Cadre de sauvegardes universelles liées aux infrastructures publiques numériques

Guide sur la création d'infrastructures publiques numériques sûres et inclusives pour les sociétés

DIGITAL PUBLIC INFRASTRUCTURE
Universal Safeguards

Nations Unies
Bureau de l'Envoyé du Secrétaire général pour les technologies

UNDP

DIGITAL PUBLIC INFRASTRUCTURE
Universal Safeguards

Cadre de sauvegardes universelles liées aux infrastructures publiques numériques

Guide sur la création d'infrastructures publiques numériques sûres et inclusives pour les sociétés

September 2024

Table des matières

À propos de ce guide

Le présent guide porte sur les modalités d'application du Cadre de sauvegardes universelles liées aux infrastructures publiques numériques, un ensemble de lignes directrices pratiques relatives à la conception et à la mise en œuvre d'infrastructures publiques numériques qui concourt à la poursuite de l'intérêt général. Le Cadre (version 1.0) est un bien public ouvert placé sous licence Creative Commons "Attribution-Partage dans les mêmes conditions 4.0 International" (CCBy-SA 4.0) . Il comporte des principes, des processus et des recommandations pratiques que les diverses autorités compétentes sont invitées à utiliser au sein de l'écosystème des infrastructures publiques numériques afin d'atténuer les risques pour la sécurité et l'inclusion. Les risques, définis au regard de chaque phase du cycle de vie des infrastructures publiques numériques, peuvent être palliés en appliquant les principes fondamentaux et opérationnels connexes. Ces principes ont été présentés dans un rapport d'étape, Leveraging DPI for Safe and Inclusive Societies (Tirer parti des infrastructures publiques numériques au profit de sociétés sûres et inclusives), publié en avril 2024.

Le Pacte pour l'avenir et son annexe, le Pacte numérique mondial, ont été adoptés le 22 septembre 2024 au Sommet de l'avenir. Dans le Pacte numérique mondial, les États Membres prennent acte du potentiel des infrastructures publiques numériques s'agissant de promouvoir une transformation numérique inclusive et de réaliser les objectifs de développement durable. Les États Membres conviennent donc qu'il importe de prévoir des sauvegardes adaptables, en ce qui concerne les infrastructures publiques numériques, si l'on veut atteindre ces objectifs.

Le Cadre de sauvegardes universelles liées aux infrastructures publiques numériques (Guide sur la création d'infrastructures publiques numériques sûres et inclusives pour les sociétés) met en lumière le rôle des infrastructures publiques numériques et des sauvegardes connexes dans le processus du Pacte numérique mondial. Fruit d'une initiative multipartite, il vise à atténuer les risques que courent les personnes et la société du fait de la mise en œuvre d'infrastructures publiques numériques, à faire progresser les objectifs de développement durable et à instaurer la confiance et l'équité dans tous les pays.

La finalité du présent guide pratique est de permettre aux lecteurs et aux praticiens de bien saisir comment le Cadre peut être appliqué de sorte qu'il garantisse une adoption sûre et inclusive des infrastructures publiques numériques. Les indicateurs clés de performance qui sont proposés à l'annexe 4 peuvent être étayés et utilisés par les autorités compétentes pour évaluer, analyser, comparer et examiner les infrastructures publiques numériques et suivre ainsi les progrès accomplis.

Résumé

Le Cadre de sauvegardes universelles liées aux infrastructures publiques numériques a été créé par DPI Safeguard, une initiative multipartite mondiale imaginée et soutenue par le Bureau de l'Envoyé spécial du Secrétaire général pour les technologies et le Programme des Nations Unies pour le développement (PNUD). Cette initiative a mobilisé 44 spécialistes des infrastructures publiques numériques issus des secteurs public et privé, de la société civile, des organismes de développement et du monde universitaire, 13 organisations membres du Groupe consultatif d'organisations internationales et 12 pays, ainsi que le public, à travers 13 réunions, et a fait l'objet de remontées provenant de plus de 100 contributeurs.

Le Cadre prend en compte plusieurs « autorités compétentes » dans l'écosystème des infrastructures publiques numériques. Il peut être adapté à différents contextes et s'applique à l'ensemble du cycle de vie des infrastructures publiques numériques. Le fait que la notion d'infrastructures publiques numériques englobe des systèmes et des services technologiques qui se situent au point de convergence entre les personnes, d'une part, et les entités civiques, publiques et privées qui détiennent le pouvoir social, politique et économique, de l'autre, est acté.

Les risques liés aux infrastructures publiques numériques ne découlent donc pas uniquement de lacunes techniques, mais aussi de l'inadéquation des cadres normatifs (déontologiques, juridiques et réglementaires), ainsi que de l'inefficacité institutionnelle et organisationnelle. Ces risques varient considérablement d'un système (de paiement, de vérification de l'identité, d'échange de données) et d'un pays à l'autre ; ils ne sont pas répartis uniformément dans la société et ne sont pas nécessairement statiques. Les préjudices éventuels peuvent être complexes et ressentis de différentes manières.

Le Cadre est ancré dans les instruments internationaux relatifs aux droits humains et les objectifs de la communauté mondiale, plus précisément les objectifs de développement durable et le Plan d'action de coopération numérique. Il est assorti de processus et de recommandations pratiques, l'objectif étant qu'il permette de pallier un large éventail de risques pour les personnes. Ces risques sont les suivants :

- Les risques pour la sécurité, qui découlent de la vulnérabilité en matière de confidentialité, de l'insécurité numérique, de l'insécurité physique et de l'inadéquation des recours.
- Les risques pour l'inclusion, qui découlent de la discrimination, de l'inégalité d'accès, de la perte de pouvoir d'agir et d'autres formes d'exclusion.

Le Cadre contient également des recommandations visant à remédier aux vulnérabilités structurelles, telles que la défiance à l'égard du numérique, la fragilité de l'état de droit, la faiblesse des institutions, les lacunes techniques et la non-durabilité. L'accent est mis sur l'importance des mécanismes de gouvernance robustes, sur le renforcement des capacités et sur la mise au point de mesures normalisées permettant de se faire une idée de l'incidence des infrastructures publiques numériques dans différents contextes.

Le Cadre est articulé autour de cinq éléments :

1. Risques à atténuer :

Le risque est la possibilité qu'un préjudice soit causé aux personnes qui interagissent avec les infrastructures publiques numériques. À l'heure actuelle, 13 risques interdépendants sont recensés.

2. Principes :

Les principes, actuellement au nombre de 18, sont des propositions fondamentales d'atténuation des risques qui ont été élaborées sur la base des risques possibles observés dans l'écosystème des infrastructures publiques numériques, qu'il s'agisse de risques nouveaux ou de vulnérabilités structurelles existantes.

3. Autorités compétentes :

Les autorités compétentes forment un groupe fonctionnel de parties prenantes qui se sont vu assigner ou qui assument des rôles, des responsabilités et une obligation de rendre compte quant à l'application et l'évolution des sauvegardes liées aux infrastructures publiques numériques.

4. Phases du cycle de vie :

Les phases du cycle de vie des infrastructures publiques numériques sont au nombre de cinq : genèse et étude préliminaire ; stratégie et conception ; mise au point ; déploiement ; exploitation et maintenance.

5. Recommandations :

Les recommandations regroupent quelque 300 processus et pratiques à suivre.
Le Cadre permet de réaliser de nombreuses permutations entre risques, principes, autorités compétentes, phases du cycle de vie et recommandations. Il est conçu comme une base de connaissances ouverte, permettant à tout utilisateur et toute utilisatrice de l'interroger pour déterminer quelles mesures prendre.

Le présent guide s'adresse donc aux parties prenantes qui jouent le rôle de facilitatrices (allant de l'étude théorique et de la mise en œuvre à l'évaluation et la dotation en ressources) dans les écosystèmes d'infrastructures publiques numériques. On y trouvera des explications sur la manière dont le Cadre peut être utilisé par toute autorité compétente à des fins de promotion de la sécurité et de l'inclusion dans les infrastructures publiques numériques et par l'entremise de ces dernières. À cet effet, le guide contient des démonstrations pas-à-pas calquées sur les différentes dimensions du Cadre : 1) risques ; 2) principes ; 3) autorités compétentes ; 4) phases du cycle de vie.

Le guide renvoie également les lecteurs vers une bibliothèque de connaissances interactive qui peut être interrogée en combinant les quatre dimensions correspondant à la situation et aux besoins des utilisateurs.

Le Cadre, qui est un bien public évolutif et ouvert, sera mis à jour en temps réel grâce aux contributions des parties prenantes et aux enseignements tirés de la mise en œuvre et de la formation au niveau des pays. La nature unificatrice et évolutive du Cadre donne à toutes les parties prenantes l'assurance que ces fondements vitaux de l'économie numérique ne laissent personne de côté et jouent un rôle essentiel dans la prestation de services publics à l'échelle de toute la société, une fonction cardinale des infrastructures publiques numériques.

Pour toute question ou pour aller plus loin, veuillez envoyer un courrier électronique à l'adresse suivante : dpi-safeguards@un.org.

1 Introduction

1.1 Les infrastructures publiques numériques replacées dans leur contexte

La notion d'infrastructure publique numérique étant modulable et évolutive, il a été décidé d'opter, dans le Cadre de sauvegardes universelles liées aux infrastructures publiques numériques, pour une description générale définissant les infrastructures publiques numériques comme un ensemble de systèmes numériques communs qui doivent être sûrs et interopérables, qui peuvent s'appuyer sur des normes et spécifications ouvertes pour fournir et assurer un accès équitable aux services publics ou privés à l'échelle de la société et qui sont régis par les cadres juridiques et les règles de base applicables, l'objectif étant de favoriser le développement, l'inclusion, l'innovation, la confiance et la concurrence ainsi que le respect des droits humains et des libertés fondamentales.[1]

Étant donné qu'il existe plusieurs modèles d'infrastructures publiques numériques et que chaque pays ou société développera et utilisera des systèmes numériques collectifs en fonction de ses priorités et de ses besoins propres, la description générale donnée ci-dessus se fonde sur la conception qu'ont de nombreuses organisations aux quatre coins du monde de ce qu'est une infrastructure publique numérique. On citera, entre autres, le G20, le Centre for Digital Public Infrastructure, Co-Develop, la Digital Impact Alliance, la Digital Public Goods Alliance, GovStack, l'Organisation de coopération et de développement économiques et la Banque mondiale.

Compte tenu de la diversité des approches et de la variété des modalités de mises en œuvre des infrastructures publiques numériques à l'heure actuelle, il est essentiel de mettre au point une approche unifiée des sauvegardes qui soit assortie de lignes directrices universelles tout en veillant à ce que l'utilité et l'utilisabilité soient adaptées au contexte.

1.2 L'initiative DPI Safeguards

L'initiative DPI Safeguards a été lancée en septembre 2023 par le Bureau de l'Envoyé spécial du Secrétaire général pour les technologies et le Programme des Nations Unies pour le développement. Elle se focalise sur les systèmes qui sont mis à la disposition de l'ensemble de la société par les pouvoirs publics ou en leur nom, voire par l'entremise de partenariats public-privé, au service d'une mission d'intérêt public. La création de cette initiative fait suite à la note d'orientation du Secrétaire général de l'Organisation des Nations Unies sur le Pacte numérique mondial et à l'appel du Secrétaire à la création de cadres communs pour les infrastructures publiques numériques. L'initiative reconnaît le potentiel de transformation des infrastructures publiques numériques tout en mesurant les risques que fait peser toute transformation numérique à l'échelle de la société.

[1] Description adoptée par le G20 (2023)

L'initiative DPI Safeguard est le fruit d'un effort multilatéral évolutif qui se fonde sur trois grands piliers :

1. **Cadre de sauvegardes universelles liées aux infrastructures publiques numériques:**
   Le Cadre regroupe une série de principes directeurs et de pratiques visant à faire en sorte que les infrastructures publiques numériques soient sûres et inclusives et couvre l'ensemble du cycle de vie des infrastructures, de la conception à la maintenance, en passant par le suivi et les remontées d'information. Il peut être consulté grâce à la bibliothèque de connaissances interactive. Dans cette dernière, les utilisateurs peuvent générer des scénarios adaptés au contexte qui est le leur et télécharger les recommandations applicables.

2. **Centre de ressources sur les sauvegardes liées aux infrastructures publiques numériques:**
   Le Centre de ressources est une plateforme en ligne dynamique, tournée vers les parties prenantes, où trouver des ressources en rapport avec les sauvegardes, des guides de mise en œuvre et des idées nouvelles sur les sauvegardes liées aux infrastructures publiques numériques.

3. **Mise en œuvre dans les pays:**
   Renvoie à la mobilisation active des parties prenantes dans les pays, dans le cadre de l'initiative et au sein de l'écosystème, en vue de créer ou de renforcer des environnements multipartites offrant des espaces d'échange de vues, des perspectives de contribution et de collaboration et des clefs permettant de remédier aux difficultés. Cette mise en œuvre passe par la facilitation d'une assistance technique, la tenue de réunions et le développement des capacités pour les pays, les secteurs et les acteurs, l'objectif étant de susciter le dialogue, de dégager un consensus et de créer des possibilités de promotion de la sécurité et de l'inclusion.

Ensemble, les piliers ci-dessus soutiennent la mise en œuvre des infrastructures publiques numériques d'une manière qui est non seulement sûre, sécurisée et inclusive, mais aussi pratique et adaptable à divers contextes et différents besoins.

Fondements de l'initiative

L'initiative DPI Safeguard est ancrée dans les instruments internationaux relatifs aux droits humains. Parmi ces instruments, citons la Déclaration universelle des droits de l'homme, qui sert de socle au droit international des droits humains, y compris aux traités juridiquement contraignants. Ces traités, en particulier le Pacte international relatif aux droits civils et politiques et le Pacte international relatif aux droits économiques, sociaux et culturels, permettent, ensemble, de protéger un large éventail de droits humains, et notamment, sans s'y limiter, les libertés civiles et politiques, les droits économiques, sociaux et culturels et le droit à la non-discrimination, ainsi que les droits des enfants, des femmes, des personnes en situation de handicap et d'autres groupes vulnérables.

L'initiative DPI Safeguards est également guidée par les objectifs de développement durable et le Plan d'action pour la coopération numérique, qui sont tous deux en phase avec la Déclaration universelle des droits de l'homme.

