséquences négatives potentielles pour les personnes ou les groupes et d'adopter des mesures afin de réduire les risques pour eux ;
- d'adopter et de mettre en œuvre des politiques et des procédures d'enquête et de gestion des incidents de sécurité susceptibles d'avoir des conséquences négatives pour les personnes ~~et leurs droits et libertés fondamentaux~~, ainsi que des procédures de signalement de ces incidents aux personnes et aux autorités de contrôle de la protection des données ;
- ~~d~~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 personnelles qu'ils contiennent ou auxquelles ils donnent accès ;

[35] Casagran, C (2021), *Fundamental Rights Implications of Interconnecting Migration and Policing Databases in the EU*, Human Rights Law Review, Volume 21, Issue 2, Juin 2021, Pages 433-457, https://academic.oup.com/hrlr/article/21/2/433/6131329

- de crypter les données en transit et fixes et de garantir que seuls des dispositifs fiables puissent accéder aux NIDS ;
- d'adopter et de mettre en œuvre des procédures pour enquêter sur les faiblesses de sécurité et y remédier et assurer une vérification régulière des mesures de 'sécurité' ;[36]
- de fournir des procédures internes et externes pour un signalement confidentiel des failles de sécurité ;[37]
- de tester régulièrement la sécurité des mesures de sécurité existantes et en tenir un registre ainsi que des mesures prises/à prendre pour remédier aux défaillances susceptibles de corrompre les données et affecter les droits et libertés des personnes~~.~~ ;
- de considérer un moyen de refuser en temps de crise l'accès aux systèmes et données d'identité nationaux, en particulier aux données biométriques ou d'en empêcher l'utilisation, lorsque ces données pourraient être utilisées intentionnellement contre des personnes.

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

3.7 Profilage et prise de décision automatisée

Les systèmes nationaux d'identité peuvent faciliter le profilage et la surveillance électronique des personnes, ce qui peut avoir des conséquences négatives importantes pour les droits de l'homme, comme l'ont souligné de manière éloquente des affaires juridiques telles que l'arrêt de la Cour suprême de Jamaïque.[38] ~~Cela peut notamment se produire lorsque les NIDS s'interconnectent avec des systèmes introduits pour faciliter la surveillance d'individus ou de groupes, ce qui peut être contraire au droit au respect de la vie privée conformément aux instruments internationaux relatifs aux droits de l'homme.~~[39] 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. [40]

[36] Par exemple, en 2017, des chercheurs ont informé les autorités estoniennes de l'existence d'un 'défaut' dans la puce électronique de la carte d'identité électronique, touchant environ 7 500 000 porteurs depuis 2014. Il a été rapport que le défaut permettait le décryptage des données privées des cartes concernées. https://news.err.ee/644250/gemalto-rep-estonian-authorities-notified-of-id-card-flaw-in-june A la suite de cet incident, les autorités estoniennes auraient poursuivi le fabricant privé de la puce électronique pour une amende de 152 million d'Euros https://www.reuters.com/article/estonia-gemalto-idUSL8N1WD5JZ Voir aussi la réponse de l'Estonie 'What we learned from the eID security risk? https://e-estonia.com/card-security-risk/

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

[38] https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

[39] ~~Déclaration du Comité des ministres du Conseil de l'Europe sur les risques pour les droits fondamentaux découlant du pistage numérique et d'autres technologies de surveillance, adoptée le 11 juin 2013 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ae15a et également référencée dans les Lignes directrices du Conseil de l'Europe sur la reconnaissance faciale, (2021) https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3.~~

[40] Recommandation CM/Rec(2010)13 et exposé des motifs du Conseil de l'Europe sur "La protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage". https://rm.coe.int/16807096c3

L'autorité britannique de protection des données reconnaît également les risques du profilage. Dans un article consacré à la proposition du gouvernement britannique de mettre en place un système d'identité numérique fiable,[41] le Bureau du commissaire à l'information du Royaume-Uni affirme que « le *profilage des données collectées à des fins d'identité numérique [...] pourrait être intrusif et impliquer que les organisations évaluent des données à la fois dans le système et en relation avec le système (comme la fréquence et l'endroit où elles ont effectué un contrôle d'identité) pour construire un portrait d'une personne. Il est important qu'aucune organisation n'utilise les données qu'elle collecte à des fins d'identité numérique pour un profilage plus large*. »[42] C'est un commentaire important étant donné la nature publique-privée possible des systèmes nationaux d'identité numérique ou des systèmes basés sur des systèmes nationaux d'identité numérique fédérés publics-privés qui utilisent des attributs de données personnelles détenus par les secteurs public et privé.

Le profilage (y compris les décisions automatisées) devrait être interdit dans les systèmes nationaux d'identité numérique et les systèmes associés, sauf si la loi le prévoit expressément. Toute finalité ainsi autorisée devrait être soumise à l'obligation de réaliser une évaluation préalable de l'impact sur les droits de l'homme. Les personnes devraient également se voir accorder des droits sur le profilage et la prise de décision automatisée, et toute exception à ces droits doit être clairement déterminée conformément à l'article 11 de la Convention108+. L'article 11 exige que les exceptions soient prévues par la loi (qui elle-même est accessible et prévisible) et qu'elles respectent l'essence des droits et libertés fondamentaux, et poursuivent un objectif légitime considéré comme une mesure nécessaire et proportionnée dans une société démocratique.

3.8 Droits de l'homme dès la conception (*human rights by design*) et évaluations d'impact sur les droits de l'homme

Les choix politiques et conceptuels peuvent avoir un impact négatif sur la vie privée et les autres droits et libertés fondamentaux, notamment en ce qui concerne les systèmes nationaux d'identité numérique. 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* ». De même, les lois sur la protection des données telles que le Règlement général sur la protection des données de l'UE[43] peuvent exiger que les responsables du traitement adoptent une "protection des données dès la conception et par défaut" et comme des lois comme le *Mauritius Data Protection Act* 2017[44] exigent des évaluations d'impact sur la protection des données avant tout traitement lorsqu'il est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes.

