

---

Cette traduction est disponible grâce à la contribution volontaire de Mme Mélanie Nédélec. Le FGI lui en est reconnaissant. Elle ne représente pas une quelconque position de l'organisation.

## Messages du FGI de Lillestrøm

La **20e réunion annuelle du Forum sur la gouvernance de l'Internet** a été organisée par le Royaume de Norvège à Lillestrøm du 23 au 27 juin 2025.

Les **messages du FGI de Lillestrøm** offrent aux décideurs un aperçu général des réflexions actuelles sur les enjeux clés de la gouvernance de l'Internet et de la politique numérique. Ils sont directement issus des 262 sessions organisées lors du FGI 2025. Les organisateurs des sessions ont été invités à identifier eux-mêmes les principaux points à retenir et les appels à l'action à la fin de leur session pour alimenter ces messages. Ces messages s'appuient également sur les rapports des initiatives nationales, régionales et jeunesse du FGI.

Un ensemble de messages préliminaires, élaboré par le Secrétariat du FGI, a été publié le 27 juin pour consultation par la communauté jusqu'au 14 juillet. Les messages définitifs du FGI 2025 font partie des conclusions de la réunion annuelle.

Le Forum s'est tenu sous le thème général « *Construire ensemble la gouvernance numérique* ». Les sessions étaient organisées autour de quatre thèmes principaux :

- [Bâtiment] **Confiance et résilience numériques**
- [Bâtiment] **Innovation durable et responsable**
- [Bâtiment] **Accès universel et droits numériques**
- [Bâtiment] **Coopération numérique**

Les messages de ce document sont structurés en conséquence.

*Avertissement : les opinions et points de vue exprimés dans ce document ne reflètent pas nécessairement ceux du Secrétariat des Nations Unies. Les désignations et la terminologie employées peuvent ne pas être conformes à la pratique des Nations Unies et n'impliquent aucune prise de position de la part de l'Organisation.*

## Table des matières

Messages du FGI de Lillestrøm	1
[Bâtiment] Confiance et résilience numériques	4
Le thème	4
Messages du FGI de Lillestrøm	4
[Bâtiment] Innovation durable et responsable	8
Le thème	8
Messages du FGI de Lillestrøm	8
[Bâtiment] Accès universel et droits numériques	12
Le thème	12
Messages du FGI de Lillestrøm	12
[Bâtiment] Coopération numérique	15
Le thème	15
Messages du FGI de Lillestrøm	15

## **Messages et autres résultats du FGI de Lillestrøm**

Les **messages du FGI de Lillestrøm** recueillent les opinions exprimées par la communauté multipartite lors de la réunion du FGI. Les rapports à l'origine de ces messages sont disponibles à l'adresse <https://intgovforum.org/en/content/IGF-2025-outputs>.

Les messages du FGI de Lillestrøm complètent les résultats et observations compilés par d'autres pistes ; ceux-ci sont répertoriés sur <https://intgovforum.org/en/content/IGF-2025-outputs>.

## [Bâtiment] Confiance et résilience numériques

### Le thème

[GDC 3, 4, 5](#) - [SMSI C5, C9, C10](#) - [ODD 9, 16, 12, 17](#) ; *Cybersécurité et confiance, Gouvernance des données, Intelligence artificielle, Médias et contenus, Droits et libertés [Renforcement des capacités]*

Un Internet résilient, interopérable et fiable est essentiel pour garantir la stabilité et la sécurité des infrastructures de communication, des services et des échanges de données face à la multiplication des cybermenaces et aux perturbations des infrastructures numériques. La désinformation, le piratage de données, les discours haineux, l'utilisation abusive d'informations privées, les réponses biaisées de l'IA et autres éléments d'information confus et imprécis sont des défis courants pour l'Internet que nous utilisons et apprécions.