Méthode

L'initiative DPI Safeguard complète, unifie et prolonge les travaux qui ont déjà été menés sur la question, y compris, sans s'y limiter, les nombreux efforts déployés pour concevoir, mettre en œuvre et alimenter les infrastructures publiques numériques. On trouvera en annexe 1 une liste non exhaustive de ces ressources. Le Cadre, qui a vocation à être universellement applicable à toutes les infrastructures publiques numériques et à répondre à tous les besoins des parties prenantes, continuera d'être développé au fil de cycles continus de remontée de l'information fondés sur les contributions multipartites.

Six groupes de travail, composés de spécialistes et de praticiens des infrastructures publiques numériques relevant d'un large éventail de parties prenantes de l'écosystème numérique mondial (annexe 2), ont piloté la création du Cadre. Le présent guide a également bénéficié des vues, des remontées et des recommandations formulées par un groupe consultatif d'organisations internationales (annexe 3), ainsi que du fruit de réunions, de mobilisations dans les pays et de consultations publiques. Le Cadre se fonde sur un rapport d'étape publié pour recueillir les suggestions du public en avril 2024. Le Cadre affine les risques et les principes qui ont été mis en évidence et fournit des indications supplémentaires sur des lignes directrices pratiques adaptables à toutes les infrastructures publiques numériques.

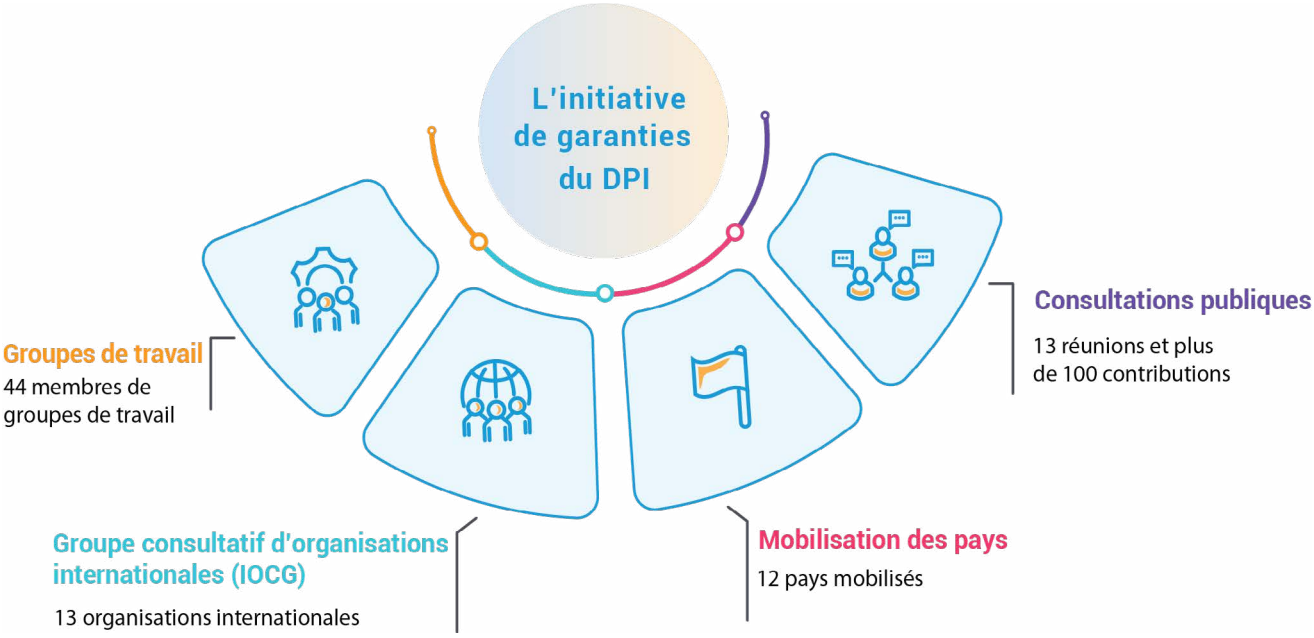

Figure 1.1 | Le cadre a été élaboré à travers des discussions dirigées par des experts et de vastes consultations avec des praticiens

2 Sécurité et inclusion pour tous

2.1 Pourquoi ? Atténuer les principaux risques

L'incidence des risques associés à des infrastructures publiques numériques qui sont mal conçues, mal mises en œuvre ou mal gérées est considérable. Les infrastructures publiques numériques sont souvent utilisées par les pouvoirs publics pour fournir directement ou en leur nom des services à l'ensemble de la société. L'initiative DPI Safeguard remédie aux risques liés aux infrastructures publiques numériques qui pourraient se présenter et qui iraient à l'encontre des instruments internationaux relatifs aux droits humains, des objectifs de développement durable et du Plan d'action de coopération numérique. Parmi ces risques susceptibles de compromettre la sécurité et de faire obstacle à l'inclusion figurent les vulnérabilités structurelles qui limitent l'efficacité des sauvegardes.

Risques pour la sécurité

Dans les infrastructures publiques numériques, on parle de risques pour la sécurité lorsque les données personnelles, les systèmes numériques et la personne physique ou les biens peuvent faire l'objet d'accès non autorisés, de cyberattaques et de menaces dans le monde réel. Les personnes et les groupes s'en trouvent exposés et vulnérables. Il n'est pas possible d'atténuer ces risques en l'absence de voies de recours et de mécanismes de réparation ou lorsque ces voies et mécanismes sont inadéquats.

L'initiative DPI Safeguards remédie aux risques pour la sécurité suivants :

On parle de **vulnérabilité en matière de vie privée** lorsque des informations personnelles sont traitées (transmises, stockées ou utilisées) sans consentement ou au mépris des attentes raisonnables en matière de protection de la vie privée, ou utilisées à mauvais escient afin de causer un préjudice. Ces violations peuvent entraîner des dommages physiques, financiers, psychologiques et émotionnels ainsi qu'une atteinte à la réputation. Les risques les plus importants sont l'usurpation d'identité et la fraude, en particulier dans le cas des services financiers, tels que les paiements et le crédit, où les pertes financières pour les victimes peuvent être lourdes. Les failles en matière de vie privée peuvent permettre aux pouvoirs publics d'accéder illégalement aux données et de les utiliser à mauvais escient dans des activités de surveillance non autorisée qui porteraient atteinte aux droits humains.

L'**insécurité numérique** se situe un cran au-dessus des vulnérabilités en matière de vie privée et englobe les interruptions de service, les perturbations à l'échelle de secteurs d'activité entiers et d'autres formes d'instabilité systémique. Les systèmes mal sécurisés peuvent être exploités à des fins malveillantes, notamment pour saboter des infrastructures critiques, pour se livrer à de la surveillance illégale, pour supprimer la liberté d'expression et le droit de se réunir, pour espionner et pour déstabiliser des pays. Les répercussions de l'insécurité numérique sont considérables, entraînant des pertes financières, des dangers physiques et des atteintes à la réputation, entre autres.

L'**insécurité physique** découle souvent de l'insécurité numérique. Par exemple, la compromission de dossiers médicaux dans un système d'échange de données peut entraîner un préjudice physique. La surveillance intrusive peut exposer les allées et venues et le lieu de résidence de personnes qui peuvent ensuite être traquées, harcelées ou soumises à la coercition. La sécurité des demandeurs d'asile, notamment, est menacée lorsque leur identité et leurs mouvements sont traçables, ce qui peut entraîner des persécutions, des discriminations ou un refus de protection. Les infrastructures publiques numériques qui sont mal sécurisées peuvent également priver les apatrides de protections juridiques ou d'accès à des services essentiels. Elles peuvent être exploitées pour menacer la sécurité des personnes qui expriment des opinions dissidentes ou participent à des manifestations en exerçant des représailles sur ces personnes, en les persécutant ou en se livrant à d'autres formes d'atteinte à l'intégrité physique.

Le **manque de recours** renvoie à l'absence de voies de recours et de mécanismes de réparation efficaces en cas de violation des droits ou à inadéquation de ces dispositifs, qui privent, dans un cas comme dans l'autre, les personnes exposées à des risques liés aux infrastructures publiques numériques de moyens d'atténuer les préjudices qui leur sont causés. Cette défaillance sape l'intégrité des infrastructures publiques numériques, érode la confiance du public et amoindrit les taux d'adoption. Résultat, la durabilité et l'efficacité des infrastructures publiques numériques s'en trouvent remises en cause, tandis que les avantages qui peuvent être ceux de ces infrastructures s'en trouvent sérieusement diminués.

Risques pour l'inclusion

Plusieurs risques associés aux infrastructures publiques numériques pourraient saper l'inclusion et l'accessibilité, décourager la mobilisation à grande échelle et réduire les avantages à leur plus simple expression. Si la discrimination et l'inégalité d'accès constituent d'importants obstacles, d'autres formes d'exclusion, comme la perte de pouvoir d'agir, contribuent également à la privation de droits.

L'initiative DPI Safeguards remédie aux risques pour l'inclusion suivants :

La **discrimination** sous toutes ses formes (raciale, socioéconomique, linguistique, géographique, culturelle ou liée au genre, au handicap ou à l'âge) entrave l'accès aux possibilités d'emploi, à l'autonomisation économique, aux services essentiels, tels que la santé et l'éducation, ainsi que la participation à la vie publique et économique. Il importe tout particulièrement d'éviter toute discrimination dans les systèmes d'identification numérique qui donnent accès aux services sociaux, aux services d'urgence ou aux services publics et sur lesquels repose l'économie au sens large. La discrimination est l'une des principales causes d'apatridie dans le monde, les personnes concernées étant souvent exclues des systèmes d'identification, entre autres. La dématérialisation des systèmes d'identification et de systèmes analogues peut perpétuer une privation des droits qui existe déjà.

L'**inégalité d'accès** aux infrastructures publiques numériques est imputable non seulement à la discrimination, mais aussi à la fracture numérique et à d'autres sources de défaillances des infrastructures (électricité, connexion à Internet, smartphones et ordinateurs), ainsi qu'à des barrières socioéconomiques (pauvreté, éducation générale, habileté numérique), ou encore à des lacunes en matière de services dans certaines zones géographiques, à des barrières linguistiques et au handicap. Les préjudices en matière de droits humains surviennent lorsque l'accès à l'information publique et aux services numériques n'est pas possible du fait de l'inégalité d'accès aux infrastructures publiques numériques et aux structures sociales et économiques sur lesquelles elles s'appuient.

L'**exclusion** se produit également lorsque la souscription aux systèmes d'infrastructures publiques numériques est onéreuse, impossible ou source de difficultés, en particulier lorsqu'elle est incontournable pour accéder à l'information ou aux services publics. Cette situation entraîne souvent un coût caché pour les personnes vulnérables qui peuvent avoir besoin de l'aide de tiers. Dans les pays en développement, où les ressources peuvent être limitées lorsqu'on a besoin d'aide, l'inexistence d'autres modes d'accès constitue un risque courant. Les tribunaux peuvent être amenés à intervenir pour protéger les droits des personnes exclues. L'exclusion peut également entraîner une concentration du pouvoir de marché qui fait grimper le coût des services, qui limite les choix et qui fait baisser la qualité de service.

La **perte de pouvoir d'agir** peut être causée par des systèmes d'infrastructures publiques numériques qui limitent le contrôle qu'ont les personnes sur leurs données personnelles, ce qui fait peser une menace sur l'autonomie et la capacité humaine d'agir. La menace est exacerbée lorsqu'une personne ignore la manière dont ses données peuvent être utilisées ou réutilisées, les répercussions qui en découlent et l'existence même, le cas échéant, de moyens lui permettant d'exercer un contrôle sur ses données. Le partage obligatoire de données peut également éroder la capacité humaine d'agir et, dans certains endroits, violer les droits humains et entraver les libertés civiles, ce qui peut s'avérer anticonstitutionnel.

Vulnérabilités structurelles

Les vulnérabilités structurelles systémiques sont nombreuses. Au premier rang de ces vulnérabilités figurent la méfiance à l'égard du numérique, la fragilité de l'état de droit, la faiblesse des institutions, les lacunes techniques et la non-durabilité.

L'initiative DPI Safeguards remédie aux vulnérabilités structurelles éventuelles suivantes :

La **méfiance à l'égard du numérique** peut découler de risques connus ou perçus pour la sécurité et l'inclusion. Cette méfiance nuit à l'adoption généralisée des infrastructures publiques numériques et à la mise au point et l'adoption d'innovations qui enrichissent ces mêmes infrastructures. Comme la discrimination, la méfiance à l'égard des infrastructures publiques numériques est souvent liée à des facteurs sociaux préexistants qui doivent être pris en compte et compris pour être corrigés comme il se doit. Quelle qu'en soit la raison, la méfiance à l'égard du numérique présente un risque réel pour la légitimité, l'efficacité, l'adoption et la pérennité des systèmes d'infrastructures publiques numériques et peut s'étendre à la méfiance vis-à-vis de tous les services numériques et des institutions publiques en général.

La **fragilité de l'état de droit** limite la possibilité d'atténuer efficacement les risques grâce aux cadres normatifs dans lesquels sont prescrites des exigences légales, réglementaires et déontologiques. Les infrastructures publiques numériques peuvent amplifier le pouvoir politique, social et économique de celles et ceux qui contrôlent ces systèmes, et la concentration de ce pouvoir fait courir un risque d'affaiblissement des institutions normalement garantes de l'état de droit ainsi qu'un risque de contournement des contre-pouvoirs essentiels, ce qui peut donner lieu à des abus. La concentration du pouvoir sous la forme de monopoles peut freiner l'innovation, limiter et appauvrir l'offre de services et abaisser la qualité de service. La soustraction au principe de responsabilité peut conduire à une utilisation malveillante, à des préjudices et à un contournement de la loi dans un anonymat relatif.

La **faiblesse des institutions** limite l'efficacité et la légitimité des sauvegardes si les institutions ne sont pas en mesure de mettre en œuvre les politiques et pratiques nécessaires. L'incapacité d'assumer les rôles clés du fait de l'insuffisance des capacités, des ressources et des mécanismes institutionnels fait peser un risque omniprésent pour les infrastructures publiques numériques, tout comme l'absence d'institutions compétentes dans la supervision de l'ensemble du cycle de vie des infrastructures. Le manque de moyens permettant aux principaux organismes et aux principales parties prenantes de l'écosystème de se coordonner ou de coopérer pour adopter une approche des infrastructures publiques numériques mobilisant l'ensemble de la société, ainsi que le manque de volonté en la matière, limite le poids et l'efficacité d'une telle approche.