[41] https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework
[42] Prise de position du commissaire à l'information sur la proposition du gouvernement britannique concernant un système d'identité numérique fiable (2021)
https://ico.org.uk/media/about-the-ico/documents/2619686/ico-digital-identity-position-paper-20210422.pdf
[43] https://ec.europa.eu/info/law/law-topic/data-protection_en
[44] Voir l'article 34 https://dataprotection.govmu.org/Documents/The%20Law/Act%20No.%2020%20-%20The%20Data%20Protection%20Act%202017.pdf

Comme évoqué précédemment, les NIDS peuvent être une combinaison d'arrangements publics et privés et, de technologies. et de soutien. Pour faire suite à la Il est important de tenir compte de la recommandation du Conseil des Ministres du Conseil de l'Europe[45], les Parties à la Convention 108+ qui demande aux États membres d'encourager devraient ou d' exiger des entreprises qu'elles "montrent une *diligence raisonnable en matière de droits de l'homme ... incluant des évaluations de l'impact sur les droits de l'homme spécifiques à un projet, le cas échéant ...*". Ces lignes directrices sont conformes aux objectifs juridiques de la Convention 108+ et de lois nationales sur la protection des données, ainsi qu'à l'objectif de la recommandation susmentionnée qui est de garantir une diligence raisonnable appropriée. L'obligation de procéder à une diligence raisonnable et à des évaluations d'impact sur les droits de l'homme s'applique également au secteur public lorsqu'il envisage l'adoption de NIDS.

S'écartant des termes utilisés dans la loi et même dans la Convention 108+, ces lignes directrices utilisent les termes d'évaluations d'impact sur les droits de l'homme (EIDH) et de droits de l'homme dès la conception (DHCD) afin de garantir une approche de l'identité numérique nationale fondée sur les droits de l'homme. Cela exige d' Le processus fondé sur les droits de l'homme doit commencer par l'identifiercation et dl'impliquercation des parties prenantes (engagement des parties prenantes), et en particulier des titulaires de droits concernés. Cela permettra d'identifier non seulement les risques pour les NIDS eux-mêmes, mais aussi pour les droits de l'homme des personnes sur lesquelles les NIDS auront un impact. Les NIDS ne peuvent être conçus pour éviter ou minimiser 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 systèmes nationaux d'identité (numérique) (NID) peuvent entrainer pour les détenteurs de droits. Les mises en question juridiques et de la société civile, que ce soit au Royaume-Uni[46], au Kenya[47] ou en Jamaïque,[48] révèlent l'importance de comprendre l'impact et les conséquences des NID pour les détenteurs de droits, ainsi que la nécessité de concevoir et de garantir la responsabilisation en matière de droits de l'homme. L'implication des parties prenantes est cruciale pour faciliter un dialogue sur les problèmes que les NIDS cherchent à résoudre, et pour faire apparaître les intérêts, les attentes, les besoins et les préoccupations des détenteurs de droits concernés, ainsi que les avantages et les risques tels qu'ils les perçoivent.[49] Une telle implication donne une voix nécessaire aux détenteurs de droits affectés et les aide à renforcer leurs pouvoirs en reflétant leurs expériences vécues et leurs besoins et peut aider à établir la confiance dans les propositions.[50]

[45] Conseil de l'Europe. Recommandation CM/Rec (2016)3 du Comité des Ministres aux États membres sur les droits de l'homme et les entreprises https://rm.coe.int/human-rights-and-business-recommendation-cm-rec-2016-3-of-the-committe/16806f2032.

46 La loi britannique de 2006 sur les cartes d'identité a été abrogée en 2010 après un examen minutieux et une campagne de la société civile. https://spyblog.org.uk/ssl/spyblog/identity-documents-bill/

47 *Nubian Rights Forum & 2 others v Attorney General & 6 others* ; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR https://www.khrc.or.ke/publications/214-judgement-on-niims-huduma-namba/file.html

48 2019, *Robinson c. Procureur général de la Jamaïque*, Cour suprême, demande n° 2018HCV01788 https://supremecourt.gov.jm/sites/default/files/judgments/Robinson%2C%20Julian%20v%20Attorney%20General%20of%20Jamaica.pdf

[49] Voir par exemple, la salle des machines, 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, Identités : Les nouvelles pratiques à l'ère connectée (2017) https://www.identitiesproject.com/wp-content/uploads/2017/11/Identities-Report.pdf

50 2021, Satterthwaite, M. *Critical legal empowerment for human rights* https://www.openglobalrights.org/critical-legal-empowerment-for-human-rights/?lang=English

Un bon exemple d'engagement des parties prenantes peut être trouvé au Royaume-Uni. L'Institut Ada Lovelace a récemment créé le *Citizens Biometrics Council* (CBC) afin de "*délibérer* publiquement *sur l'utilisation des technologies biométriques telles que la reconnaissance faciale"*, notamment sur les préoccupations relatives à l'identité, aux biais et à la discrimination que les données biométriques peuvent engendrer. Un rapport qui s'en est suivi sur les recommandations et les conclusions du CBC[51] affirme que "*la consultation continue et la représentation d'un échantillon représentatif de la société sont fondamentales pour garantir que les technologies biométriques ne soient déployées que d'une manière fiable, responsable et acceptable".* Ceci est vrai pour les NIDS si l'on veut qu'ils soient considérés comme légitimes, dignes de confiance et qu'ils respectent et protègent les droits et libertés fondamentaux, en particulier les NID qui intègrent la biométrie. Une consultation efficace des parties prenantes devrait être considérée comme une exigence politique et juridique fondamentale des systèmes basés sur l'identité qui, par nature, interfèrent avec le droit à la vie privée et peuvent créer des risques pour d'autres droits et libertés. La consultation des parties prenantes devrait être un élément clé des évaluations d'impact et de la conception.

L'Institut danois pour les droits de l'homme (DIHR) a produit un document utile sur l'engagement des parties prenantes, en complément de son guide d'évaluation de l'impact sur les droits de l'homme.[52] Si les conseils sur l'engagement des parties prenantes et les droits de l'homme semblent avoir leurs racines dans les industries extractives,[53] et/ou le secteur des entreprises[54], des conseils tels que ceux du DIHR peuvent offrir une base sur laquelle envisager un engagement efficace des parties prenantes dans le contexte des NID.