### Messages du FGI de Lillestrøm

#### Infrastructure numérique

- À mesure que la dépendance aux services numériques augmente, la tolérance aux perturbations diminue. L'appairage et le transit sont essentiels à une interconnexion robuste, permettant un internet plus rapide et plus fiable. Une coopération étroite entre les gouvernements et les propriétaires d'infrastructures privées est essentielle pour garantir la résilience et renforcer et développer les infrastructures numériques.
- Il est nécessaire de cartographier les différents modèles et mécanismes de réponse aux crises au sein du système des Nations Unies et au-delà, et d'analyser comment ils peuvent être extrapolés pour répondre aux situations où les communications sont perturbées et les infrastructures Internet critiques attaquées dans les zones de conflit et de crise. La mise en place d'un mécanisme multipartite pour garantir le financement, l'engagement politique et d'autres facteurs devrait permettre de réagir efficacement, rapidement et dans le respect du droit international relatif à la protection des droits de l'homme et à l'aide humanitaire.
- L'engagement de la communauté multipartite en faveur d'un Internet ouvert et interopérable recèle un fort potentiel d'action pour garantir l'accès des civils et la sécurité des infrastructures Internet de base dans les contextes de conflit et de crise. Cependant, il se heurte également à d'importantes limites. De même, les cadres normatifs et réglementaires, notamment le droit international humanitaire et le droit international des droits de l'homme, offrent des outils importants, mais ne sont pas exempts de contraintes. Le Forum sur la gouvernance de l'Internet (FGI) et son Forum des meilleures pratiques devraient servir d'espace où ils se connectent, interagissent et se renforcent mutuellement pour relever ces défis cruciaux.
- La résilience du réseau mondial de câbles sous-marins repose sur une planification proactive, une redondance intégrée et une capacité de réaction rapide aux incidents. Les menaces pesant sur les infrastructures de câbles sous-marins transcendant les frontières nationales, la collaboration régionale et internationale est essentielle, tout comme le soutien aux pays aux ressources limitées.
- Les États devraient prendre des mesures concrètes pour mettre en œuvre le Cadre des Nations Unies pour un comportement responsable des États, qui devrait devenir un cadre concret. La coordination et la traduction avec toutes les parties prenantes concernées devraient avoir lieu

aux niveaux national, régional et mondial. Le soutien au renforcement des capacités (notamment par des exercices de simulation et le renforcement de la coopération entre CERT), le partage des meilleures pratiques et la discussion sur la manière d'améliorer la protection des infrastructures critiques constituent un élément essentiel de la mise en œuvre.

- Une infrastructure cloud plus résiliente, diversifiée et souveraine pourrait réduire la dépendance à l'égard d'un petit nombre de fournisseurs mondiaux dominants. Elle pourrait soutenir l'innovation locale, garantir la clarté réglementaire et renforcer la confiance. Elle permettrait aux pays et aux communautés de façonner leur infrastructure numérique selon leurs propres conditions.
- Promouvoir des pratiques responsables dans les infrastructures Internet nécessite la mise en place d'un processus multipartite fiable pour favoriser la collaboration face à des défis tels que les activités nuisibles et la censure. Ce processus doit privilégier une communication ouverte plutôt qu'une élaboration de normes rigides, et privilégier la transparence plutôt que la restriction de l'accès. Il doit favoriser la responsabilité mutuelle et l'interopérabilité afin d'instaurer la confiance et de permettre une coopération efficace.
- Une analyse politique et juridique complète est nécessaire pour identifier et clarifier les ambiguïtés réglementaires, examiner les conflits entre les cadres juridiques, évaluer l'influence commerciale et remédier aux incohérences juridictionnelles qui entravent une gouvernance responsable de l'Internet. Une stratégie de plaidoyer coordonnée devrait être élaborée pour promouvoir des lignes directrices harmonisées, transparentes et applicables dans toutes les juridictions concernées.
- La confiance dans l'infrastructure d'Internet, y compris dans son système de noms de domaine (DNS), est essentielle. Les collisions avec les identifiants blockchain doivent être évitées. Les discussions multipartites sur l'intégration responsable des identifiants blockchain offrent à la communauté Internet l'occasion de poursuivre l'objectif collectif de construire un Internet sûr, fiable et digne de confiance.
- Les discussions sur les systèmes d'armes autonomes (SAA) et leurs impacts technologiques, juridiques, éthiques, sécuritaires et développementaux doivent être inclusives et transparentes, et ne pas se limiter à des forums fermés et spécialisés. Il est urgent de coopérer au niveau international, comme l'ont souligné le Secrétaire général des Nations Unies et le CICR, qui ont appelé à la négociation d'un instrument juridiquement contraignant sur les SAA d'ici 2026. Des solutions globales exigent l'engagement actif des gouvernements, de la société civile, du monde universitaire, de la communauté technique et de l'industrie. Le Groupe d'experts gouvernementaux sur les systèmes d'armes létaux autonomes (GGE sur les SALA), les résolutions de l'Assemblée générale des Nations Unies menées par l'Autriche, l'initiative néerlandaise et coréenne de la Commission mondiale sur l'intelligence artificielle responsable dans le domaine militaire (GC REAIM) et les plateformes multipartites telles que le FGI jouent un rôle essentiel dans la promotion de l'action collective et la sensibilisation du public.