Les **lacunes techniques** peuvent nuire à la protection des infrastructures publiques numériques. Une technologie qui n'est pas conçue pour garantir la sécurité, l'inclusion et la prévention des préjudices fait courir des risques. Parmi les points faibles, citons les risques de sécurité pour les infrastructures publiques elles-mêmes et pour les personnes, par exemple lorsqu'une configuration est inadaptée ou malvenue pour certains groupes ou certaines personnes (en raison du genre, de l'âge, de la situation de handicap, etc.), les choix technologiques laissant à désirer qui conduisent à la mise en place de solutions non normalisées, non interopérables ou excessivement coûteuses, la propriété restreinte, conditionnelle ou grevée des solutions complètes, ou encore l'inaptitude et l'incompétence en matière d'infrastructures publiques numériques. Entre autres préjudices, les lacunes techniques érodent la confiance dans les infrastructures publiques numériques.

La **non-durabilité** des infrastructures publiques numériques couvre un large spectre, allant de l'environnement aux partenariats (dépendance technologique des fournisseurs), en passant par le financement. Elle présente des risques importants pour celles et ceux qui ont investi dans les services fournis grâce à ces infrastructures et qui en dépendent, et elle limite l'adoption par ses utilisateurs potentiels et ceux d'autres infrastructures publiques numériques. Ces risques découlent de l'insuffisance de la valeur pour les utilisateurs, de lacunes dans la conception, du défaut de maintenance, du manque d'améliorations et de mises à jour et du déficit de ressources. Parmi les menaces d'ordre financier, citons les coûts d'exploitation et de maintenance élevés, l'obsolescence du matériel et des logiciels et la détérioration des composants. La dépendance technologique des fournisseurs limite la souplesse et l'adaptabilité aux nouvelles technologies, ce qui entraîne des coûts lourds et d'autres problèmes. En outre, le défaut de stratégie visant à réduire l'empreinte carbone des infrastructures publiques numériques et à gérer l'impact environnemental des déchets d'équipements électriques et électroniques qui sont produits par ces infrastructures pourrait fragiliser le rôle qui est le leur dans la réalisation des objectifs de durabilité environnementale et, par voie de conséquence, leur propre durabilité. Les conséquences de la non-durabilité des infrastructures publiques numériques sont considérables, car ces infrastructures ont d'importantes répercussions sociétales.

Figure 1.2 | Risques

2.2 Qui ? L'écosystème des infrastructures publiques numériques

L'écosystème des infrastructures publiques numériques regroupe des organisations du secteur public, des spécialistes de la planification, des parlementaires, des spécialistes de la réglementation et des tiers décideurs, des organisations industrielles, des prestataires du secteur privé (spécialisés dans les logiciels, la cybersécurité, les services en nuage, les données et la fourniture d'autres produits et services), des responsables de la maintenance des infrastructures, des organismes internationaux et nationaux de normalisation, des organisations internationales, des bailleurs de fonds, des organisations à but non lucratif, des groupes de pression, des représentants locaux, des particuliers et une variété d'autres acteurs.

Aucun groupe d'autorités compétentes ne peut à lui seul créer, assurer la maintenance ou faire fonctionner des infrastructures publiques numériques ; ces infrastructures ne peuvent être efficaces, sûres et inclusives que si l'écosystème est utilisé dans le cadre d'une approche mobilisant la société dans son ensemble.

Pour atténuer les risques, il est primordial que les bons acteurs pilotent, mettent en œuvre et supervisent toutes les étapes de la création d'une infrastructure publique numérique et qu'ils puissent s'appuyer sur les mécanismes institutionnels et les capacités nécessaires pour assumer les rôles qui leur incombent. Pour les besoins du Cadre, on s'est intéressé à un échantillon d'acteurs qui participent activement à la mise en place de services liés aux infrastructures publiques numériques. La figure 2.1 présente ces autorités compétentes classées en grandes catégories : pouvoirs publics ; spécialistes de la réglementation ; donateurs ; fournisseurs de technologie ; espace civique. Si ces autorités compétentes ne sont en aucun cas exhaustives et pourraient être classées autrement, elles constituent néanmoins un échantillon représentatif des principales parties prenantes des sauvegardes liées aux infrastructures publiques numériques.

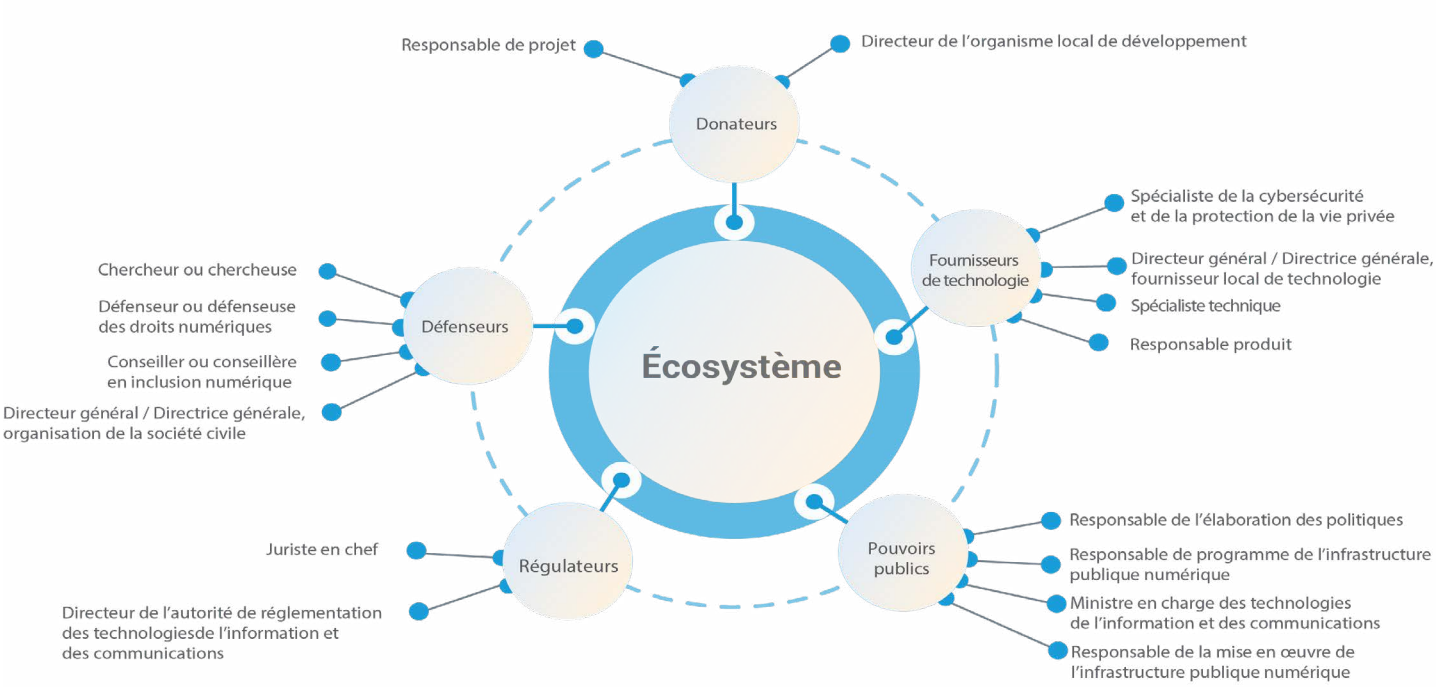

Figure 2.1 | Cartographie de l'écosystème des infrastructures publiques numériques

Le Table 2.1 illustre à grands traits les rôles associés aux infrastructures publiques numériques qui sont endossés par les diverses personas composant les autorités compétentes dans l'écosystème des infrastructures. Ces personas jouent un rôle actif, assurent des fonctions et assument des responsabilités dans les services liés aux infrastructures publiques numériques et la mise en œuvre effective du Cadre. Elles ont toutes des objectifs, des besoins, des motivations, des frustrations et des points de friction qui leur sont propres et qui déterminent en quoi et pourquoi le Cadre peut être important pour elles, mais aussi pourquoi et comment elles pourraient l'utiliser.

Table 2.1 | Rôles et cas d'utilisation possibles au sein du Cadre

Autorité compétente	Persona type (non exhaustif)	Fonctions et attributions types associées aux infrastructures numériques publiques	Utilisation possible du Cadre
Pouvoirs publics	Responsable de l'élaboration des politiques Directeur ou directrice de programme d'une infrastructure publique numérique Responsable de la mise en œuvre des infrastructures publiques numériques Ministre des technologies de l'information et des communications	• Gouvernance globale : de l'élaboration des politiques à la prestation de services publics. • Politiques visant à fixer les objectifs de développement et à guider la numérisation inclusive. • Appui budgétaire à des fins de développement et de création d'infrastructures publiques numériques. • Présentation d'éléments attestant de l'avancée des projets aux électeurs. • Écoute des remontées d'information et amélioration des procédures législatives, exécutives et judiciaires.	Adoption du Cadre pour : • Bâtir une société sûre et inclusive . • Se montrer proactif et répondre aux besoins de la population . • Créer des mécanismes d'atténuation des risques . • Faire un état des lieux et recenser les mesures à prendre. • Tracer une trajectoire sûre et inclusive vers les objectifs de développement durable.
Spécialistes de la réglementation	Juriste en chef Chef de l'autorité de réglementation des technologies de l'information et des communications	• Mise en place des bons garde-fous. • Supervision et application des lois et de la réglementation.	Promouvoir les sauvegardes liées aux infrastructures publiques numériques dans les domaines suivants : • Cadres et programmes liés aux services universels. • Obligation et application des concessions. • Politique en matière de concurrence . • Campagnes de relations publiques. • Codes de pratique volontaires.
Donateurs	Responsable de projet Responsable de l'organisme local de développement	• Fourniture d'un financement et d'un appui financier. • Recherche d'éléments attestant d'avancées dans la réalisation des objectifs de développement.	Ajouter les sauvegardes liées aux infrastructures publiques numériques aux critères de financement pour soutenir et mettre en avant l'engagement en faveur de progrès fondés sur les droits, sûrs et inclusifs, via les sauvegardes, afin d'obtenir certains résultats liés aux objectifs de développement durable

Autorité compétente	Persona type (non exhaustif)	Fonctions et attributions types associées aux infrastructures numériques publiques	Utilisation possible du Cadre
Fournisseurs de technologie	Spécialiste de la cybersécurité et de la protection de la vie privée PDG, fournisseur local de technologie Responsable produit Spécialiste technique	• Personne référente pour les activités techniques, le recensement des risques et les stratégies d'atténuation. • Influence allant du conseil à la mise en œuvre concrète, en passant par la maintenance des infrastructures publiques numériques et l'appui à ces infrastructures.	Adopter et intégrer dans la pratique les sauvegardes liées aux infrastructures publiques numériques pour : • Instaurer la confiance en tant que conseillers et conseillères des pouvoirs publics. • Assurer la réussite et l'adoption pérenne des infrastructures publiques numériques. • Mesurer les progrès accomplis et élaborer un plan d'action relatif à l'évolution à long terme des infrastructures publiques numériques. • Mettre en commun les meilleures pratiques en matière de sécurité et d'inclusion avec les parties prenantes. • Participer activement à la communauté des sauvegardes liées aux infrastructures publiques numériques et mettre à profit ses connaissances spécialisées.
Espace civique	Défenseur ou défenseuse des droits numériques Conseiller ou conseillère en inclusion numérique Responsable, organisation de la société civile Chercheur ou chercheuse	• Conduite des activités de sensibilisation aux sauvegardes liées aux infrastructures publiques numériques. • Défense des droits humains . • Représentation des intérêts des pans marginalisés et multiformes de la société. • Formulation d'idées novatrices visant à rendre les infrastructures publiques numériques plus inclusives. • Mise en lumière des incohérences vis-à-vis des lois ou réglementations existantes.	Utiliser le Cadre pour : • Évaluer la sûreté et l'inclusion des pratiques. • Mettre en commun les meilleures pratiques en matière de sécurité et d'inclusion avec les parties prenantes. • Recueillir les éclairages singuliers des populations locales et en faire part à la communauté des sauvegardes liées aux infrastructures publiques numériques.

2.3 Quand ? Le cycle de vie itératif des infrastructures publiques numériques

Les infrastructures publiques numériques résultent rarement d'un processus linéaire dans lequel le point de départ et le point final précis peuvent être clairement définis parmi d'autres scénarios. Elles peuvent résulter de l'évolution de systèmes numériques publics ou privés existants. Les infrastructures publiques numériques continuent d'évoluer par itérations progressives et peuvent apporter de nouvelles solutions au fil du temps. Le maintien de l'utilité et de la valeur sociétale des infrastructures publiques numériques passe par des ajustements itératifs.

Pour atténuer les risques décrits précédemment, il convient de mettre en place des sauvegardes à mesure que les infrastructures publiques numériques évoluent aux différentes phases du cycle de vie type de ces infrastructures, comme le montre la **figure 2.2**. Ces phases sont les suivantes :

- Genèse et étude préliminaire
- Stratégie et conception
- Mise au point
- Déploiement
- Exploitation et maintenance

Certaines activités, telles que l'apprentissage à partir de modèles d'infrastructures publiques numériques concluants et de bonnes pratiques, sont les mêmes à toutes les phases du cycle de vie. Divers facteurs contextuels, dont la maturité de la mise en œuvre, déterminent la trajectoire d'évolution d'une infrastructure publique numérique donnée. D'autres facteurs, tels que le type d'infrastructure publique numérique, le secteur et le service, déterminent les activités prioritaires à mener pour chaque phase du cycle de vie à différentes périodes de son évolution. Le cycle de vie type d'une infrastructure publique numérique offre un cadre utile pour le recensement, l'atténuation et la gestion des risques.