Ces orientations suggèrent qu'il est essentiel de consulter les principales parties prenantes suivantes dans le cadre des programmes nationaux d'identité numérique. Il ne s'agit pas d'une liste exhaustive de parties prenantes, mais elle comprend les éléments suivants :

- **Gouvernement**
  - Les principaux départements, agences et ministères du gouvernement responsables ~~de~~ :
    - des t~~T~~echnologies d'information et de communication (TIC)
    - de l'agenda et de l~~éc~~'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

51 Rapport des recommandations et des conclusions de la délibération publique sur la technologie, la politique et la gouvernance en matière de biométrie (2021) https://www.adalovelaceinstitute.org/wp-content/uploads/2021/03/Citizens_Biometrics_Council_final_report.pdf
52 Guide et boîte à outils pour l'évaluation de l'impact sur les droits de l'homme : Supplément pour les praticiens de l'engagement des parties prenantes https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/stakeholder_engagement/stakeholder_engagement_prac_sup_final_jan2016.pdf
53 Voir par exemple https://www.oecd.org/daf/inv/mne/OECD-Guidance-Extractives-Sector-Stakeholder-Engagement.pdf
54 voir https://www.ohchr.org/Documents/Publications/HR_PUB_12_2_fr.pdf

        - de l'approvisionnement
        - de la protection des données
        - des droits de l'homme
- **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 ~~ou~~ et des responsabilités en matière de droits de l'homme
    - Autorités chargées de la protection des données
    - Commissions des droits de l'homme ou de l'égalité[55]
    - 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[56]
    - Associations des barreaux
    - Organisations communautaires qui soutiennent la résolution des conflits en matière de droits de l'homme
- **Détenteurs et représentants des droits**
    - Représentants associatifs
    - Société civile / Organisations de défense des droits de l'homme[57]
    - Conseils de citoyens
- **Secteur de l'entreprise**
    - Fournisseurs d'identification - matériel et logiciels
    - Associations professionnelles
    - Opérateurs mobiles[58]
    - Services financiers/agents de monnaie mobile
- **Université / Recherche**
    - Universitaires spécialisés dans l'identité numérique nationale et les droits de l'homme
    - Institutions axées sur l'identité numérique nationale et les droits de l'homme[59]
- **Acteurs internationaux**
    - Organisations humanitaires
    - Banque mondiale
    - Organisations des Nations unies[60]
    - Union internationale des télécommunications (UIT)

[55] Par exemple, le chancelier de la justice d'Estonie https://www.oiguskantsler.ee/en.
[56] 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.
[57] Par exemple, des organisations telles que Namati et le réseau d'autonomisation juridique https://namati.org/network/.
[58] 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) https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/04/Digital-Identity-Access-to-Mobile-Services-and-Proof-of-Identity-2021_SPREADs.pdf.
[59] 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' https://digitalid.design/*
[60] Voir par exemple l'Agence des Nations unies pour les réfugiés, Enregistrement et gestion de l'identité https://www.unhcr.org/registration.html ou le PNUD https://unstats.un.org/legal-identity-agenda/meetings/2021/UNLIA-FutureTech/docs/Agenda.pdf.

- Organisation de coopération et de développement économiques (OCDE)
- Union africaine
- Commission africaine des droits de l'homme
- Conseil de l'Europe
- UE[61]

Esteves et al, écrivent que « l'*égalité et la non-discrimination, la participation et l'inclusion, la responsabilité et la transparence constituent les principes clés qui sous-tendent une approche fondée sur les droits de l'homme. La non-discrimination signifie que divers groupes de titulaires de droits - en particulier les personnes vulnérables, les femmes, les enfants, les peuples autochtones et d'autres groupes marginalisés - nécessitent une attention particulière pour pouvoir jouir de leurs droits fondamentaux*. » [62] Les programmes nationaux d'identité numérique exigent un engagement et une responsabilisation des parties prenantes qui soient inclusifs et participatifs.

Évaluations d'impact sur les droits de l'homme et "*Human Rights by Design*" (droits de l'homme dès la conception)

Les cadres de protection des données comme la Convention 108+ et le RGPD exigent que l'on prenne en considération les risques pour les intérêts, les droits et les libertés fondamentales des personnes et que l'on protège contre de telsces risques par le biais d'une série de mesures comprenant la conduite d'une évaluation d'impact sur la protection des données (AIPD) centrée sur les opérations de traitement 'à risques'.~~de gouvernance et de conception.~~ Mais de telsces cadres n'identifient ~~e précisent~~ pas toujours suffisamment ce que ~~sont~~ ces intérêts, droits et libertés sont dans la pratique et limitent les évaluations à ce qui est défini et spécifié dans la loi., ~~ni les circonstances dans lesquelles les risques peuvent se matérialiser et les préjudices se produire.~~

S'appuyant sur le concerpt de l'AIPD, c~~L~~es présentes lignes directrices adoptent un terme plus inclusif d'évaluation de l'impact sur les droits de l'homme (~~"~~EIDH~~"~~). D'emblée, les EIDH obligent ~~qui oblige d'emblée~~ à dépasser les questions de conformité basées sur la protection des données pour prendre en compte les droits autres que la vie privée sur lesquels les NIDS peuvent avoir un impact et pour lesquels il convient d'agir (dans les politiques, les technologies et les pratiques). Une EIDH est une approche davantage centrée sur l'être humain et qui met au centre les personnes et les communautés, ainsi que leurs besoins, préoccupations et perception des risques.