### **Sécurité en ligne / intégrité de l'information / sécurité des enfants**

- La vision du Pacte numérique mondial d'un espace numérique inclusif, ouvert, sûr et sécurisé n'est pas seulement une aspiration, mais un cadre pratique qui devrait guider notre travail quotidien. Que ce soit en coordonnant les efforts pour l'intégrité des élections, en élaborant des lignes directrices pour la protection de l'enfance ou en établissant des partenariats multipartites, nous contribuons activement à cette vision mondiale.

- Les initiatives impliquant les gouvernements, les scientifiques, les médias, les annonceurs, les influenceurs et autres professionnels concernés apportent des réponses plus efficaces et durables aux menaces à l'intégrité de l'information. Plutôt que de se concentrer sur des acteurs isolés, elles devraient s'adresser à l'ensemble de l'écosystème informationnel, en le réorientant vers des contenus fiables et scientifiques, favorisant la sensibilisation du public et l'élaboration de politiques éclairées. Dans ce contexte, il est important de mettre en place des mesures réglementaires fondées sur des données probantes, facilitant l'accès aux algorithmes et aux flux de contenus sur les grandes plateformes à des fins de recherche.
- La confiance transcende la technologie. Elle est fondamentalement humaine et sociale. Une cybersécurité efficace repose sur l'intégration de la transparence, d'un engagement communautaire inclusif et d'une culture numérique citoyenne afin de renforcer la confiance du public et de contrer des pratiques telles que le « privacy-washing ». Cela nécessite la mise en œuvre de mandats de sécurité dès la conception grâce à des outils politiques appropriés, le lancement d'initiatives de renforcement de la confiance et de culture numérique centrées sur l'humain, et l'établissement de cadres d'interopérabilité régionaux et internationaux.
- Lutter efficacement contre les abus en ligne, notamment la fraude et les abus DNS, nécessite une coordination, une collaboration intersectorielle et une action fondée sur les données. Aucun acteur ni secteur ne peut relever ces défis seul. La communauté Internet doit collaborer avec d'autres secteurs, tels que le secteur des paiements, l'hébergement et les fournisseurs de cloud, pour apporter des réponses ciblées. Il est essentiel de créer un écosystème permettant un partage d'informations efficace, grâce à des initiatives telles que Global Signal Exchange et Net Beacon. Cet effort doit être à la fois intersectoriel et multipartite.
- Le débat sur le chiffrement devient souvent enraciné et conflictuel, les positions polarisées entravant toute avancée significative. Pour progresser, les parties prenantes devraient se concentrer sur des domaines spécifiques où un compromis est à la fois possible et urgent, plutôt que de laisser les affrontements idéologiques bloquer l'action. La communauté du FGI devrait jouer un rôle clé en facilitant des discussions ciblées afin d'explorer et de tester des solutions techniques et politiques garantissant à la fois un chiffrement fort et un accès légal, notamment dans des contextes comme la protection de l'enfance.
- Les pays, quelles que soient leur région et leur contexte, sont confrontés au défi de créer des environnements numériques sûrs et stimulants pour les enfants. Construire un avenir numérique inclusif et respectueux des droits de l'enfant ne se limite pas aux entreprises technologiques traditionnelles et aux plateformes en ligne. D'autres acteurs du secteur, des marques aux investisseurs, ont un rôle essentiel à jouer, notamment en utilisant leur influence sur les autres acteurs de l'écosystème.
- Les plateformes devraient adopter une approche fondée sur les droits de l'enfant, respectueuse de la dignité, de la vie privée et de l'intérêt supérieur de l'enfant. L'absence de mécanismes solides, normalisés et appliqués à l'échelle mondiale pour protéger les enfants dans l'environnement numérique demeure une lacune critique. Une approche transparente et centrée sur l'enfant est essentielle pour créer un espace en ligne sûr. La protection des enfants en ligne doit aller au-delà des rapports et des statistiques de transparence, et exiger un engagement durable et significatif. Des mécanismes de signalement accessibles et adaptés aux enfants sont essentiels pour leur permettre de s'exprimer. Ils doivent savoir comment et où signaler un préjudice, et se sentir en sécurité, soutenus et confiants lorsqu'ils le font.