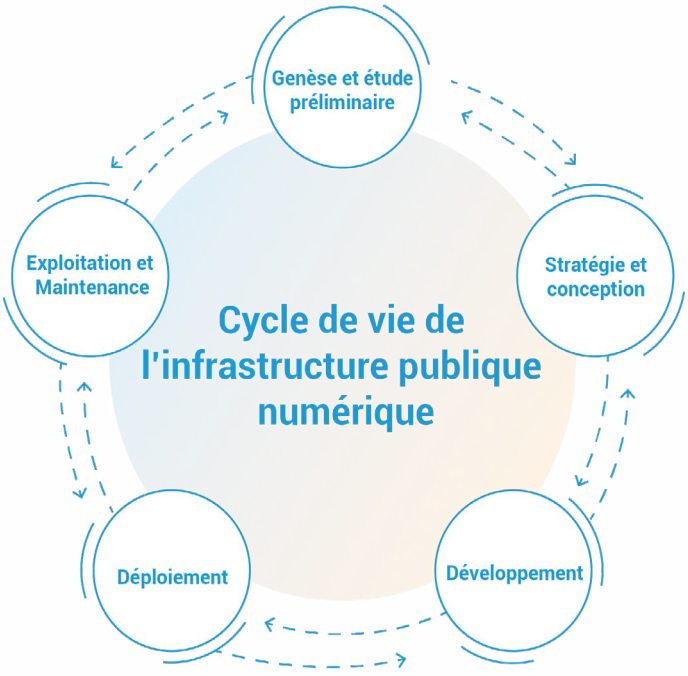

Figure 2.2 | Cycles itératifs de l'évolution des infrastructures publiques numériques

Genèse et étude préliminaire

Le phase de la genèse et de l'étude préliminaire du cycle de vie des infrastructures publiques numériques est crucial, car il permet de poser et d'étudier la raison d'être, les buts, les contraintes et les limites de l'infrastructure. Ces paramètres guident la prise de décision qui s'ensuit et permettent de s'aligner sur les objectifs stratégiques et opérationnels ainsi que sur les besoins des personnes. Les activités types sont les suivantes :

- Définition des buts et des objectifs.
- Recensement des grands problèmes et des principales difficultés.
- Évaluation des effets pouvant être attendus.
- Analyse de l'environnement porteur afin de repérer les entraves à la mise en œuvre, à l'efficacité et à l'adoption de l'infrastructure, en tenant compte des risques associés.
- Ancrage de l'état de droit et des capacités institutionnelles permettant d'assurer une mise en œuvre sûre et inclusive.

Stratégie et conception

C'est à ce phase qu'un plan global de conception et d'ajustement de l'infrastructure publique numérique est dressé, l'objectif étant de traduire les objectifs fonctionnels et les objectifs de performance en mesures pratiques, notamment en ce qui concerne l'extensibilité et la durabilité de l'infrastructure, mais aussi la planification visant à assurer une prestation de services optimale. Les activités types sont les suivantes :

- Cartographie et mobilisation des parties prenantes afin de comprendre les besoins des personnes et ceux de la société.
- Identification des parties prenantes parmi les autorités compétentes et les personas qui seront amenées à collaborer.
- Sensibilisation aux obstacles à la mise en œuvre de l'infrastructure dans l'environnement porteur et mobilisation pour qu'ils soient levés.
- Établissement de normes, de protocoles et de paramètres de mesure visant à évaluer l'adoption et l'incidence sociétale.
- Définition d'objectifs de conception et établissement d'un cahier des charges conformément aux meilleures pratiques et aux principes, en mettant l'accent sur les améliorations progressives et la résilience de l'architecture, et adoption de stratégies fondées sur des données factuelles afin d'atténuer les risques liés à la conception.

Mise au point

Au cours du phase de la mise au point, on crée un prototype d'infrastructure publique numérique conformément au cahier des charges fixé, en prêtant une attention particulière à la fonctionnalité, la fiabilité et l'extensibilité. Les composantes techniques existantes sont évaluées avant d'aller plus loin. Ce phase permet d'affiner les solutions et de les mettre à l'essai afin de réduire les risques au minimum et de maximiser l'efficacité des sauvegardes avant la mise en œuvre à grande échelle. L'atténuation des risques liés à la mise en œuvre est essentielle à ce phase et dépend de la maturité de la mise en œuvre de l'infrastructure publique numérique et du contexte local. Ce phase offre une occasion précieuse de confier des responsabilités aux promoteurs locaux. Les activités types sont les suivantes:

- Évaluation et sélection des composantes existantes, notamment les piles technologiques.
- Codage du logiciel en fonction du cahier des charges, s'il y a lieu.
- Création d'interfaces de programmation d'applications et d'espaces d'expérimentation ouverts.
- Analyse de l'environnement porteur afin de repérer les entraves à la mise en œuvre, à l'efficacité et à l'adoption de l'infrastructure, en tenant compte des risques associés.
- Exécution et itération par le truchement de projets pilotes, en mettant l'accent sur l'aspect pratique et l'atténuation des risques liés à la sécurité, à la confidentialité et à l'expérience.
- Comblement des lacunes des structures, politiques et réglementations institutionnelles.

Déploiement

Au phase du déploiement, l'infrastructure publique numérique est mise en œuvre dans son environnement opérationnel. Tous les changements institutionnels en suspens sont apportés afin de créer de la valeur pour les utilisateurs et de protéger la sécurité et l'inclusion. Des stratégies de gestion du changement sont recommandées. Ce phase est essentiel pour garantir l'adoption à grande échelle de l'infrastructure publique numérique. Les activités types sont les suivantes :

- Installation, configuration, activation et mise à l'échelle des composantes matériel, logiciel et réseau.
- Renforcement des capacités des autorités compétentes et des personas.
- Ajustements fondés sur des éléments factuels, les données importantes et les remontées d'information.
- Mise en place d'un dispositif de gouvernance robuste assorti de mesures de suivi et de voies de recours.
- Entrée en fonction prévue et progressive des personnes concernées afin de gérer de près la mise à l'échelle du système et les questions d'intégrité pendant la période d'adoption.

Exploitation et maintenance

La régularité de l'exploitation et de la maintenance permet d'assurer une performance, une stabilité et une efficacité ininterrompues et optimales de l'infrastructure publique numérique dans l'environnement opérationnel. Les activités types sont les suivantes :

- Surveillance, gestion, maintenance, évaluation et mise à niveau continues afin de garantir la sûreté et la sécurité grâce à des moyens techniques, institutionnels et normatifs.
- Emploi de méthodes innovantes afin d'assurer la mobilisation ininterrompue dans l'ensemble de l'écosystème.
- Contrôle de l'adaptation des mécanismes de recours à l'objectif visé.
- Évaluation permanente de l'état de préparation afin de tirer parti des fenêtres politiques ou des possibilités d'extension.
- Gestion de l'impact environnemental.
- Apprentissage et amélioration continus.

Le système global qui naît de l'infrastructure publique numérique nécessite un apprentissage, une réflexion et un ajustement permanents. Les apprentissages doivent être cycliques, itératifs, et assortis de recadrages s'il y a lieu. La transition d'un phase à l'autre du cycle de vie est déterminée par certaines conditions. La trajectoire de l'infrastructure publique numérique fait émerger de nouvelles capacités étape par étape tout en garantissant en permanence la sécurité et l'inclusion. Ce processus se répète à mesure que de nouveaux cas d'utilisation apparaissent, ce qui permet de veiller à ce que l'infrastructure continue de servir l'intérêt public et à ce que l'évolution et l'efficacité de la gouvernance suivent le rythme de l'adoption dans la société.

2.4 Comment ? Les principes d'harmonisation

Les principes sont des propositions fondamentales formant le socle d'un cadre souple et universel qui soit à même d'orienter le fonctionnement efficace d'une infrastructure publique numérique. La finalité d'une infrastructure publique numérique est de maximiser la participation, la capacité d'agir et la confiance de toutes et tous. Il convient pour ce faire d'atténuer les risques décrits plus haut et de gérer les risques résiduels dans le contexte de l'environnement sociopolitique de chaque pays. Pour y parvenir, toutes les autorités compétentes (voir tableau 2.1) doivent être guidées par un ensemble de principes visant à instaurer la confiance et à assurer la coordination des interventions tout au long du cycle de vie de l'infrastructure. Ces principes forment un langage commun qui aide à renforcer la compréhension mutuelle et à soutenir la coopération continue.

Les principes énumérés dans le Cadre sont le fruit de plusieurs méthodes de recherche, notamment la consultation de diverses parties prenantes, l'examen de ressources secondaires, l'analyse d'études de cas et la discussion avec les entités chargées de la mise en œuvre dans les pays. Ces principes doivent être régulièrement réexaminés et actualisés à mesure que le paysage des infrastructures publiques numériques évolue.

Les principes sont divisés en deux catégories : **(1) Les principes fondamentaux** , **(2) les principes opérationnels**. La première catégorie regroupe les principes qui devraient servir de base à toute infrastructure publique numérique, tandis que la seconde réunit ceux qui entrent en jeu au niveau opérationnel et peuvent varier selon le contexte.

Principes fondamentaux : les éléments constitutifs d'une infrastructure publique numérique sûre et inclusive

F1. Ne pas nuire

Les préjudices causés à des personnes ne sautent pas toujours aux yeux. Le respect d'un cadre fondé sur les droits humains tout au long du cycle de vie de l'infrastructure publique numérique permet d'anticiper, d'évaluer et d'atténuer efficacement tout préjudice éventuel en matière de droits humains et toute inégalité de pouvoir.

F2. Ne pas discriminer

Toutes les personnes, quelles que soient leurs identités croisées, devraient bénéficier d'un accès impartial et de l'égalité des chances dans l'emploi. Les risques liés à la situation de toutes les communautés vulnérables, des groupes généralement marginalisés et de celles et ceux qui se désinscrivent devraient être atténués.

F3. Ne pas exclure

Toute personne devrait avoir le choix du canal (numérique ou non numérique) lui permettant d'accéder aux services offerts via l'infrastructure publique numérique et d'en bénéficier en fonction des capacités et des ressources qui sont les siennes. L'accès ne doit pas être limité, conditionné ou obligatoire, que ce soit de manière explicite ou dans la pratique.

F4. Renforcer la transparence et la responsabilité

L'infrastructure publique numérique devrait résulter d'une participation démocratique, être contrôlée par le public, promouvoir une concurrence commerciale loyale et éviter la dépendance technologique des fournisseurs. Tous les partenariats devraient être transparents, responsables et gérés en public.

F5. Respecter l'état de droit

Le fondement juridique de l'infrastructure publique numérique doit clair, les aspects juridiques et réglementaires requis doivent être pris en compte dès la conception, et l'infrastructure doit être assortie de capacités d'adaptation sectorielle (par exemple pour la santé), de mise en œuvre, de contrôle et de réglementation par le droit.

F6. Promouvoir l'autonomie et la capacité d'agir

Veiller à ce que chacun (en particulier les communautés autochtones jouissant de droits sui generis) puisse, seul ou avec de l'aide, prendre le contrôle de ses données, promouvoir sa capacité d'agir, exercer ses choix et contribuer au bien-être de la société.

F7. Promouvoir la mobilisation de la population

Tous les phases du cycle de vie de l'infrastructure publique numérique doivent être axés sur les besoins et l'intérêt des personnes et des populations en situation de vulnérabilité. Ces personnes et ces populations devraient participer aux moments critiques et faire remonter l'information dans un environnement placé sous le signe de la transparence et de la confiance.

F8. Garantir un recours et une réparation efficaces

Les mécanismes de recueil des plaintes et de réparation ainsi que les possibilités de recours sans crainte de représailles, soutenus par un examen administratif et judiciaire robuste, devraient être accessibles à toutes et tous de manière transparente et équitable au cours de la prestation de services.

F9. Donner la priorité à la durabilité future

Il est essentiel d'inculquer la prévoyance pour anticiper et limiter les préjudices persistants et intergénérationnels. Il convient par exemple d'atténuer l'impact environnemental en adoptant une stratégie zéro émission nette ou en réduisant au minimum les besoins en ressources grâce à la réutilisation des logiciels.

1. **Ne pas nuire**
2. **Ne pas discriminer**
3. **Ne pas exclure**
4. **Renforcer la transparence et la responsabilité**
5. **Respecter l'État de droit**
6. **Promouvoir l'autonomie et la capacité d'agir**
7. **Favoriser l'engagement des communautés**
8. **Garantir un recours et une réparation efficaces**
9. **Se concentrer sur la durabilité future**

Figure 2.3 | Principes fondamentaux

Principes opérationnels : favoriser la confiance et l'adaptation permanentes

O1. Tirer parti de la dynamique du marché

L'infrastructure publique numérique doit favoriser l'instauration d'un environnement toujours plus inclusif pour l'innovation publique et privée, l'objectif étant que les acteurs du marché puissent être en concurrence et proposer une variété de solutions équitables qui répondent aux nouveaux besoins de toutes les personnes dans l'ensemble de la société.

O2. Évoluer en s'appuyant sur des données factuelles

Les évaluations, enquêtes et audits indépendants, transparents et continus doivent mobiliser la population, tenir compte des préoccupations de cette dernière, être fondés sur des données factuelles et faire rapidement cesser toute activité accentuant les risques ou préjudices.

O3. Garantir la confidentialité des données dès la conception

L'infrastructure publique numérique doit intégrer des principes juridiques, réglementaires et techniques visant à faire appliquer les principes fondamentaux liés à la protection de la vie privée (par exemple la minimisation des données, les dispositions relatives à la dissociation, la possibilité de limiter l'observabilité), et des sauvegardes juridiques relatives à ces principes devraient édictées.

O4. Garantir la sécurité des données dès la conception

L'infrastructure publique numérique doit prendre en compte et améliorer en permanence les mesures de sûreté, telles que le chiffrement ou la pseudonymisation, afin de protéger les données personnelles. Un cadre juridique devrait combler les lacunes lorsque la conception technique ne suffit pas à assurer la sécurité des données.

O5. Garantir la protection des données pendant l'utilisation

Les données personnelles ne devraient être traitées ou conservées, dans le respect du droit et de manière transparente, que par le personnel qui y est autorisé et dans les limites d'un cadre juridique prenant en compte l'historique des opérations, les droits des sujets de données et les protections contre les demandes abusives.