Une EIDH tient compte de la nécessité de prendre en considération les valeurs morales et sociales[63] des droits fondamentaux de l'homme énoncés dans les instruments ~~droit~~ internationaux~~l~~ des droits de l'homme, comme la Convention européenne des droits de

[61] 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/en/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

[62] Esteves et al (2017) Adapter l'évaluation de l'impact social pour traiter les impacts et les risques d'un projet en matière de droits de l'homme. https://www.sciencedirect.com/science/article/abs/pii/S0195925517300070

[63] Mantelero, A (2018) *IA et Big Data : Un plan pour une évaluation de l'impact sur les droits de l'homme, le social et l'éthique* https://www.sciencedirect.com/science/article/pii/S0267364918302012

l'homme (CEDH)[64], la Déclaration universelle des droits de l'homme,[65] la Charte des droits fondamentaux de l'Union européenne[66] ou les constitutions des pays. Plus largement, une EIDH exige une participation inclusive des titulaires de droits concernés et l'examen de l'impact des politiques et des lois qui visent à imposer des systèmes nationaux d'identité numérique sur leurs intérêts, leurs droits et leurs libertés.

Une approche d'EIDH oblige les décideurs et les responsables du traitement à ~~réfléchir au-delà des règles de "protection des données" et à~~ se demander si un programme ne risque pas d'exclure des catégories de personnes ou d'entraîner une discrimination, par exemple. Une EIDH au seul niveau politique peut aider à évaluer la proportionnalité d'une proposition. Il s'agit par exemple, de déterminer si l'avantage perçu est compensé par la gravité du préjudice subi par les personnes et, par conséquent, par la légitimité du traitement.[67] Or, une AIPD n'exige ni ne facilite une telle approche. Comme l'affirme Mantelero, "*une évaluation centrée sur les droits de l'homme ... offre une meilleure réponse à la demande d'une évaluation plus complète, incluant non seulement la protection des données ... mais aussi les effets de l'utilisation des données sur d'autres libertés et droits fondamentaux*." [68]

~~Une EIDH contribue à renforcer la transparence, la légitimité et la responsabilisation. Une EIDH va au-delà d'une évaluation qui cherche une conformité à la loi et place les individus et les groupes, ainsi que leurs besoins, leurs préoccupations et les risques qu'ils perçoivent au centre de l'évaluation. Une EIDH exige la transparence sur la manière dont la NID sera utilisée au sens large, sur les systèmes avec lesquels elle devra interagir et sur ses objectifs et son raisonnement, ainsi que la prise en compte des éventuels impacts négatifs sur les droits de l'homme et leur minimisation.~~

Mais une EIDH ne doit pas être un exercice de type "case à cocher". Comme l'affirme Götzmann, une EIDH doit aller "*au-delà d'une simple consultation ou d'un ajout technique à la conception d'un projet [et] au lieu que la consultation des parties prenantes ne soit qu'une des étapes de l'évaluation d'impact, [une] EIDH doit prévoir la participation inclusive des détenteurs de droits à des points critiques tout au long du processus d'évaluation*".[69]

Il n'y a pas une seule et bonne façon de mener une EIDH, mais les ressources indiquées dans ce document peuvent aider les décideurs, les régulateurs, les responsables du traitement et les fournisseurs de technologies d'identité à en comprendre les principaux éléments. [70] Les

[64] https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=
[65] https://www.un.org/sites/un2.un.org/files/udhr.pdf
[66] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT
[67] 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
[68] Voir note de bas de page 58
[69] Götzmann, N (2016), *Évaluation de l'impact des activités des entreprises sur les droits de l'homme : Critères clés pour l'établissement d'une pratique significative* https://www.cambridge.org/core/journals/business-and-human-rights-journal/article/human-rights-impact-assessment-of-business-activities-key-criteria-for-establishing-a-meaningful-practice/D964B80AC12F33C0FBEE4EF6A2F323C4.
[70] 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 (page 38) https://www.humanrights.dk/sites/humanrights.dk/files/media/document/A%20HRIA%20of%20Digital%20Activities%20-%20Introduction_ENG_accessible.pdf. Voir également (2020) Le secteur de la technologie et les plans d'action nationaux sur les entreprises et les droits de l'homme https://www.humanrights.dk/sites/humanrights.dk/files/media/document/The%20Tech%20Sector%20and%20National%20Action%20Plans%20on%20Business%20and%20Human%20Rights_2020_accessible.pdf 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, https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf.

normes internationales sur la gestion de l'identité - bien qu'elles ne traitent pas explicitement des droits de l'homme - 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.[71]

3.9 Responsabilité

L'une des principales exigences de la Convention 108+[72] et des lois modernisées sur la protection des données est que les "responsables du traitement" doivent être en mesure de démontrer que le traitement des données sous leur contrôle est conforme aux principes et obligations énoncés dans ces instruments.

Toutefois, une approche fondée sur les droits de l'homme étend le principe de responsabilité au-delà de l'obligation de démontrer aux régulateurs le respect des principes de protection des données, mais a pour but de garantir la responsabilité de manière transparente, tout au long des étapes clés des NIDS, de l'élaboration des politiques à l'engagement des parties prenantes, l'élaboration de la loi, la conduite des EIDH et la conception des droits de l'homme dans les NIDS.[73]

Les organisations concernées doivent :

- documenter et publier leur engagement en faveur d'une approche fondée sur les droits de l'homme ;
- documenter et publier un plan pour s'assurer que les impacts sur les droits de l'homme sont pris en compte à chaque étape des NIDS - depuis les politiques jusqu'à l'engagement des parties prenantes, la loi, les EIDH, la conception et le fonctionnement des NIDS ;
- documenter et publier 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 y sera donnée ;
- élaborer des politiques, des procédures et des pratiques qui démontrent la manière dont 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) ;
- élaborer et mettre en œuvre des programmes de sensibilisation et de formation aux droits de l'homme et à la protection des données et de la vie privée en particulier ;
- établir des procédures d'audit pour garantir non seulement le respect des obligations énoncées dans la législation sur la protection des données et les NIDS, mais aussi pour éviter et minimiser les effets négatifs sur les droits de l'homme ;
- veiller à ce que toutes les parties participant à la fourniture et à l'exploitation du NIDS respectent les principales exigences applicables, et en particulier les principes clés de la protection des données ;
- établir des politiques et des procédures pour respecter les droits des personnes et les publier ;

[71] 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
[72] Article 10
[73] Voir la note de bas de page 64

- publier un processus clair de plaintes individuelles ou de groupes et des mécanismes de recours ;
- veiller 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 soient une exigence du processus d'achat. Les organisations fournissant du matériel, des logiciels ou des services d'appui, par exemple, doivent être tenues d'attester de la manière dont elles aborderont les droits de l'homme, notamment en réalisant des EIDH à l'appui des contrats de soutien aux NIDS ;
- mettre 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 ;
- envisager des examens indépendants du point de vue de l'évaluation de l'impact sur les droits de l'homme.