- Les problèmes liés aux deepfakes et aux deepfakes sexuels s'intensifient à l'échelle mondiale, alimentés par les violences sexistes et l'évolution rapide des plateformes en ligne. Les systèmes juridiques, éducatifs et techniques peinent à suivre le rythme. La résolution de ce problème nécessite une collaboration coordonnée et multipartite, mais les efforts actuels restent fragmentés et insuffisants. Pour renforcer la prévention et la responsabilisation, des investissements ciblés sont nécessaires dans des bases de données de détection localisées et des technologies d'imagerie immuables. Parallèlement, des programmes complets d'éducation numérique sont nécessaires pour éduquer les jeunes et les décideurs. les décideurs sur les risques, les préjudices et les responsabilités associés à l'utilisation et à la mauvaise utilisation de ces technologies.
- Les cybercrimes causant des préjudices personnels ou des répercussions émotionnelles sont tout aussi cruciaux à combattre que ceux motivés par des motivations financières. Des réponses sensibles au genre doivent être intégrées aux efforts de lutte contre la cybercriminalité et les préjudices en ligne, qui touchent de manière disproportionnée les femmes et les filles. Des cadres juridiques et des instruments législatifs solides sont essentiels, mais ils doivent s'accompagner d'une formation complète de l'ensemble du système de justice pénale, des forces de l'ordre aux procureurs et aux juges, sur la manière d'accompagner efficacement les victimes.

## [Bâtiment] Innovation durable et responsable

### Le thème

*[GDC 1, 2, 4, 5](#) - [SMSI C1, C6, C7, C10, C11](#) - [ODD 7, 8, 9, 13, 14, 15, 16, 17](#); Durabilité environnementale et changement climatique, Enjeux économiques et développement, Technologies émergentes et innovation, Intelligence artificielle, Thèmes techniques et opérationnels*

Les avancées en intelligence artificielle, en informatique quantique, en blockchain, en Internet des objets et dans d'autres domaines offrent le potentiel d'améliorer l'efficacité, la décentralisation et l'accessibilité, stimulant ainsi la croissance économique, l'inclusion numérique et le développement sociétal. Cependant, leur développement et leur adoption comportent des risques, notamment des conséquences environnementales négatives et des impacts socio-économiques importants. La surveillance éthique et la gouvernance inclusive sont de plus en plus importantes à mesure que le rôle de ces technologies s'accroît au sein de la société. Un équilibre doit être trouvé entre innovation, responsabilité et durabilité dans les plateformes numériques et les technologies émergentes.

### Messages du FGI de Lillestrøm

#### Biens publics numériques

- Les biens publics numériques (BPN) sont essentiels à la création d'une société inclusive où chacun peut participer et réaliser ses aspirations. Ils sont essentiels à la réalisation des Objectifs de développement durable.
- Aucun pays ne peut mener seul la transformation technologique. Nous devons utiliser nos ressources plus efficacement, coopérer et partager les technologies grâce à des partenariats mondiaux, au partage des connaissances et au développement collaboratif.

#### IA, travail et compétences

- L'IA s'infiltré dans tous les secteurs. La révolution de l'IA va au-delà des suppressions d'emplois et transforme fondamentalement la création de valeur et les bénéficiaires. Ceux qui savent utiliser l'IA seront très recherchés, tandis que ceux qui n'ont pas accès à la formation ou aux outils risquent d'être laissés pour compte.
- Nous pouvons tracer la voie de l'avenir du travail par nos politiques et nos choix ; la technologie elle-même ne le détermine pas. Nous devons veiller à ce que les travailleurs soient autonomes, et non marginalisés, afin d'éviter d'élargir la fracture numérique. Il est essentiel d'investir dans la maîtrise du numérique, notamment pour les femmes, les jeunes et les travailleurs de l'économie informelle, et de promouvoir la transparence, la responsabilité et l'équité sur le lieu de travail.
- Investir dans les compétences numériques des citoyens est nécessaire pour la compétitivité, mais aussi pour que chacun puisse bénéficier des technologies et services numériques. Les systèmes éducatifs devraient aider les citoyens à savoir quand remettre en question les systèmes d'IA et leur permettre d'exploiter leurs propres données.

- Les stratégies nationales devraient donner la priorité à l'éducation inclusive et à la maîtrise de l'IA afin de donner aux sociétés les moyens d'un avenir numérique soucieux du climat et d'intégrer la maîtrise de l'environnement et les principes de l'IA verte dans les programmes d'IA.