O6. Tenir compte du genre, de la situation de handicap et de l'âge

L'expérience de l'infrastructure publique numérique n'est pas pour tout le monde la même, et certaines personnes continuent de se heurter à des difficultés et des obstacles liés à l'accès ou à l'utilisation. La mise en œuvre de l'infrastructure ne devrait pas exacerber les problèmes existants, dresser de nouveaux obstacles ou créer de nouvelles inégalités.

O7. Mettre en pratique la gouvernance inclusive

L'efficacité à long terme de l'infrastructure publique numérique dépend de la mise en place d'un cadre juridique, réglementaire et institutionnel solide qui devrait promouvoir une gouvernance multipartite transparente et participative, axée sur la sécurité et l'inclusion.

O8. Assurer la viabilité financière

Les infrastructures publiques numériques étant des infrastructures publiques, elles devraient être assorties de modèles de financement diversifiés, échelonnés et durables. Les pouvoirs publics peuvent prendre en main la phase de mise en place et les partenaires numériques locaux ou le secteur privé peuvent assurer l'exploitation et la maintenance.

O9. Créer et diffuser des ressources ouvertes

Les infrastructures publiques numériques devraient mettre en commun et réutiliser des protocoles, des spécifications et des biens publics numériques ouverts ainsi que les connaissances connexes. Il s'agit d'améliorer la souplesse et de faire en sorte que les systèmes propriétaires ne limitent pas la capacité d'améliorer la sécurité et l'inclusion.

1. **Tirer parti de la dynamique du marché**
2. **Évoluer en s'appuyant sur des données factuelles**
3. **Garantir la confidentialité des données dès la conception**
4. **Garantir la sécurité des données dès la conception**
5. **Garantir la protection des données pendant l'utilisation**
6. **Tenir compte du genre, du handicap et de l'âge**
7. **Pratiquer une gouvernance inclusive**
8. **Assurer la viabilité financière**
9. **Construire et façonner des actifs ouverts**

Figure 2.4 | Principes opérationnels

Les principes énoncés ci-dessus devraient être respectés aux différentes phases du cycle de vie des infrastructures publiques numériques, faute de quoi ils risquent de demeurer à l'état de déclarations de bonnes intentions. Le Cadre traduit ces principes en processus et les illustre par des pratiques observées afin que les autorités compétentes puissent les replacer dans leur contexte et les appliquer.

3 Quoi? Un cadre pratique

3.1 Le Cadre de sauvegardes universelles liées aux infrastructures publiques numériques

Le Cadre, qui traduit des principes en recommandations pratiques, n'a pas vocation à prôner telle approche ou telle définition. Il est conçu comme un point de départ commun pour l'examen des risques dans les pays et l'atténuation de ces risques tout au long du cycle de vie d'une infrastructure publique numérique. Ces risques peuvent surgir dans les systèmes d'identification ou de protection sociale, dans les procédures d'accès à la justice et à la santé, dans les interactions entre les registres de vérification de l'identité, de paiements et de gestion des dossiers ou dans d'autres cas de figure.

Le Cadre est conçu pour évoluer et s'adapter aux différents contextes sociétaux. Comme il est un bien public ouvert, les contributions de toutes les parties prenantes sont les bienvenues. Le Cadre n'est pas un ensemble figé de lignes directrices, mais un corpus évolutif de connaissances qui se développe grâce à la collaboration active. On trouvera à la section 4 de plus amples informations sur l'aspect collaboratif du Cadre.

Les cinq composantes du Cadre sont décrites ci-dessous :

1. **Risques à atténuer (Section 2.1):**
   Le risque est la possibilité qu'un préjudice soit causé aux personnes qui interagissent avec les infrastructures publiques numériques.

2. **Autorités compétentes (Section 2.2):**
   Groupe fonctionnel de parties prenantes qui se sont vu assigner ou qui assument des rôles, des responsabilités et une obligation de rendre compte quant à l'application et l'évolution des sauvegardes liées aux infrastructures publiques numériques.

3. **Phases du cycle de vie (Section 2.3):**
   Un cycle de vie est décomposé en plusieurs étap phases. Dans le cas de l'infrastructure publique numérique, ces étapesstades sont les suivantes : 1) genèse et étude préliminaire, 2) stratégie et conception, 3) mise au point, 4) déploiement, 5) exploitation et maintenance.

4. **Principes (Section 2.4):**
   Les principes sont des propositions fondamentales qui servent de socle à un cadre universel, souple, applicable et efficace. On a défini 18 principes visant à atténuer les risques observés dans l'écosystème.

5. **Recommandations**
   Les recommandations regroupent les processus et pratiques définis comme suit :
   a. Un processus est une série d'activités à mener pour produire un résultat qui peut être ponctuel ou récurrent. Dans le Cadre, les principes sont traduits en processus pertinents pour les autorités compétentes à différentes phases du cycle de vie.

b. Les pratiques sont liées aux processus et mettent en lumière ce qui a été fait ou non dans le passé. Ces pratiques sont données à titre d'exemple et peuvent évoluer ; elles ne sont pas nécessairement des meilleures pratiques, mais elles peuvent servir de référence pour la mise au point de pratiques propres au contexte.

Le Cadre est une structure de connaissance de risques interdépendants qui permet à des autorités compétentes ayant défini des principes à respecter à différentes phases du cycle de vie de l'infrastructure publique numérique de se renseigner sur les processus et pratiques à suivre. Il permet à chacun et chacune d'interroger l'outil comme toute base de connaissances ouverte et de définir les mesures à prendre.

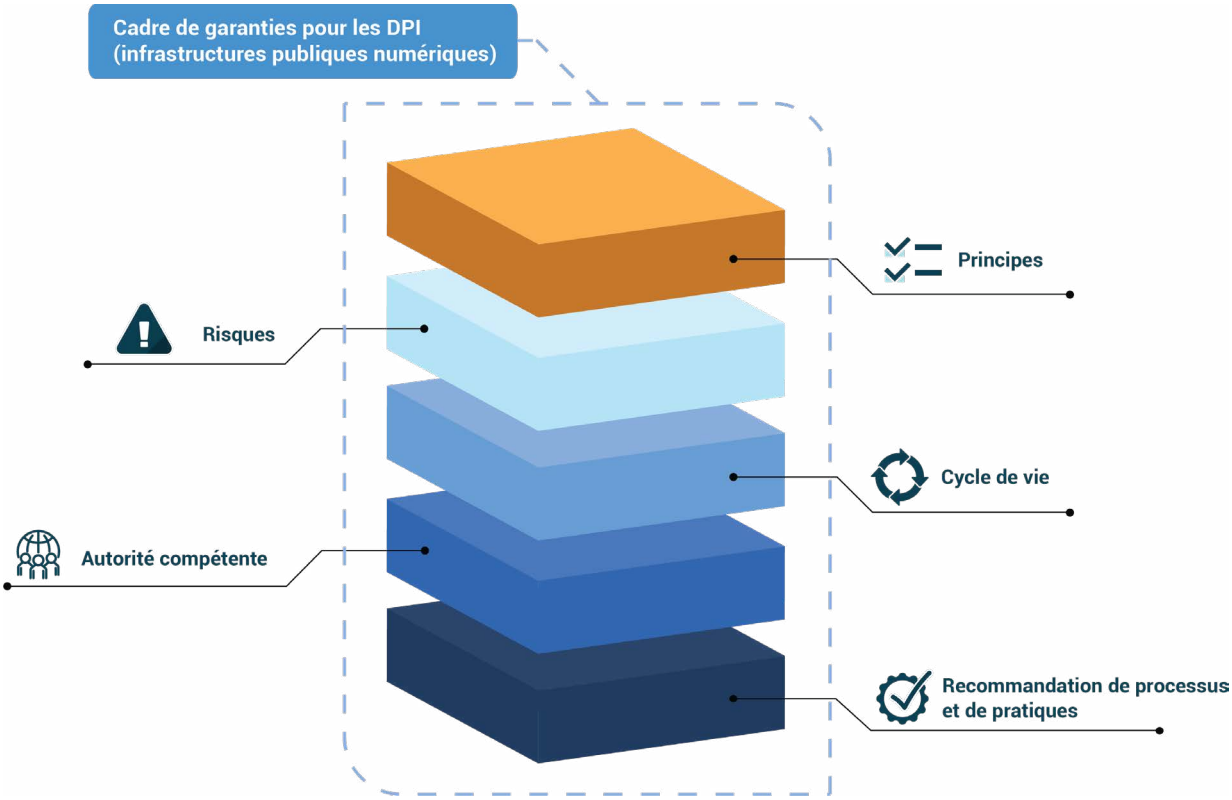

Figure 3.1 | Représentation de la bibliothèque de interactive de connaissances

3.2 Exploration du Cadre

On accède au Cadre par l'intermédiaire d'une bibliothèque de connaissances interactive ou du Centre de ressources en ligne. Les utilisateurs peuvent consulter la bibliothèque de connaissances interactive pour explorer différents scénarios, tels que les suivants :

1. Je souhaite pallier le risque d'inégalité d'accès pour les personnes marginalisées.
   Que dois-je faire?

2. Je suis un ou une fonctionnaire chargé(e) de conceptualiser une infrastructure publique numérique et de mener une étude préliminaire.
   Par où commencer?

3. Je conçois une infrastructure publique numérique et je dois remédier au risque d'inégalité d'accès.
   À quoi dois-je prêter attention?

4. Je dois mettre en œuvre le principe selon lequel une infrastructure publique numérique ne doit pas exclure.
   Où puis-je trouver plus d'informations?

5. Je souhaite intégrer la prise en compte de la protection de la vie privée et des données dans la législation sur les infrastructures publiques numériques.
   Quelles sont les étapes à suivre?

6. Je veux garantir la participation efficace du public tout au long du cycle de vie d'une infrastructure publique numérique.
   À qui dois-je m'adresser?

7. Je dois concevoir des mécanismes de recours efficaces pour les services fournis grâce aux infrastructures publiques numériques.
   Que dois-je prendre en compte?

Créer des canevas grâce à la bibliothèque de connaissances interactive

La modularité et la souplesse de la bibliothèque de connaissances interactive permettent de créer des canevas pour chacune des 5 autorités compétentes, pour n'importe lequel des 18 principes fondamentaux et opérationnels, à n'importe quelle des 5 phases du cycle de vie, afin d'atténuer n'importe lequel des 13 principaux risques.

Dans la section ci-dessous, on a simulé différents scénarios en se mettant dans la peau d'une utilisatrice type, ici, la directrice de programme d'une infrastructure publique numérique, qui souhaite savoir comment le Cadre peut générer des recommandations de meilleures pratiques. La bibliothèque de connaissances interactive permet de trouver ce processus. Notons que ces recommandations sont fournies dans un format que l'on appelle « Canevas de sauvegardes universelles liées aux infrastructures publiques numériques » et qu'elles peuvent être téléchargées.

Les scénarios suivants décrivent les besoins d'une directrice de programme qui se penche sur quatre scénarios et cas d'utilisation.

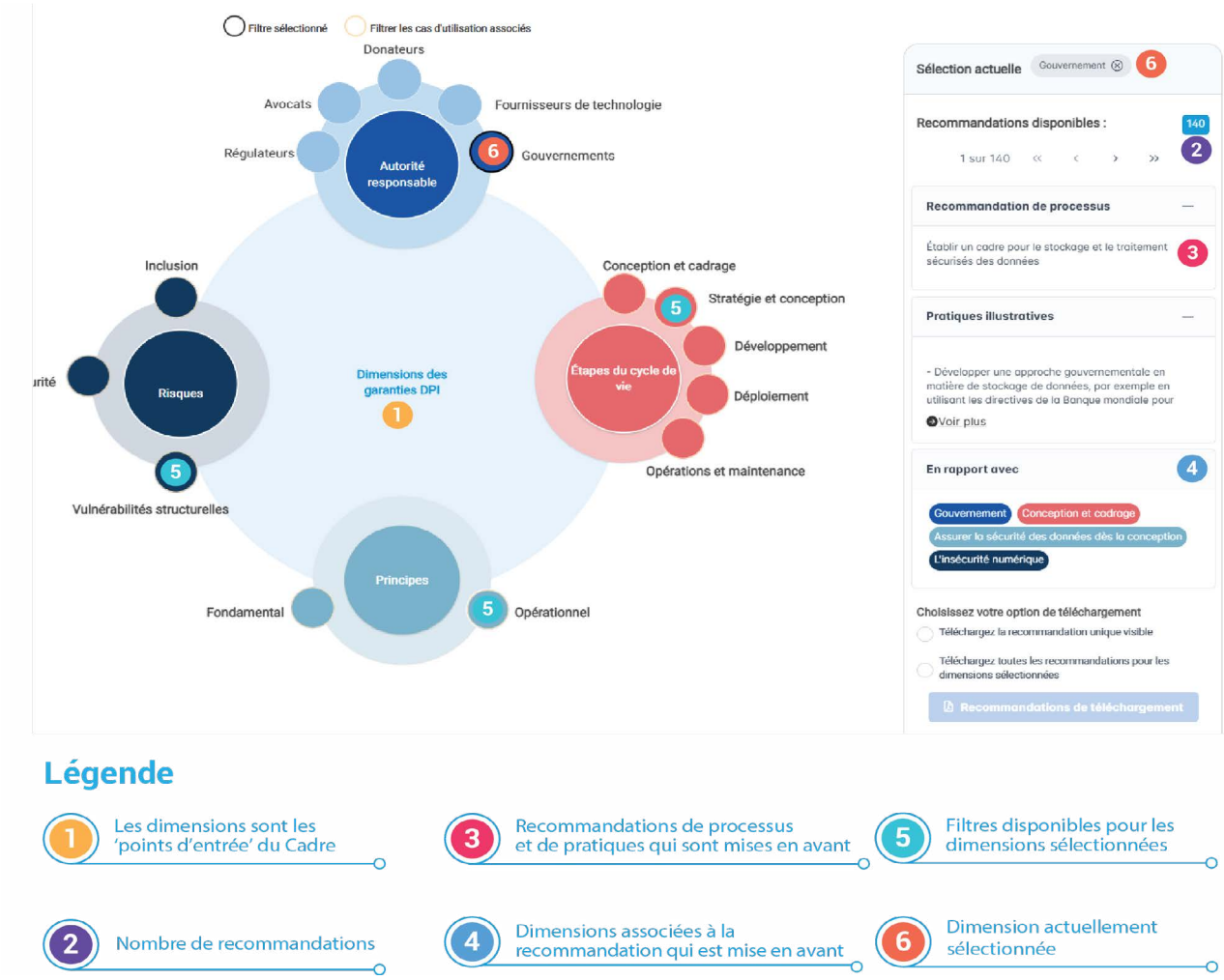

Figure 3.2 | Représentation de la bibliothèque de interactive de connaissances

1. Accès aux recommandations pour différents phases du cycle de vie

La directrice de programme, fonctionnaire, accède à la bibliothèque de connaissances interactive et sélectionne la description qui correspond le mieux au rôle qui est le sien (ou celui de son autorité compétente), à savoir « Pouvoirs publics ».