3.10 Droit des personnes

L'article 9 de la Convention 108+ donne aux individus un certain nombre de droits en ce qui concerne le traitement de leurs données personnelles et de catégories spéciales de données. Ces droits doivent être établis par la loi et appliqués aux NIDS et à tout service interconnecté ou interdépendant qui demande une preuve d'identité légale ou NID, ou NIN, etc,

Les droits conférés par la Convention 108+ et par le droit international des droits de l'homme tel que la CEDH, *ne* peuvent être restreints[74] *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, et que cela doit toujours respecter l'essence des droits et libertés fondamentaux.

Les personnes doivent être informées de leurs droits et toute éventuelle restriction ainsi que des contextes dans lesquels ces restrictions peuvent s'appliquer. Les droits des personnes s'appliquent indépendamment de sa citoyenneté, de sa nationalité ou de son statut de résidence. Il est essentiel que les NIDS 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 période pendant laquelle les données seront conservées et des parties auxquelles leurs données seront communiquées ou auxquelles elles seront accessibles
    - Il est important que les personnes soient informées de manière claire et simple et culturellement appropriée et suffisamment pour garantir que le traitement est équitable pour elles ;
- le droit d'accéder à leurs données personnelles et d'obtenir une copie des données personnelles traitées, gratuitement et à des intervalles raisonnables le droit de faire corriger les données inexactes ;

[74] Article 11 de la convention 2018+.

- le droit d'obtenir l'effacement de leurs données (gratuitement) lorsque leur traitement est contraire aux dispositions de la loi sur la protection des données applicable/de 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 personnelles ;
- le droit de ne pas faire l'objet d'un profilage et/ou d'une prise de décision automatisée, sauf lorsque cela est clairement prévu par la législation nationale sur l'identité numérique ;
- le droit de déposer une plainte auprès d'une autorité de contrôle ;
- le droit à des recours judiciaires et non judiciaires (comme prévu par l'article 12 de la Convention 108+).

4. Recommandations pour les décideurs

Qu'ils soient membres de parlements, législateurs ou officiels gouvernementaux ou encore conseillers politiques, les décideurs politiques 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 d'identité nationale.

Les poliques et les décideurs devraient

- veiller à ce que les objectifs suivis par les NIDS soient bien définis, basés sur des preuves, proportionnés et nécessaires ;
- élaborer et rendre publique une politique nationale centrée sur les droits de l'homme afin d'aider le développement d'une loi spécifique réglementant un système d'identité nationale ;
- garantir que les politiques et l'élaboration de la loi soient fondées sur un engagement et une participation des parties prenantes qui aient une réelle possibilité de contribuer et de les examiner avant leur adoption ;
- publier les résultats de l'engagement de parties prenantes ;
- préciser dans la loi que le traitement de données personnelles et des catégories particulières de données notamment n'est permis que pour des finalités spécifiques et légitimes et avec une base juridique précise ;
- garantir l'exigence de mesures de protection appropriées dans les politiques et dans la loi, y compris celle de protection supplémentaires pour les catégories particulières de données ;
- exiger que les NIDS soient soumis à des évaluations et des obligations en matière de de solidité et de cybersécurité compte tenu de leur rôle potentiel dans des infrastructures critiques ;
- exiger des évaluations d'impact sur les droits de l'homme et un examen continu des impacts des NIDS sur les détenteurs des droits – cela depuis l'élaboration de politiques, de la loi et jusqu'au design, la mise en œuvre et le fonctionnement des NIDS
- exiger le développement d'une méthodologie et de lignes directrices en matière 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 sur l'identification nationale inclue le droit à connaître l'utilisation faite des données de cette identification, sous réserve des exceptions prévues par l'article 11 de la Convention 108+ ;
- garantir la mise en place de mécanismes de recours civils et judiciaires permettant aux les 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 réduction des dommages qui pourraient survenir du fait d'une corruption du NIDS comme le vol de données, des attaques entraînant le refus de service ou toute autre forme d'actes de cyber criminalité, l'appropriation de systèmes nationaux d'identité pour nuire intentionnellement à des personnes ou des catégories de personnes ;
- pénaliser l'utilisation malveillante de données collectées pour les NIDS, par exemple, la vente ou l'utilisation frauduleuse des données pour des bénéfices financiers.

5. Recommandations pour les responsables du traitement

Aux termes de l'article 2 de la Convention 108+, les responsables du traitement, qu'ils soient publics ou privés, devraient suivre les indications fournies par ce document. Toutefois, ces indications ne sauraient remplacer les lois applicables en matière de protection des données auxquelles ils doivent se conformer dans le traitement de données personnelles et celui de données particulières de données telle que les données biométriques. Ils doivent dument tenir compte des risques pour les droits et les libertés des personnes et être en mesure de démontrer que leur traitement de données est à la fois proportionné et nécessaire.