### **Désinformation, modération de contenu, IA et médias/journalisme**

- Les grands modèles linguistiques (LLM) sont apparus comme un nouvel outil de modération de contenu, mais ils présentent des risques de renforcement de la discrimination systémique, de la censure et de la surveillance. La plupart des plateformes peaufinent un petit nombre de modèles fondamentaux plutôt que de développer leurs propres modèles, ce qui entraîne une concentration du pouvoir dans la modération de contenu, les décisions prises lors de la formation LLM se répercutant sur les plateformes.
- La modération des contenus par l'IA manque de transparence quant à sa mise en œuvre et à la gestion des risques, car l'engouement suscité par l'IA occulte souvent les atteintes avérées aux droits humains. Nous devons investir dans des outils favorisant la transparence des contenus par l'IA et favoriser la co-conception de produits impliquant des acteurs multiples, associant experts politiques, utilisateurs, société civile et groupes sous-représentés dès les premières phases de conceptualisation et de test. L'émergence de l'intelligence artificielle modifie fondamentalement la lutte contre la désinformation, avec des réponses générées par l'IA souvent détachées des sources originales et rendant impossible l'identification des sources fiables.
- Un engagement intersectoriel accru et la création de coalitions entre les acteurs des médias (notamment les organisations de défense des droits numériques et les médias pour le développement) sont nécessaires pour comprendre l'impact de l'IA et intégrer une utilisation responsable et éthique de l'IA dans les médias. Les voix des médias indépendants et d'intérêt public du Sud doivent être activement impliquées.
- Les déclarations sur l'IA éthique sont importantes, mais nous devons également surveiller leur traduction dans la pratique et évaluer leur impact pour garantir une utilisation éthique de l'IA dans le travail médiatique quotidien.

### **Infrastructure**

- La construction d'infrastructures de nouvelle génération est impérative pour l'inclusion numérique à l'échelle mondiale. La gestion des données est essentielle à un avenir numérique juste et inclusif, et cela doit se refléter dans les mécanismes de financement internationaux, le renforcement des capacités et l'élaboration de normes. L'autonomisation des utilisateurs des pays du Sud grâce à la gestion des données soutient l'innovation locale, permet une participation compétitive aux marchés numériques et réduit la dépendance aux plateformes centralisées.
- Il est essentiel de relier l'innovation technique aux politiques publiques. Les constructeurs, les investisseurs, les décideurs politiques et les acteurs de la société civile doivent collaborer plus étroitement pour garantir que les infrastructures de nouvelle génération reflètent à la fois les réalités du marché et les valeurs publiques. Les stratégies multilatérales et nationales de développement numérique devraient privilégier les infrastructures qui autonomisent les utilisateurs dès leur conception.

- L'intérêt public, l'égalité, l'interopérabilité et l'inclusion sont essentiels aux infrastructures publiques numériques (IPN). Garantir que les IPN soient développées et utilisées de manière inclusive et sécurisée est un fondement essentiel de la coopération numérique mondiale. Il est crucial de renforcer les capacités des gouvernements, d'adopter des politiques open source lorsque cela est possible et de mettre en place des cadres de gouvernance numérique complets pour instaurer la confiance et garantir une adoption sûre des IPN.
- Les infrastructures publiques numériques (IPN) présentent des caractéristiques de monopole naturel qui, en particulier dans les plateformes d'identité fondamentale, de paiement et de santé, créent le risque que les partenariats public-privé accordent un contrôle opérationnel excessif aux entreprises en place, leur permettant de monétiser les données publiques avec un rendement sociétal minimal.
- Nous devons concevoir des accords contractuels qui maintiennent l'infrastructure publique numérique (IPN) en tant qu'infrastructure publique partagée, tout en favorisant l'innovation grâce à des partenariats avec le secteur privé. Nous devons établir des cadres réglementaires propices aux approches participatives de gouvernance des données, investir dans le renforcement des capacités des fonctionnaires, des autorités de protection des données, des organisations de la société civile et des dirigeants communautaires afin de garantir que les décisions politiques soient éclairées par les connaissances locales, afin d'éviter la concentration du marché et de garantir une utilisation compétitive des données.

### **Connectivité**

- Environ 2,6 milliards de personnes dans le monde ne sont toujours pas connectées à Internet. Accélérer la collaboration internationale est essentiel pour combler la fracture numérique. L'accessibilité et la connectivité à Internet sont un droit. Les parties prenantes doivent collaborer à l'élaboration de politiques inclusives et de modèles de connectivité favorisant l'ouverture et l'accessibilité financière.
- Nous devons donner aux utilisateurs d'Internet dans les zones rurales les moyens d'agir en leur fournissant les compétences numériques nécessaires à un avenir durable des réseaux communautaires.