Elle sélectionne le phase du cycle de vie dans lequel elle se trouve actuellement. Comme le processus ne fait que commencer, elle choisit « Genèse et étude préliminaire », comme le montre la **figure 3.2**.

Les filtres permettent à la directrice de programme de faire ressortir une série de recommandations, tel qu'illustré dans la **figure 3.3** ci-dessous.

Dimensions sélectionnées

Autorité compétente	Phase du cycle de vie	Risque	Principe
Pouvoirs publics	Stratégie et conception	Exclusion, inégalité d'accès	Ne pas exclure

Nombre total de recommandations 92

Recommandation 1 sur 92

Principe
Ne pas exclure

Risque atténué
Exclusion, inégalité d'accès

Autorité compétente
Pouvoirs publics

Phase du cycle de vie
Stratégie et conception

Recommandation de processus

Mettre au point des processus alternatifs afin de donner la possibilité d'accéder aux services sans devoir s'abonner à un système d'infrastructure publique numérique.

Exemples de pratiques

* Conserver les services analogiques en permettant aux prestataires de services de donner aux personnes choisissant de ne pas utiliser les systèmes d'infrastructures publiques numériques la possibilité de s'authentifier sur papier et d'accéder aux versions imprimées des documents essentiels.

* Mener un dialogue continu avec les organisations de la société civile afin d'identifier de nouvelles voies d'inclusion, telles que des parcours de désinscription, et veiller à ce que les méthodes d'accès alternatives soient régulièrement actualisées et pertinentes.

* Garantir la possibilité de payer en espèces en conservant une option de paiement de petites sommes en espèces, l'objectif étant d'éviter que des personnes ne soient privées de services essentiels. Dans les cas où ces options ne sont pas viables, veiller à ce que les modes de paiement numérique restent abordables et accessibles aux populations les plus vulnérables.

Autres ressources ou références

s.o.

Figure 3.3 | Représentation du canevas des sauvegardes universelles pour les infrastructures publiques numériques (DPI) à l'intention du Responsable de programme DPI, au phase de la stratégie et de la conception

La **figure 3.3** montre les grands principes sur lesquels se concentrer, les processus connexes, les exemples de pratiques qu'elle peut suivre et les risques à prendre en compte si elle met en œuvre ces processus et pratiques au phase de la genèse et de l'étude préliminaire.

Ce canevas personnalisé peut être téléchargé et sert de référence pour le choix des mesures qu'il convient de prendre.

La figure ci-dessous montre comment le canevas créé grâce à la bibliothèque de connaissances interactive apparaît dans ce format. Le contenu change en fonction des filtres sélectionnés par l'utilisateur ou l'utilisatrice.

On trouvera d'autres exemples de cas d'utilisation ci-dessous.

La directrice de programme passe au phase de la mise au point afin d'avoir accès aux recommandations propres à ce phase. Le Canevas de sauvegardes universelles liées aux infrastructures publiques numériques qui ressort est le suivant :

Figure 3.4 | Représentation du Canevas de sauvegardes universelles liées aux DPI (Infrastructures publiques numériques) pour le responsable de programme DPI, au phase de la mise au point

2. Accès aux recommandations pour les différentes autorités compétentes

La directrice de programme peut aussi accéder à cette bibliothèque de connaissances interactive comme si elle était toute autre autorité compétente (un fournisseur de technologie, par exemple) et prendre connaissance de ce qui est attendu de l'autorité choisie au phase de la genèse et de l'étude préliminaire. Elle peut ainsi extraire un canevas comme celui qui est illustré dans la figure 3.5. Cela signifie aussi que tout fournisseur de technologie peut accéder à la bibliothèque de connaissances interactive du Cadre et consulter le même canevas pour le même phase, ou pour tout autre phase qui l'intéresse.

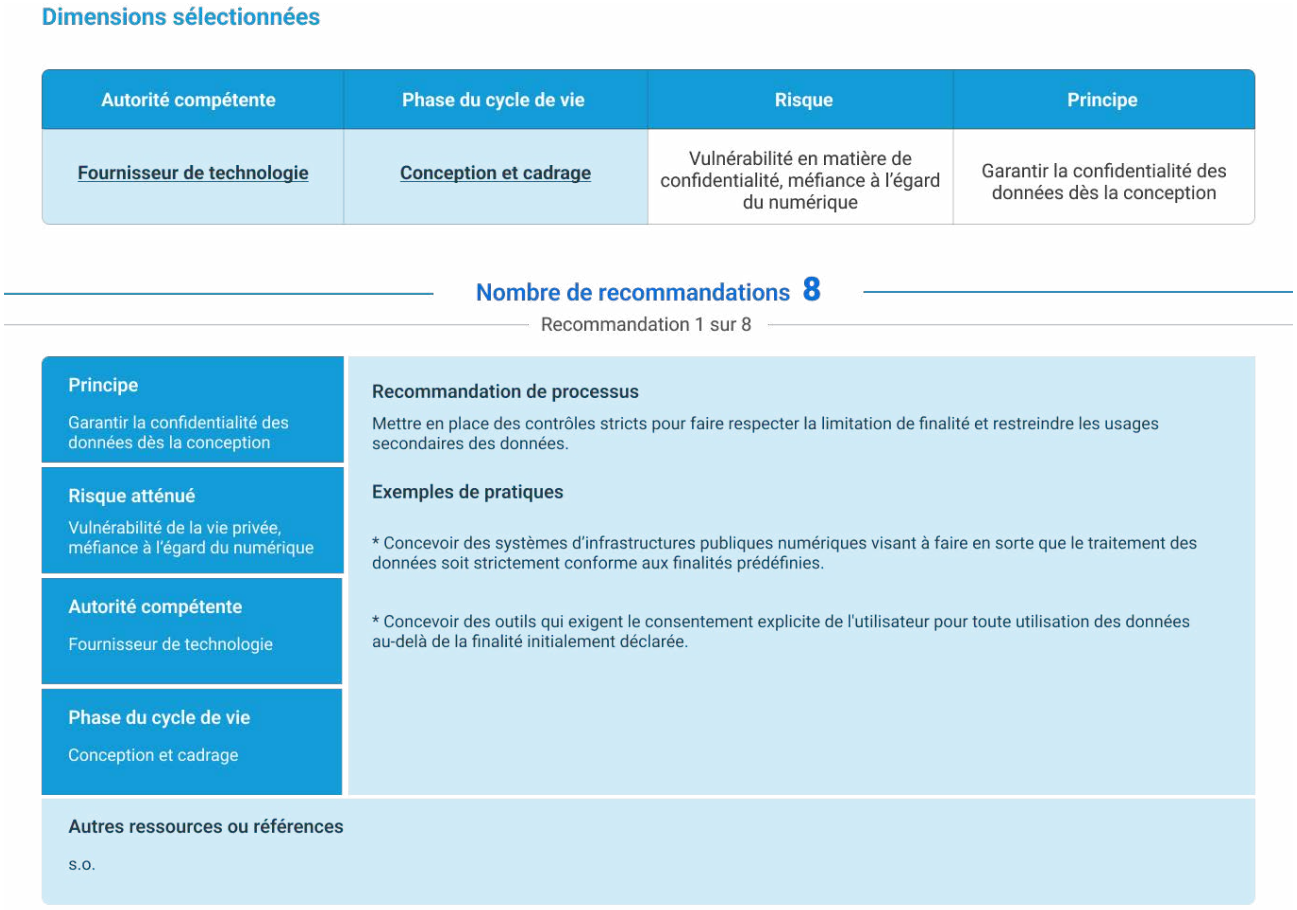

Figure 3.5 | Représentation du Canevas de sauvegardes universelles liées aux infrastructures publiques numériques pour un fournisseur de technologie, au phase de la genèse et de l'étude préliminaire

3. Accès aux recommandations par principes

La directrice de programme souhaite en savoir plus sur les recommandations de processus et de pratiques pour ce qui est d'un principe précis. Elle sélectionne le principe « Promouvoir la mobilisation de la population » (F7). Cela lui permet d'extraire un canevas qui met en évidence les processus et pratiques clés, ainsi que les risques à atténuer lors de la mise en œuvre du principe P7 sur l'ensemble du cycle de vie de l'infrastructure publique numérique. Les utilisateurs peuvent répéter cette opération pour chacun des principes fondamentaux ou opérationnels, et extraire des recommandations pour chaque phase du cycle de vie.

Dimensions sélectionnées

Autorité compétente	Phase du cycle de vie	Risque	Principe
Pouvoirs publics	Conception et cadrage Stratégie et conception Développement Déploiement et transformation Exploitation et maintenance	Méfiance à l'égard du numérique, manque de recours	**Favoriser l'engagement communautaire**

Nombre total de recommandations 13

Recommandation 1 sur 13

Principe
Favoriser l'engagement communautaire

Risque atténué
Méfiance à l'égard du numérique, manque de recours

Autorité compétente
Pouvoirs publics

Phase du cycle de vie
Conception et cadrage
Stratégie et conception
Développement
Déploiement et transformation
Exploitation et maintenance

Recommandation de processus

Créer un mécanisme de dialogue permanent avec la population afin d'éclairer la mise en place de l'infrastructure publique numérique et de veiller à ce qu'elle conserve sa pertinence.

Exemples de pratiques

* Créer une plateforme ou un forum dédié au dialogue permanent, permettant aux parties prenantes de partager régulièrement leurs retours et leurs idées.

* Favoriser une participation inclusive en veillant à ce que le mécanisme de dialogue soit accessible et représente la diversité des voix et des points de vue au sein de la communauté.

Autres ressources ou références

s.o.

Figure 3.6 | Représentation du Canevas de sauvegardes universelles liées aux infrastructures publiques numériques pour les principes et recommandations

4. Accès aux recommandations par phase du cycle de vie

La directrice de programme souhaite en savoir plus sur les processus et pratiques recommandés pour un risque donné. Elle sélectionne le risque « Inégalité d'accès ». En résulte un canevas dans lequel apparaissent les principes qui permettent d'atténuer ce risque, ainsi que les processus et pratiques qui sont conseillés aux cinq phases du cycle de vie de l'infrastructure publique numérique. Les utilisateurs peuvent répéter ce processus pour chaque risque. Les permutations et combinaisons possibles sont nombreuses.

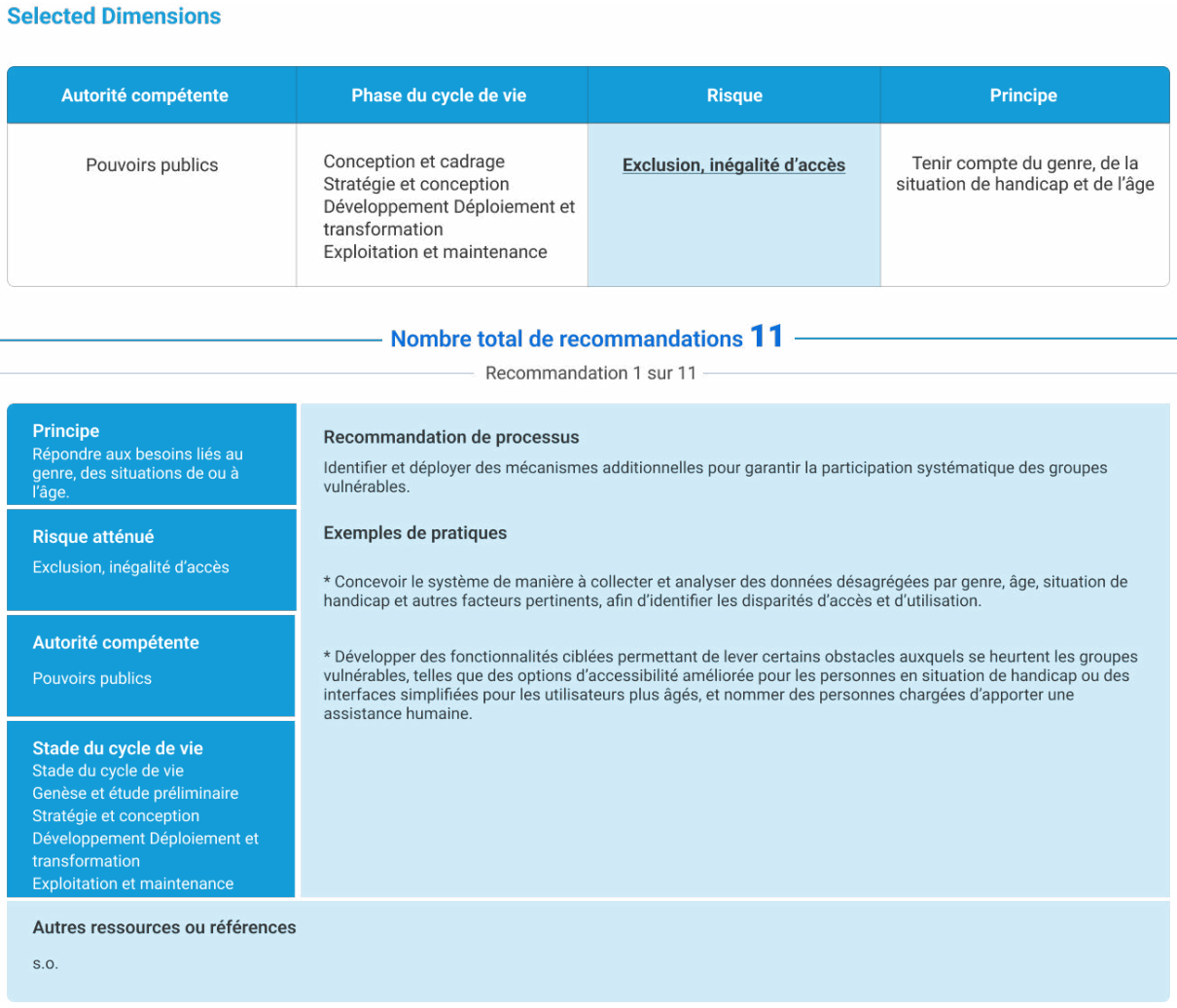

Figure 3.7 | Représentation du Canevas de sauvegardes universelles liées aux infrastructures publiques numériques pour l'atténuation des risques

Toute autorité compétente qui souhaite faciliter l'utilisation régulière du Cadre dans les pays peut télécharger un canevas à l'aide de la bibliothèque de connaissances interactive. Des notes de mise à jour seront envoyées à tous les abonnés du Cadre à chaque ajout de nouveau contenu.