Les responsables du traitement devraient

- mettre en place un cadre de gestion approprié et fixer des responsabilités pour la protection des données, de la vie privée et des droits de l'homme ;
- considérer la nomination d'un délégué à la protection des données avec des compétences et des connaissances appropriées ;
- garantir que son personnel soit correctement formé en matière de protection des données et de 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 ;[75]
- 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 transparence, qualité des données et autres principes clés de la protection de données et que les personnes soient sensibilisés à leurs droits et puissent les exercer facilement ;
- développer et adopter une méthodologie d'évaluation d'impact sur les droits de l'homme et de droits de l'homme dès la conception (*human rights by design*) qui s'appuie sur l'évaluation d'impact sur la protection des données – et aille au-delà – pour veiller à ce que, par exemple, les personnes ne soient pas victimes d'exclusion ou de discrimination ;
- prévoir un point de contact qui permette aux personnes de soulever les problèmes ou poser les questions portant sur la collecte et l'utilisation de leurs données ;
- mettre en œuvre effectivement des mesures techniques et d'organisation pour une protection contre les risques pour les personnes ;
- le partage des données entre responsables de traitement ne peut être effectué que sicela est clairement établi par la loi et soumis aux normes appropriées de protection des données ;
- garantir que des contrôles d'accès appropriés sont maintenus pour retreindre l'accès aux systèmes d'identité nationale et aux enregistrements spécifiques pour autoriser les personnes et les dispositifs et conserver un registre des accès ;

[75] Le cours HELP du Conseil de l'Europe sur les droits à la protection des données et à la vie privée est une bonne introduction https://rm.coe.int/help-course-brief-data-protection-and-privacy-rights/16809cd3a7

- empêcher le profilage des personnes sauf s'il est expressément prévu par la loi.

- ~~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 transparence, qualité des données et autres principes clés de la protection de données et que les personnes soient sensibilisés à leurs droits et puissent les exercer facilement ;développer et adopter une méthodologie d'évaluation d'impact sur les droits de l'homme et de droits de l'homme dès la conception (*human rights by design*) qui s'appuie sur l'évaluation d'impact sur la protection des données – et aille au-delà –~~

~~4.~~6. Recommandations pour l'industrie de l'identité – les fabricants, les prestataires de services et les développeurs

Un mouvement et une industrie émergent qui font la promotion de 'l'identité juridique' comme étant un droit fondamental.[76] Les fabricants d'équipement, les prestataires de services et les développeurs de logiciels auxquels il est fait appel dans le cadre des systèmes d'identité nationale devraient veiller à atteindre les principes clé d la Convention 108+ pour respecter les droits humains et les libertés des personnes. Les entités de l'industrie de l'identité peuvent être concernés par le simple fait que les responsables du traitement et leurs sous-traitants, auxquels ils fournissent équipements et services, doivent se conformer à la législation applicable en matière de protection des données et ont l'obligation de concevoir le traitement des données de manière à prendre en compte et réduire, voire empêcher les risques sur les droits de l'homme et les libertés des personnes. Or, ces entités elles-mêmes traitent des données pour tester des matériels et des logiciels, par exemple.

Un des exemples de l'application de la Convention 108+ est l'article 5. Il exige que les systèmes d'identité nationale soient conçus de telle manière à garantie 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 qu'avec une base légale spécifiée – comme le consentement – et que les systèmes prévoient que les personnes 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 gardées à jour. Cela implique que les systèmpes d'identité nationale doivent être conçus pour permettre de modifier un nom – à la suite d'un acte notarié ou un mariage, par exemple, ou pour corriger une erreur sur un nom enregistré – ou encore pour changer les données biométriques d'une personne quand elles rendent inutilisables les modèles biométriques en cours ;
- corerctes, pertinentes et non excessives. Cela implique que les systèmpes d'identité nationale doivent être 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 telels que les données biométriques ou les données concernant les origines raciales ou ethniques d'une personne, données de plus en plus incluses dans les systèmes d'identité nationale. L'article 6 exige que des mesures de sécurité appropriées

[76] Thales 'Legal identity, a fundamental human right'. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/legal-identity

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*… »[77]

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

7. Recommandations à l'intention des autorités de ~~surveillance~~contrôle de la protection des données

L'article 15 paragraphe 3 de la Convention 108+ impose des obligations aux États pour garantir que les autorités de contrôle soient consultées sur toute proposition pour des mesures législatives ou administratives impliquant le traitement de données à caractère personnel. Les décideurs de politiques et les législateurs devraient donc veiller à ce que les autorités de contrôle soient consultées en tant que parties prenantes clés, et ce dès le début de la formulation des politiques nationales sur les NIDS puis tout au long des processus législatifs. Avec son droit d'être consultée sur des mesures telles que les NIDS, une autorité de contrôle a l'autorité pour émettre une opinion sur les opérations de traitement des données qui présentent des risques particuliers pour les droits et les libertés des personnes que les NIDS peuvent engendrer. Ainsi, une autorité de contrôle devrait considérer d'émettre de telles opinions lors des consultations réalisées en application de l'article 15 paragraphe 3, sur tout aspect des propositions d'introduire ou de modifier un NIDS.

L'article 15 impose aussi aux autorités de contrôle de rendre leurs activités publiques – cela devrait inclure son engagement et ses activités particulières en relation avec le NIDS et comprendre des rapports périodiques. Cela correspond au rôle crucial des autorités de contrôle d'avocat 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 les lois nationales applicables en matière de protection des données. En tant qu'autorités, elles ont une position et une expertise que n'ont pas les détenteurs de droits affectés et grâce auxquelles elles peuvent aider à garantir que les intérêts de ces personnes soient prises en compte dans les NIDS, depuis les politiques jusqu'à la pratique.

Les autorités de contrôle peuvent travailler avec des groupes de parties prenantes pour sensibiliser aux considérations primordiales de l'impact des NIDS sur les droits de l'homme et les libertés et les mesures appropriées pour réduire ces 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 envisager, à partir des approches de l'évaluation d'impact sur la protection des données et la vie privée, de créer une méthodologie d'évaluation d'impact sur les droits de l'homme. Une approche de l'EIDH dépasse l'esprit de la conformité aux normes de la protection des données pour intégrer l'engagement et la participation en considérant les intérêts des personnes et des groupes que les lois sur la protection des données et l'AIPD ne prennent pas en compte. De même, une EIDH permet d'identifier les

[77] Rapport explicatif de la Convention 108+, paragraph 89

problèmes, les besoins et les risques perçus des détenteurs des droits, ce que n'aborde pas une AIPD.

Les autorités de protection des données devraient considérer la mise en place de forums réguliers où toutes celles qui ont un rôle dans les NIDS pourraient se réunir pour veiller à un respect effectif des normes, aborder les risques et élaborer de bonnes pratiques.