### **Environnement et santé**

- Des modèles évolutifs et économes en énergie sont déjà opérationnels et permettent un déploiement de l'IA à faible coût et à faible consommation d'énergie dans des environnements vulnérables au changement climatique et pauvres en ressources. L'IA open source peut réduire considérablement les doublons, les coûts et la consommation d'énergie, tout en favorisant la collaboration mondiale.
- Intégrer la transparence tout au long du cycle de vie de l'IA afin de garantir que la consommation d'énergie et de ressources soit mesurée, divulguée et minimisée est un élément clé d'une gouvernance équitable de l'IA. Les gouvernements et l'industrie devraient prioriser et encourager l'innovation en matière d'IA économe en énergie, et exiger des développeurs et des déployeurs qu'ils mesurent et rendent compte de l'impact des systèmes d'IA sur l'énergie, les émissions et l'eau, au moyen de normes de durabilité, de cadres d'audit et d'exigences de divulgation tout au long du cycle de vie.
- La qualité et la granularité des données numériques demeurent essentielles à une modélisation crédible des risques environnementaux et sanitaires. Pour répondre aux préoccupations d'accessibilité, de normalisation et d'interopérabilité, nous devons investir dans la maîtrise du

numérique et le renforcement des capacités en matière de santé publique, en particulier dans les pays du Sud.

- Les solutions numériques doivent être fondées sur une conception axée sur la valeur et régies par des cadres inclusifs. Nous devons passer d'écosystèmes numériques axés sur l'engagement à des écosystèmes numériques axés sur les objectifs, en particulier pour les communautés mal desservies.

### **Écart d'équité en matière d'IA, éthique de l'IA et petits acteurs de l'IA**

- Le fossé mondial en matière d'équité en matière d'IA se creuse, exposant les pays du Sud à un risque croissant d'exclusion. Des approches d'IA locales, inclusives et centrées sur l'humain sont essentielles pour obtenir un impact significatif. Il est nécessaire de renforcer les capacités locales en investissant délibérément dans la formation, les infrastructures et l'inclusion linguistique.
- Les décideurs politiques devraient concevoir une réglementation de l'IA qui protège les valeurs publiques et favorise l'innovation. Les considérations éthiques ne peuvent être ajoutées après coup aux technologies émergentes. L'éthique doit être une compétence fondamentale pour toutes les parties prenantes, et les développeurs doivent trouver un équilibre entre réussite technique et perspective éthique et durable à chaque étape.
- Les petits États et les start-ups peuvent rester compétitifs dans le domaine de l'IA en s'appuyant sur des outils open source, une expertise métier et des partenariats stratégiques, notamment dans les domaines où l'agilité, une expertise pointue et la confiance contextuelle comptent plus que l'échelle. Ils ne doivent pas attendre d'être invités, mais se positionner comme co-créateurs de l'avenir numérique.
- Les grandes entreprises technologiques devraient s'engager dans une véritable collaboration avec les petits acteurs en investissant dans des écosystèmes ouverts, en soutenant le développement d'une IA légère et en co-développant des outils qui reflètent des contextes et des contraintes divers.

## [Bâtiment] Accès universel et droits numériques

### Le thème

[GDC 1, 2, 3, 4](#) - [SMSI C2, C3, C4, C7, C8, C10](#) - [ODD 1, 2, 3, 4, 5, 8, 10, 11, 16](#); *Droits et libertés, Accès universel et connectivité significative, Questions économiques et développement*

Les disparités et les inégalités en matière d'accès au numérique constituent des défis majeurs pour les communautés du monde entier. Ces fractures numériques ne peuvent être comblées sans reconnaître le lien essentiel entre accès universel et droits humains : un avenir numérique inclusif, ouvert, durable, juste, sûr et sécurisé ne peut se concrétiser que si les droits humains sont respectés, en ligne comme hors ligne.