3.3 Adoption du Cadre

Les parties prenantes chargées de la mise en œuvre de l'infrastructure publique numérique doivent, pour tirer tous les bénéfices escomptés du Cadre et prévenir tout préjudice pour la société, appliquer les recommandations du Cadre dans leurs activités quotidiennes. Le Cadre est particulièrement utile pour renforcer les capacités des parties prenantes, réaliser des évaluations régulières et améliorer la gouvernance d'une infrastructure publique numérique afin d'atténuer de façon proactive les risques et les préjudices.

Renforcement des capacités

L'une des conséquences de l'adoption du Cadre est le fait que les autorités compétentes et les besoins en renforcement des capacités ne seront pas les mêmes d'un groupe de parties prenantes à l'autre. Il est recommandé de concevoir le renforcement des capacités liées aux sauvegardes de manière transparente, participative et inclusive. Procéder ainsi permet à toutes les parties prenantes de bénéficier d'avantages à long terme non négligeables tout au long du cycle de vie de l'infrastructure publique numérique.

Les organisations locales, telles que les associations de défense des droits et les organisations de la société civile, aident la population à adopter les services fondés sur les infrastructures publiques numériques d'une manière inclusive et adaptée à la situation des personnes marginalisées. Elles promeuvent ces systèmes et fournissent aux équipes chargées de la mise en œuvre des remontées d'information sur les besoins des groupes habituellement marginalisés.

Cela étant, ces organisations manquent souvent des ressources nécessaires pour mener des programmes de sensibilisation, recueillir des avis et représenter les populations dans les consultations publiques. Il suffirait, pour combler cette lacune, de leur fournir un financement ou un appui régulier leur permettant de renforcer les capacités juridiques et techniques qui sont les leurs.

Les composantes et les systèmes dérivés des infrastructures publiques numériques peuvent être créés par le secteur privé, par des écosystèmes numériques locaux et par des start-ups. La prise en compte des sauvegardes passe par le renforcement des capacités de ces parties prenantes. Les autorités compétentes devraient associer la formation et le renforcement des capacités aux collaborations interinstitutions ou interdisciplinaires, notamment lors du renforcement du personnel ou en cas d'embauche dans ces domaines. Il convient d'intégrer des initiatives de renforcement des capacités s'agissant des sauvegardes liées aux infrastructures publiques numériques dans la formation professionnelle des acteurs du secteur judiciaire, l'objectif étant de permettre à ces derniers de jouer un rôle efficace dans l'application des lois et le respect des cadres réglementaires tout en supervisant les activités dans la pratique.

Enfin, toutes les phases du cycle de vie des infrastructures publiques numériques doivent être axés sur l'amélioration des capacités des personnes en situation de vulnérabilité. Il convient de mettre en œuvre des initiatives appropriées (mécanismes de financement, séries de supports explicatifs, groupes de discussion, etc.) pour éduquer en permanence les personnes dans divers contextes (langue, modes d'accès), permettre leur participation à des moments critiques et réagir à leurs remontées d'information dans un environnement placé sous le signe de la transparence et la confiance.

Évaluations régulières

Les parties prenantes doivent comprendre les retombées sociétales à court et à long terme d'une infrastructure publique numérique. Il n'existe actuellement aucun outil complet qui permette de mesurer l'efficacité et l'incidence d'une infrastructure publique numérique. La mesure de l'incidence est souvent vue par le prisme des anciennes boîtes à outils de développement numérique, qui mettent davantage l'accent sur la connectivité et l'accès.

La catégorie actuelle d'indicateurs est en grande partie centrée sur les contributions ou le niveau d'accès, en prêtant moins d'attention à l'expérience et à l'incidence sur les personnes ou au cycle de vie de l'infrastructure publique numérique, de la conception à la maintenance, en passant par la mise en œuvre. Les méthodes de mesure se fondent sur l'accès et l'adoption d'infrastructures publiques numériques en tant qu'indicateurs supplétifs de l'incidence et reposent en très grande partie sur une approche quantitative. Ces méthodes peuvent empêcher les ajustements ou les mises en œuvre agiles des politiques nécessaires pour favoriser l'inclusion et instaurer la confiance.

Il est impératif, dès les premières étapes de la conception d'une infrastructure publique numérique, de normaliser les indicateurs clés de performance s'appliquant au cycle de vie de l'infrastructure et de veiller à ce qu'ils soient ventilés, analysés et étudiés en tenant compte du genre, de l'âge, de la situation de handicap et d'autres facteurs démographiques. Les principaux indicateurs clés de performance doivent couvrir cinq éléments : 1) les personnes, 2) les institutions, 3) les politiques, 4) la technologie, 5) l'innovation. Les listes de contrôle, les questions et les indicateurs mesurables qui figurent à l'annexe 4 illustrent comment les autorités compétentes et les principales parties prenantes peuvent mettre au point et déployer des évaluations contextuelles dans les pays en tirant parti des processus d'évaluation, d'analyse, de comparaison et d'examen tout au long du cycle de vie de l'infrastructure.

Renforcement de la gouvernance

Les autorités compétentes doivent mettre au point un cadre global axé sur les résultats qui régisse la gouvernance, le contrôle et la collaboration pour ce qui est de la mise en œuvre de l'infrastructure publique numérique tout au long de son cycle de vie. Ce cadre doit reposer sur quatre piliers : **1) les normes de gouvernance, 2) les mécanismes de contrôle, 3) le renforcement des capacités, 4) le développement équitable**.

Pilier	Conception	Mise en œuvre	Contrôle
Normes de gouvernance	Mise au point de normes de gouvernance sur l'ensemble du cycle de vie de l'infrastructure publique numérique à partir des principes et processus du Cadre.	Incitation à l'adoption de ces normes dans les politiques, lois, réglementations et collaborations nouvelles ou remises au goût du jour.	Contrôle du respect des normes de gouvernance et de leur efficacité.
Mécanismes de contrôle	Mise en place d'organes de contrôle communs.	Création de procédures normalisées d'examen des processus et pratiques du cycle de vie de l'infrastructure publique numérique.	Publication de rapports réguliers sur la gouvernance des infrastructures publiques numériques.
Renforcement des capacités	Mise au point de programmes visant à renforcer les capacités humaines et la mobilisation de société civile dans la gouvernance des infrastructures publiques numériques.	Mise en place de programmes de formation et de sensibilisation à l'intention des autorités compétentes, de la population et du secteur privé.	Évaluation de l'incidence des initiatives de renforcement des capacités sur la gouvernance des infrastructures publiques numériques.
Développement équitable	Mise au point de cadres et politiques portant sur la réutilisation des technologies et la mise en commun des ressources d'une infrastructure publique numérique à l'autre.	Mise en place de mécanismes de financement en faveur du développement équitable des infrastructures publiques numériques.	Mesure de la réduction de la fracture numérique et de l'amélioration de la sophistication des infrastructures publiques numériques.

Table 3.1 | Mesures qui sont recommandées pour améliorer la gouvernance des infrastructures publiques numériques

4 Évolution du Cadre

L'évolution rapide du paysage des infrastructures publiques numériques exige du Cadre qu'il soit dynamique et adaptable. À l'instar de l'élaboration du Cadre selon un processus de cocréation inductif et déductif, son évolution suivra un processus d'actualisation continue qui sera fondé sur l'écoute et l'apprentissage. Cette version 1.0 du Cadre repose sur cinq composantes (voir fig. 3.1). Précisons que la liste des autorités compétentes, des pratiques et des processus n'est pas exhaustive, et que d'autres remontées d'information et observations recueillies au cours de son déploiement seront synthétisées et intégrées dans la nouvelle base de connaissances à mesure que le Cadre évoluera.

L'initiative DPI Framework utilisera les canaux ci-dessous pour écouter, apprendre et faire évoluer le Cadre:

1. **Mobilisation de l'écosystème**

   L'initiative continuera de recueillir des remontées informations lui permettant d'élaborer de nouveaux processus et pratiques, de définir de nouveaux indicateurs clés de performance et de tirer les enseignements des contributions de spécialistes et de praticiens. Elle continuera de mobiliser l'écosystème en le sensibilisant grâce à des campagnes (récits d'expériences réussies, témoignages et études de cas), des ateliers et des appels à contribution. Le public sera invité à donner son avis sur des forums en ligne et dans des webinaires ouverts. Les groupes sous-représentés feront l'objet d'une attention particulière. Les avis seront systématiquement examinés et pris en compte afin de veiller à ce que le Cadre intègre les différents points de vue et besoins.

2. **Mise en œuvre dans les pays**

   L'initiative collaborera activement avec les parties prenantes dans les pays, directement et à travers l'écosystème, afin de les accompagner dans leur trajectoire d'adoption d'infrastructures publiques numériques. Il s'agira notamment de recenser les projets, de faciliter la mise en relation avec les entités chargées de l'assistance technique ou des financements, et d'apporter un appui au suivi ou à l'évaluation afin d'améliorer les retombées. Les enseignements à retenir de la mise en œuvre dans ces pays inspireront les mises à jour et améliorations continues du Cadre en veillant à ce que ce dernier conserve toute son utilité et à ce qu'il demeure efficace dans des situations multiformes.

3. **Organisations internationales**

   L'initiative continuera de collaborer avec des organisations internationales et de défendre et de soutenir l'utilisation efficace du Cadre de sauvegardes universelles liées aux infrastructures publiques numériques tout au long du cycle de vie de ces dernières. Les commentaires reçus dans le cadre de ces engagements et les processus et pratiques utilisés par ces organisations seront utilisés pour améliorer le Cadre.

Les nouveautés seront annoncées et exposées dans des notes de mise à jour régulières et détaillées. Ces nouveautés seront accessibles à toutes et tous dans la bibliothèque de connaissances interactive accessible depuis de site Web de l'initiative DPI Safeguards et le Centre de ressources sur les sauvegardes liées aux infrastructures publiques numériques. Les mises à jour pourront être téléchargées dans différents formats, ce qui permettra à chacun et chacune d'accéder facilement à la dernière version en date du Cadre et de se tenir au courant de son évolution.

Contactez-nous pour savoir plus sur l'initiative DPI Safeguards, et rendez-vous sur le Site Web et consultez le Centre de ressources pour:

- Contribuer au Cadre de sauvegardes universelles liées aux infrastructures publiques numériques.
- Demander des conseils et un appui à la mise en œuvre du Cadre.
- Nous faire part de vos observations générales sur le guide.
- Faire circuler les études de cas, les récits d'expérience et les vues qui se font jour dans votre pays, s'agissant de vos infrastructures publiques numériques ou au sein de votre collectivité.

Pour toute question supplémentaire ou pour dialoguer directement avec nous, veuillez nous contacter à l'adresse suivante : dpi-safeguards@un.org.

Annexes

Annexe 1

Liste non exhaustive de ressources sur lesquelles se fonde le Cadre

- Charte des Nations Unies. Nations Unies (1945).
- Déclaration universelle des droits de l'homme. Nations Unies (1948).
- Pacte international relatif aux droits civils et politiques. Nations Unies (1966).
- Pacte international relatif aux droits économiques, sociaux et culturels. Nations Unies (1966).
- Objectifs de développement durable. Nations Unies (2015).
- Level One Project Guide. Gates Foundation (2019).
- ID4D Practitioner's Guide (version 1.0). Banque mondiale, Washington, Clark, J. (2019).
- Plan d'action de coopération numérique. Nations Unies (2020).
- The OECD Digital Government Policy Framework: Six dimensions of a Digital Government. OECD
  Public Governance Policy Papers, No. 02. OECD Publishing (2020).
- 10 Principles for Creating Digital Public Services. e-Estonia (2021).
- Principes sur l'identification pour un développement durable : Vers l'ère numérique. Banque mondiale, Washington (2021).
- UNDP Model Governance Framework for Digital Legal Identity Systems. PNUD (2022).
- GovStack Implementation Playbook, GovStack (2022).
- Next Generation G2P Payments: Building Blocks of a Modern G2P Architecture. Banque mondiale, Washington, D.C. (2022).
- Notre Programme commun. Note d'orientation no 5. Un Pacte numérique mondial – un avenir numérique ouvert, libre et sûr pour tout le monde. Nations Unies (2023).
- DPI Tech Architecture Principles. Centre for Digital Public Infrastructure (2023).
- UK digital identity and attributes trust framework. GOV.UK (2023).
- Framework for Systems of Digital Public Infrastructure (Annex 1). G20 (2023).
- The DPI Approach: A Playbook. UNDP (2023).
- Outcome Document & Chair's Summary. Réunion des ministres chargés de l'économie numérique du G20 (2023).
- G20 Policy Recommendations for Advancing Financial Inclusion and Productivity Gains through Digital Public Infrastructure. Partenariat mondial pour l'inclusion financière. G20 (2023).
- Leveraging DPI for Safe and Inclusive Societies: Interim Report. PNUD et Bureau de l'Envoyé du Secrétaire général pour les technologies (2024).
- UN Principles for Responsible Digital Payments. Alliance « Better Than Cash » (Mieux que de l'argent liquide) (2024).
- Texte issu de la réunion ministérielle sur l'industrie, la technologie et le numérique. G7 (2024).
- ASEAN Singapore Declaration. ASEAN (2024).
- Principles for Digital Development. Principles for Digital Development (2024).

On trouvera une liste complète de ressources et de documents, sélectionnés et référencés par les six groupes de travail de l'initiative, à l'annexe 1 (page 52) du rapport d'étape Leveraging Digital Public Infrastructure for Safe and Inclusive Societies, qui a été publié par le PNUD et le Bureau de l'Envoyé du Secrétaire général pour les technologies.