~~5.~~8. Glossaire

Attribut : caractéristique ou propriété attribuée à une personne, comme son nom, son sexe, sa date de naissance, le nom de ses parents, ses données biométriques et même son numéro de téléphone portable.

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 de naissance ou le passeport d'une personne, par exemple.

Autorité de contrôle : une autorité établie pour assurer le respect des dispositions de la législation nationale sur la protection des données.

Catégories particulières de données : conformément à l'article 6 de la Convention 108+, il s'agit des données génétiques ; des données à caractère personnel relatives aux infractions, aux procédures pénales et aux condamnations, ainsi que des mesures de sécurité y afférentes ; des données biométriques permettant d'identifier une personne de manière unique ; 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.

Convention 108+ : le Protocole (ETCS n°223) amendant la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention CET 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 NIN, un numéro de téléphone mobile ou un identifiant de dispositif.

Données biométriques : caractéristiques physiologiques ou comportementales qui peuvent être utilisées pour identifier un individu de manière unique.

Droits de l'homme dès la conception : (anglais : 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 dans le traitement des données personnelles et des catégories particulières de données.

Evaluation d'impact sur les droits de l'homme – EIDH (anglais : HRIA) : un procéder par lequel les risques potentiels présentés par les NIDS pour les individus et les communautés en tant que détenteurs de droits sont évalués – depuis la proposition de politique et de loi, jusqu'à la mise en œuvre et l'application.

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

Identification - le processus d'établissement de l'identité d'une personne sur la base d'attributs vérifiables.

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

Identité : un attribut ou une combinaison d'attributs qui identifie de manière unique un individu.

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

Numéro d'identité national (NIN) : Un numéro unique attribué par un NIDS qui relie une personne à une identité légale et par lequel une personne peut être identifiée de manière unique par référence à la vérification des attributs liés à la saisie lors de la création d'un NID.

Profilage : désigne le traitement automatisé de données à caractère personnel ou de catégories particulières de données afin d'évaluer des aspects 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.~~

~~**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 d'identité fédéré : repose sur des données détenues par différentes autorités publiques et entités du secteur privé qui facilitent l'utilisation des attributs d'identité entre les systèmes sur la base de relations de confiance autorisées. Les données peuvent être utilisées pour prouver et authentifier l'identité d'une personne dans un contexte spécifique.

Système d'identité fondamental : un système polyvalent à l'échelle de la population qui vise à créer une identité légale officielle du gouvernement. Ces systèmes visent à garantir qu'un individu est identifiable de manière unique au sein d'une population nationale. Une identité fondatrice peut soutenir des identités fonctionnelles.

Un **système d'identité fonctionnel** sert un objectif spécifique et souvent sectoriel, comme la gestion des impôts individuels ou la fourniture de soins de santé nationaux, ou encore un permis de conduire, voire l'inscription sur les listes électorales.

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.

~~**Identification** : le processus d'établissement de l'identité d'une personne sur la base d'attributs vérifiables.~~

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

~~**Identité** : un attribut ou une combinaison d'attributs qui identifie de manière unique un individu.~~

~~**Identité numérique nationale (NID)** : Traitement des attributs d'un individu de manière à ce que celui-ci soit un individu **identifiable de manière unique** dans des contextes donnés.~~

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

~~**Numéro d'identité national (NIN)** : Un numéro unique attribué par un NIDS qui relie une personne à une identité légale et par lequel une personne peut être identifiée de manière unique par référence à la vérification des attributs liés à la saisie lors de la création d'un NID.~~

~~**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 NIN, un numéro de téléphone mobile ou un identifiant de dispositif.~~

~~**Profilage** : désigne le traitement automatisé de données à caractère personnel ou de catégories particulières de données afin d'évaluer des aspects 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.~~

~~**Catégories particulières de données :** conformément à l'article 6 de la Convention 108+, il s'agit des données génétiques ; des données à caractère personnel relatives aux infractions, aux procédures pénales et aux condamnations, ainsi que des mesures de sécurité y afférentes ; des données biométriques permettant d'identifier une personne de manière unique ; 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.~~

~~**Autorité de contrôle** : une autorité établie pour assurer le respect des dispositions de la législation nationale sur la protection des données.~~

Annexe A - Exemple d'approche 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,[78] produit 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.

TABLEAU A : Identification des parties prenantes					
Groupe de parties prenantes	**Types spécifiques de parties prenantes**	**Entité et caractéristiques générales** *Exemples fournis*	**Relation avec le sponsor de l'identité nationale/autres parties prenantes**	**Opinions / influence 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.			

[78] Voir https://www.humanrights.dk/sites/humanrights.dk/files/media/dokumenter/business/hria_toolbox/stakeholder_engagement/stakeholder_engagement_prac_sup_final_jan2016.pdf

TABLEAU A : Identification des parties prenantes					
Groupe de parties prenantes	**Types spécifiques de parties prenantes**	**Entité et caractéristiques générales** *Exemples fournis*	**Relation avec le sponsor de l'identité nationale/autres parties prenantes**	**Opinions / influence sur les NID**	**Type d'engagement, c'est-à-dire** *quand et comment (en personne, à distance).*
	Organisations de la société civile/ défenseurs des droits de l'homme	Les organisations non gouvernementales locales/internationales et les organisations communautaires telles que les conseils communautaires, les organisations de défense des droits de l'homme, les réseaux juridiques, etc. qui représentent les groupes affectés et qui peuvent également faciliter les rôles de recours/ombudsman.			
Les responsables	**Acteurs gouvernementaux**	Autorités nationales, agences ou départements gouvernementaux spécifiques, décideurs et régulateurs ayant une responsabilité directe au niveau politique, juridique, technique, de 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.			