### Messages du FGI de Lillestrøm

#### Droits de l'homme et préjudices numériques

- Il est nécessaire de renforcer la protection des droits numériques et la responsabilisation face aux préjudices numériques, notamment toutes les formes de surveillance numérique, étatiques et non étatiques, et les violations de la confidentialité des données. La responsabilisation exige une action multipartite et des lois nationales plus strictes pour lutter contre l'utilisation abusive des logiciels espions et protéger la société civile.
- Les parties prenantes devraient plaider en faveur d'un engagement politique en faveur d'une interprétation progressiste du droit international qui protège les individus et les communautés contre les violations des droits humains dans l'espace numérique. Les juristes et les praticiens devraient mettre en commun leur expertise pour concilier les principes des droits humains et du droit international afin de garantir leur respect dans les activités numériques et cybernétiques.
- La transparence et la réforme des lois nationales sur la surveillance sont nécessaires, notamment en matière de contrôle judiciaire, de publication d'informations et d'interdiction de toute intrusion incontrôlée de l'État. Il est nécessaire de soutenir les victimes et la société civile par le biais d'une aide juridique, de tests d'appareils et d'une solidarité transfrontalière pour lutter contre les abus liés aux logiciels espions et obtenir réparation. Les droits numériques doivent être garantis à tous.
- Les politiques numériques efficaces intègrent la diversité des voix dans leur formulation. Les entreprises technologiques, les gouvernements et les régulateurs devraient investir dans des garanties adéquates et des mécanismes de responsabilisation qui tiennent compte des inégalités numériques croissantes au sein des communautés majoritaires mondiales. Les voix du Sud doivent être amplifiées dans les cadres mondiaux afin que les politiques tiennent compte des réalités régionales, et pas seulement des priorités du Nord.
- Les violations des droits de l'homme peuvent survenir par des actions ou par l'inaction et la prévention d'actes répréhensibles. Les États comme les entreprises ont des responsabilités, mais les frontières entre responsabilité des États et des entreprises sont actuellement floues. Des efforts sont en cours pour remédier à ce problème, mais doivent être approfondis.
- Les Principes directeurs des Nations Unies définissent clairement les responsabilités en matière de diligence raisonnable en matière de droits de l'homme, mais la responsabilité des entreprises doit

### Messages du FGI de Lillestrøm

devenir la responsabilité de la plateforme en élaborant une méthode d'application qui reflète ce que signifie la diligence raisonnable en matière de droits de l'homme dans le contexte numérique.

- Les menaces numériques touchent tout le monde. Cependant, certains groupes sont bien plus vulnérables, car les schémas réels d'inégalité et d'oppression se reproduisent et s'aggravent dans les espaces numériques. Les femmes et les filles sont parmi les plus touchées, avec des antécédents plus élevés d'intimidation ou de menaces de violence en ligne, en particulier après avoir participé à des activités militantes ou de défense des droits humains.
- Il est important de prendre en compte les perspectives des personnes et des communautés les plus exposées aux préjudices et à l'exclusion numériques dans les processus de gouvernance numérique afin de garantir que ceux-ci restent fondés sur les droits, multipartites, transparents et démocratiques. Les technologies numériques doivent servir les droits humains et le bien social, et non privilégier le profit de quelques-uns au détriment du bien-être de tous.

## **IA éthique**

- La mise en œuvre de lignes directrices éthiques en matière d'IA est primordiale. Leur formulation doit prendre en compte de multiples aspects, notamment la vie privée et la confidentialité ; le consentement éclairé ; les biais et l'équité ; l'intégration de la supervision humaine ; l'amélioration continue ; le codage avec des garde-fous éthiques ; et le soutien aux solutions communautaires/locales.
- Sans lignes directrices éthiques, le développement, la mise en œuvre et le déploiement de modèles d'IA peuvent donner lieu à une technologie qui diffuse de la désinformation et des stéréotypes nuisibles, qui manque de vérification des faits en temps réel, qui viole les préoccupations éthiques et de confidentialité, qui fonctionne avec une compréhension limitée des émotions humaines complexes et qui perpétue les préjugés et la discrimination.
- Il est nécessaire d'intégrer la sensibilisation à la santé mentale et au suicide dans les discussions politiques, les lignes directrices et les normes relatives au développement d'Internet et de l'IA. Les parties prenantes devraient coopérer pour faciliter l'élaboration de cadres communautaires qui privilégient le contrôle des utilisateurs sur leurs données et informations personnelles de santé mentale.

## **Accès significatif**

- La connectivité numérique ne se limite pas à l'accès à Internet ; elle est fondamentale pour l'inclusion. Les écarts sont causés par une combinaison d'obstacles infrastructurels, économiques, politiques et socioculturels. De profondes disparités numériques existent dans les régions en développement, les nouvelles technologies accentuant souvent les fractures hors ligne. Alors que les économies s'empressent de répondre aux nouvelles technologies émergentes, des défis persistants en matière de connectivité et d'accès significatif persistent.
- L'inclusion numérique nécessite une approche fondée sur les droits et impliquant l'ensemble de la société, incluant la construction flexible de systèmes numériques adaptés aux besoins nationaux ou régionaux. Aucune entité ne peut à elle seule combler la fracture numérique : les gouvernements, le secteur privé, les ONG et les communautés doivent collaborer pour obtenir un impact à long terme, réalisable grâce à des politiques inclusives et des partenariats public-privé. Les efforts déployés par les partenaires multipartites pour accompagner, encourager, promouvoir et mesurer un accès significatif doivent être permanents.