Annexe 2

Membres des groupes de travail sur les sauvegardes universelles

L'expérience et les compétences spécialisées des membres des groupes de travail sur les sauvegardes universelles liées aux infrastructures publiques numériques qui participent à l'initiative couvrent, entre autres, les différentes phases du cycle de vie des infrastructures, la cybersécurité, les technologies à source ouverte et l'intelligence artificielle. Bénévoles engagés, ils se sont regroupés afin de se focaliser sur l'élaboration d'un dispositif pratique qui permette de tirer parti des infrastructures publiques numériques pour bâtir une société inclusive plus sûre et accélérer la réalisation des objectifs de développement durable.

André Xuereb
Angelina Fisher
Anir Chowdhury
Anit Mukherjee
Armando Manzueta
Assane Gueye
Ben Le Roy
Bilal Mateen
Björn Richter
CK Cheruvettolil
Catherine Highet
Cesar Perez
Chris Mahony
Clélia Cothier
Fabro Steibel
Giulia Fanti
Hilda Mwakatumbula
Janaina Costa
José Arraiza
Kasim Sodangi
Kim Mallalieu
Konstantin Peric
Laura Bingham
Laura O'Brien
Lea Gimpel
Liam Maxwell
Linda Bonyo
Maria Luciano
Marte Eidsand Kjørven
Matthew McNaughton
Moctar Yedaly
Monica Greco
Mouloud Khelif
Mphatso Augustine Sambo
Priya Jaisinghani Vora
Rahul Matthan
Robert Ochola
Sanjay Purohit
Sheryl Gutierrez
Siim Sikkut
Thomas Lohninger
Urvashi Aneja
Ville Sirviö
Yuliya Shlychkova

Annexe 3

Groupe consultatif d'organisations internationales

Le Groupe consultatif d'organisations internationales réunit des entités qui participent à la mise en œuvre et à l'élaboration des programmes de développement à l'échelle mondiale, régionale et locale, au niveau des pays ou des états. Ce groupe joue un rôle de cocréation de premier plan dans la mise au point, la validation et l'application du Cadre.

- Banque Asiatique de Développement (ADB)
- Banque africaine de développement (AFDB)
- Banque européenne pour la reconstruction et le développement (EBRD)
- Banque islamique de développement (IsDB)
- Union internationale des télécommunications (ITU)
- Organisation de coopération et de développement économiques (OECD)
- Haut-Commissariat des Nations Unies aux droits de l'homme (OHCHR)
- Haut-Commissaire des Nations Unies pour les réfugiés (UNHCR)
- Fonds des Nations Unies pour l'enfance (UNICEF)
- Université des Nations Unies (UNU)
- Entité des Nations Unies pour l'égalité des sexes et l'autonomisation des femmes
- Alliance « Better Than Cash » (Mieux que de l'argent liquide)
- Banque mondiale World Bank

Annexe 4

Indicateurs clés de performance recommandés

On trouvera ci-dessous les listes de contrôle, les questions et les indicateurs mesurables qui illustrent le type d'indicateurs clés de performance qui peuvent être étayés et appliqués par les autorités compétentes afin d'évaluer, d'analyser, de comparer et d'examiner les processus et pratiques tout au long du cycle de vie d'une infrastructure publique numérique, l'objectif étant de garantir et d'assurer la sécurité et l'inclusion des personnes.

PERSONNES	
Conception	● Pourcentage de représentation de la société dans son ensemble lors de la conception. ● Combien d'infrastructures publiques numériques sont conçues et mises en œuvre localement ? ● Combien de services sont-ils accessibles seulement en passant par une infrastructure publique numérique ? ● Pourcentage de services liés aux infrastructures publiques numériques offrant un accès alternatif ou analogique. ● Pourcentage de services offrant une solution de remplacement lorsqu'une langue n'est pas prise en charge.
Déploiement	● Nombre et pourcentage de personnes inscrites à des services fournis via des infrastructures publiques numériques ou fondés sur de telles infrastructures. ● Pourcentage de la population dont l'accès aux infrastructures publiques numériques est limité. Où vivent les personnes concernées ? ● Pourcentage d'inscription des populations habituellement marginalisées. ● Pourcentage de personnes non inscrites qui peuvent accéder aux services par d'autres moyens. ● Couverture géographique des solutions analogiques. Combien d'entre elles ne sont pas disponibles hors ligne ?
Exploitation et maintenance	● Pourcentage de la population ayant accès à des services sociaux grâce à des innovations tirant parti des infrastructures publiques numériques. ● Pourcentage de la population accédant à des prestations sociales grâce à des innovations fondées sur des infrastructures publiques numériques.

RÉPARATION	
Conception	● Nombre de mécanismes permettant d'obtenir une réparation efficace et rapide. ● Type de mécanismes de recours disponibles (administratifs, judiciaires, autres).
Déploiement	● Existence de campagnes d'information et de sensibilisation expliquant les mécanismes de recours ? (Clarté et facilité, en ligne et hors ligne, langues minoritaires.) ● Les délais et l'état d'avancement des demandes sont-ils clairement communiqués ?
Exploitation et maintenance	● Pourcentage de problèmes ayant des répercussions importantes ou graves. Pourcentage de demandes sans suite. ● Délai moyen des suites données aux plaintes ou aux demandes, globalement, pour les populations habituellement marginalisées et pour les personnes ayant un accès limité aux infrastructures publiques numériques. ● Pourcentage de problèmes réglés pour lesquels les personnes concernées ont exprimé leur satisfaction ou confirmé la qualité de la prise en charge. ● Satisfaction moyenne à l'égard des mécanismes de recours. ● Pourcentage de compensations par rapport aux pertes.

INSTITUTIONS ET PROCESSUS	
Conception	● Les institutions requises (associées et indépendantes) sont-elles en place ? Quel est le niveau de préparation aux infrastructures publiques numériques ? Une étude d'impact sur les droits humains a été menée ? ● Quel niveau de performance a-t-il été enregistré s'agissant des indicateurs relatifs à l'état de droit ? ● Comment les populations marginalisées peuvent-elles accéder aux infrastructures publiques numériques avec un soutien analogique ?

Déploiement	● Quel est le modèle de viabilité des institutions ? ● A-t-on signalé des cas d'exclusion imputable à des obligations de procédure ? ● Quelles sont les mesures de responsabilisation et de transparence applicables aux institutions ? ● Dans quelle mesure les institutions sont-elles prêtes à contrôler le déploiement d'infrastructures publiques numériques ?
Exploitation et maintenance	● Quels sont les services d'assistance à valeur ajoutée, par exemple les centres d'appel ? ● Pourcentage de disponibilité et de couverture des centres publics s'agissant du support analogique ? ● Professionnels de soutien disponibles par personne. ● Personnel technique formé pour prêter une assistance à trois niveaux sur les infrastructures publiques numériques. ● Niveau de compatibilité, de complémentarité ou de convergence entre les approches et les instruments de réglementation qui permettent aux données de circuler en toute confiance. ● Les institutions sont-elles en mesure d'intégrer les remontées d'information (boucles de remontée de l'information) ? Nombre d'améliorations fondées sur une remontée d'information participative.

LOIS ET POLITIQUES	
Conception	La loi établit-elle clairement : ● l'obligation pour les services de prévoir une solution de remplacement lorsqu'une langue n'est pas prise en charge. ● le droit à une identité juridique pour toutes et tous et le droit de savoir quels sont les éléments enregistrés et quelle est l'autorité compétente. ● le régime de répartition des pertes en cas d'utilisation non autorisée et forcée. ● les règles relatives à la charge de la preuve assortie d'une présomption légale en faveur des victimes. ● le droit à une aide juridique en cas de refus d'accès ou d'utilisation frauduleuse. ● le droit égal d'accès aux services essentiels par d'autres voies, notamment analogiques ?
Déploiement	● Indicateurs concrets et pratiques en ce qui concerne le respect de l'état de droit ● Mise en œuvre équitable des lois et réglementations sur la protection de la vie privée et des politiques relatives aux données ● Institutions de contrôle qui veillent au respect des normes liées aux infrastructures publiques numériques ● Qui est autorisé à accéder aux données ? Les personnes dont les données ont été consultées peuvent-elles avoir accès aux registres indiquant qui a consulté leurs données et pourquoi ?
Exploitation et maintenance	● Affaires en cours, en instance et classées qui relèvent de la violation de droits ● Litiges signalés et réglés s'agissant du paiement numérique ● Combien d'institutions utilisant des infrastructures publiques numériques respectent-elles les normes minimales associées à ces infrastructures ?

DYNAMIQUE DU MARCHÉ	
Conception	● Combien de cas d'utilisation ont-ils été conçus avec le secteur privé ou des organisations de la société civile ? ● Les boucles de remontée de l'information efficaces sont-elles conçues pour améliorer l'inclusion ? ● Les boucles de remontée de l'information efficaces et inclusives sont-elles conçues de sorte qu'elles améliorent la sécurité ? ● Données sur les infrastructures publiques numériques diffusées sur des plateformes de données ouvertes afin de soutenir l'innovation.
Déploiement	● Quels sont les programmes qui encouragent l'innovation dans le secteur privé et les organisations de la société civile ?
Exploitation et maintenance	● Combien de cas d'utilisation mettent-ils en lumière une utilisation des infrastructures publiques numériques pour la conception de nouveaux produits et services ? ● Recettes directes générées grâce aux innovations fondées sur les infrastructures publiques numériques. ● Nombre de personnes employées grâce à des innovations fondées sur les infrastructures publiques numériques. ● Que l'infrastructure publique numérique a-t-elle apporté à l'écosystème de l'innovation ou de l'entrepreneuriat ? ● L'infrastructure publique numérique ou les exigences connexes ont-elles entravé l'accès des entreprises au marché ? ● Quelle est l'incidence de l'infrastructure publique numérique sur le ratio entre économie formelle et économie informelle ?

TECHNOLOGIE	
Conception	● Sur quelles normes et orientations techniques l'infrastructure publique numérique se fonde-t-elle ? ● L'infrastructure publique numérique est-elle interopérable avec d'autres systèmes dans le pays ? ● Les technologies déployées sont-elles aussi inclusives pour les citadins que pour les ruraux ? ● L'infrastructure publique numérique dépend-elle de technologies propriétaires ? À quel point est-elle ouverte ?
Déploiement	● Délai moyen d'inscription et nombre de problèmes d'inscription recensés. ● Comment les données circulent-elles d'un système interopérable à l'autre ? ● Comment et où les données sont-elles stockées ?
Exploitation et maintenance	● Pourcentage d'échecs d'opérations chez les ruraux et chez les citadins. ● Une évaluation de l'impact sur l'environnement a-t-elle été menée ?

Annexe 5

Directives relatives à l'indexation du Cadre pour le Centre de ressources

Explorez le Centre de ressources sur les sauvegardes universelles liées aux infrastructures publiques numériques, où chaque élément du Cadre est indexé afin de faciliter la navigation.

Risques

- RS1-RS4 s'agissant des risques pour les personnes (sécurité)
- RI1-RI14 s'agissant des risques pour les personnes (inclusion)
- SV1-SV5 s'agissant des risques pour les sociétés (vulnérabilités structurelles)

Cycles de vie

- L1 à L5

Principes

- F1-F9 s'agissant des principes fondamentaux
- O1–O9 s'agissant des principes opérationnels

Les processus sont ensuite indexés sous F1.1, F1.2 et ainsi de suite, et alignés sur chaque principe. Ce système permet aux utilisateurs de localiser les informations utiles et d'adopter les mesures qu'il convient de prendre à partir du Cadre. Cette indexation facilite le recensement et le référencement des changements à venir à mesure que les différents éléments évolueront.

Annexe 6

La bibliothèque de connaissances interactive

Veuillez scanner le code QR ci-contre pour accéder à la bibliothèque de connaissances interactive et créer un canevas de recommandations.

À propos de DPI Safeguards

L'initiative DPI Safeguards est un processus multipartite regroupant différentes voix invitées à se mettre d'accord sur un cadre de sauvegardes visant à guider la conception et la mise en œuvre d'infrastructures publiques numériques aux quatre coins du monde.

Lancée le 17 septembre 2023, l'initiative incarne un engagement à inclure et à protéger chaque personne, où que ce soit, tout en accélérant la réalisation des objectifs de développement durable.

À propos du Bureau de l'Envoyé(e) du Secrétaire général pour les technologies

Le Bureau de l'Envoyé(e) du Secrétaire général pour les technologies a été créé pour promouvoir la coopération numérique mondiale. Chargé de remédier aux difficultés nouvelles liées au numérique, de coordonner les initiatives numériques multipartites et de conseiller les hauts responsables onusiens sur les tendances technologiques, le Bureau joue un rôle essentiel dans l'exploitation du potentiel des technologies au service des objectifs de développement durable. Mettant l'accent sur une approche ouverte et inclusive, l'Envoyé(e) pour les technologies assure la synergie entre les entités des Nations Unies et sert de principal point de contact s'agissant de la coopération numérique dans le système des Nations Unies au sens large.

Pour en savoir plus, consultez le site un.org/techenvoy/fr et suivez-nous sur LinkedIn ou X.

À propos du Programme des Nations Unies pour le développement

Le Programme des Nations Unies pour le développement (PNUD) est le principal organisme des Nations Unies luttant pour mettre fin aux injustices liées à la pauvreté, à l'inégalité et aux changements climatiques. Collaborant avec un vaste réseau de spécialistes et de partenaires présents dans 170 pays, le PNUD aide les pouvoirs publics à mettre au point des solutions intégrées et durables pour les populations et la planète.

Pour en savoir plus, consultez le site undp.org et suivez-nous sur LinkedIn ou X.

New York, NY 10017, États-Unis

Donateurs

L'Initiative de Sauvegardes de l'Infrastructure Publique Numérique remercie chaleureusement les partenaires suivants pour leurs contributions financières et en nature, sans lesquelles elle n'aurait pas pu remplir ses responsabilités :

Union européenne
Co-Develop
Fondations Gates
Organisation internationale de la Francophonie (OIF)

DIGITAL PUBLIC INFRASTRUCTURE
Universal Safeguards

Nations Unies
Bureau de l'Envoyé du Secrétaire général pour les technologies

UNDP