TABLEAU A : Identification des parties prenantes					
Groupe de parties prenantes	**Types spécifiques de parties prenantes**	**Entité et caractéristiques générales** *Exemples fournis*	**Relation avec le sponsor de l'identité nationale/autres parties prenantes**	**Opinions / influence sur les NID**	**Type d'engagement, c'est-à-dire** *quand et comment (en personne, à distance).*
	Judiciaire/réparation	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 NIDS. Fournisseurs de NIDS en coentreprise. Les entreprises complémentaires qui peuvent 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 NIDS.			
	Marchés publics	Les autorités chargées des achats et qui devraient s'assurer que le matériel et les logiciels peuvent intégrer les droits de l'homme et les libertés fondamentales dans la conception et le fonctionnement des NIDS, de la qualité des données à la conservation et à l'effacement des			

TABLEAU A : Identification des parties prenantes					
Groupe de parties prenantes	**Types spécifiques de parties prenantes**	**Entité et caractéristiques générales** *Exemples fournis*	**Relation avec le sponsor de l'identité nationale/autres parties prenantes**	**Opinions / influence sur les NID**	**Type d'engagement, c'est-à-dire** *quand et comment (en personne, à distance).*
		données en passant par l'exercice des droits individuels. Le processus de passation de marchés devrait 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)	Organisme autonome ayant un mandat constitutionnel ou législatif pour promouvoir et protéger les droits de l'homme, comme les commissions des droits de l'homme ou le médiateur.			
	Experts et chercheurs	Des experts nationaux/juridiques en matière d'identité numérique, notamment des universitaires et des chercheurs spécialisés dans les droits de l'homme aux niveaux politique, juridique et technologique.			

TABLEAU A : Identification des parties prenantes					
Groupe de parties prenantes	**Types spécifiques de parties prenantes**	**Entité et caractéristiques générales** *Exemples fournis*	**Relation avec le sponsor de l'identité nationale/autres parties prenantes**	**Opinions / influence sur les NID**	**Type d'engagement, c'est-à-dire** *quand et comment (en personne, à distance).*
	Médias/journalistes	Les 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 de s'engager directement 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 NIDS est censé résoudre. • la base juridique sur laquelle les NID sont établies.	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 numérique nationale.

TABLEAU B : Exemples d'étapes à suivre avant de s'engager directement avec les parties prenantes		
Étapes	**Processus**	**Domaines nécessitant une attention et des considérations supplémentaires**
	• les liens entre le NIDS 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 NIDS 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 NIDS 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.	
2. Contacter les détenteurs 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.	• considérer le nombre d'individus à engager, leur position au sein des communautés et ce qui constituerait un échantillon représentatif des opinions. • quelle est 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

TABLEAU B : Exemples d'étapes à suivre avant de s'engager directement avec les parties prenantes		
Étapes	**Processus**	**Domaines nécessitant une attention et des considérations supplémentaires**
	• 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.)	manque d'équipement TIC et de connectivité peut empêcher la participation. • Y a-t-il d'autres obstacles à l'engagement ? La langue ? Culturels ? Polémique ? La peur ? • Réfléchissez 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	• Envisagez 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 les groupes de femmes uniquement ? • Tenez compte des paramètres et des horaires culturellement appropriés. • Réfléchissez 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. • Le lieu dispose-t-il d'installations appropriées et est-il un endroit où les parties prenantes se sentiront à l'aise ? • Examinez s'il est nécessaire de collecter des données à caractère personnel et, dans l'affirmative, obtenez le consentement des intéressés et expliquez-leur comment ils peuvent changer d'avis et quels sont leurs droits en matière de données.	• Ne prenez pas de photos sans le consentement explicite des personnes concernées et informez-les au préalable si les photos seront publiées (presse écrite ou en ligne, sites web, médias sociaux). • Examinez 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 de s'engager directement avec les parties prenantes		
Étapes	**Processus**	**Domaines nécessitant une attention et des considérations supplémentaires**
4. Évaluer le contexte de sécurité	• **Effectuez 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. • Demandez-vous si la visite du lieu de rencontre proposé est considérée comme sûre par des groupes spécifiques ? • S'assurer que les réponses des participants sont sécurisées de manière appropriée - qu'elles soient informatisées ou sur papier. • **Ne prenez pas de photos sans le consentement explicite des** personnes concernées et informez-les 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 s'exprimer : • le processus des parties prenantes et son objectif • le problème qu'un NIDS est censé résoudre. • le souhait de comprendre et de réfléchir dûment aux points de vue, intérêts, besoins et préoccupations des participants • expliquer comment les données collectées seront utilisées - être transparent • expliquer les droits relatifs à l'utilisation des données personnelles Évitez 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.) Soyez respectueux et sensible aux participants. Soyez attentif aux personnes qui peuvent être marginalisées/vulnérables. Soyez attentif aux relations de pouvoir et efforcez-vous d'inclure avec tact ceux qui peuvent sembler réticents à participer, mais n'exercez pas de pression sur ces individus ou groupes.	**Renforcer les capacités des titulaires de droits** en expliquant la relation entre l'identité numérique nationale, la protection des données et les droits de l'homme et les garanties pour les droits et libertés. Expliquez 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. Faites une brève présentation sur la protection des données, les NID et les droits de l'homme.
2. Assurer une participation volontaire	• Veillez 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.	

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**
	• 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. • Validez votre compréhension de la discussion avec les personnes interrogées à la fin d'un entretien. Permettez aux personnes de poser des questions.	
3. Respecter la vie privée des participants	• **Ne recueillez pas 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. • Examinez 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).	Réfléchissez, pendant la phase de planification des parties prenantes, à la manière dont vous répondrez/assisterez les individus ou les groupes si vous avez connaissance de graves **violations des droits de l'homme** pendant les consultations.
4. Assurer la sécurité et la	• 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.	

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**
sûreté - ne pas nuire	• Soyez prêt à interrompre l'événement si un groupe ou un individu ne se sent pas en sécurité.	
5. Soyez respectueux - communiquez d'une manière culturellement appropriée.	• Facilitez les discussions, ne les dominez pas. • 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. • Soyez attentif aux relations de pouvoir et à l'inclusion. Efforcez-vous d'inclure ceux qui sont moins désireux de s'exprimer dans les entretiens. • Envisagez 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 et de partager les résultats et les prochaines étapes, et communiquer un plan à cet effet.