- Pour les nombreuses personnes non connectées vivant dans des zones couvertes par la téléphonie mobile, les inégalités numériques ne se résument plus uniquement à la couverture des infrastructures. Les principaux obstacles sont désormais l'accessibilité financière (notamment le coût des appareils), la maîtrise du numérique et la maîtrise des compétences d'utilisation. Répondre à ces besoins nécessite une approche globale intégrant l'investissement dans les infrastructures, l'accessibilité financière, la maîtrise du numérique et l'engagement local.
- Nous devons garantir que chacun ait accès à des services utiles et pertinents dans sa propre langue. Internet et les technologies qui l'entourent peuvent être des outils puissants pour la préservation et l'utilisation des langues autochtones menacées. Les enseignants, les chercheurs et les experts du secteur peuvent télécharger des codes open source afin de promouvoir et de multiplier l'impact de la revitalisation de ces langues. La collaboration avec le secteur privé et l'utilisation des langues locales renforceront l'impact des programmes d'alphabétisation numérique.
- Les parties prenantes doivent concevoir et soutenir des solutions évolutives, telles que des réseaux communautaires et des initiatives Wi-Fi public, adaptées aux besoins spécifiques des régions mal desservies. Il est également nécessaire de subventionner les appareils numériques et la connectivité pour les groupes marginalisés, ainsi que le renforcement des capacités locales dans les langues locales. Le FGI a développé des outils lors d'activités intersessions pour encourager la reproduction, la mise à l'échelle et la localisation de projets significatifs et réussis.
- Un écosystème diversifié de fournisseurs est essentiel pour l'accès au dernier kilomètre. Le modèle traditionnel, qui repose uniquement sur les grands opérateurs mobiles, ne suffit pas à atteindre les communautés marginalisées. Parmi ces acteurs figurent les réseaux communautaires, les bibliothèques locales, les bureaux de poste et autres intermédiaires capables de proposer des solutions culturellement adaptées et abordables. Les cadres réglementaires doivent encourager cette diversité plutôt que de créer des barrières qui ne favorisent que les grands opérateurs conventionnels.

### **Infrastructure publique numérique**

- Toutes les régions aspirent à des infrastructures publiques numériques (IPN) inclusives, résilientes et centrées sur l'humain. Une approche de la gouvernance des IPN fondée sur les biens communs peut fédérer ces efforts sans les homogénéiser, en respectant l'appropriation locale et en favorisant l'harmonisation mondiale. De plus, la gouvernance peut être « intégrée au code ». Les systèmes IPN doivent être structurés de manière à refléter d'emblée des principes tels que la responsabilité, la confidentialité et l'équité.
- Les politiques doivent viser à promouvoir un accès équitable et sûr aux technologies numériques. Elles doivent garantir que les droits et les besoins des groupes traditionnellement marginalisés et opprimés soient prioritaires. Pour soutenir le développement et le déploiement de solutions numériques inclusives, il est essentiel de diversifier les modalités de financement et d'orienter l'action des bailleurs de fonds.

## [Bâtiment] Coopération numérique

### Le thème

*[GDC 3, 4, 5](#) - [SMSI C1, C2, C3, C4, C6, C10, C11](#) - [ODD 9, 10, 11, 16](#); Coopération numérique, Technologies émergentes et innovation, Intelligence artificielle, Gouvernance multipartite durable*

2025 est une année charnière dans les efforts multipartites déployés pour affiner et faire évoluer la gouvernance et la coordination de notre monde numérique. Le Forum sur la gouvernance de l'Internet (FGI) constitue une plateforme essentielle à cet effet, en s'appuyant sur un large éventail de parties prenantes et de processus, notamment l'examen du SMSI+20, le Pacte numérique mondial récemment adopté et les dialogues mondiaux en cours sur la gouvernance de l'IA, afin de relever un éventail de défis de plus en plus vaste.

### Messages du FGI de Lillestrøm

- Le risque d'inégalités numériques s'accroît, notamment dans les pays en développement, face aux avancées rapides des technologies émergentes comme l'IA. Les coûts de déploiement élevés et les compétences numériques limitées empêchent de nombreuses communautés, notamment dans les pays du Sud, de bénéficier pleinement des progrès numériques.
- Il est essentiel d'accroître la participation des pays du Sud et de la société civile aux dialogues numériques mondiaux. Il est important de renforcer l'articulation autour d'objectifs communs, mais aussi la compréhension des besoins et des réalités locales.
- Internet n'est pas sans propriétaire, et la concentration croissante du pouvoir et la dépendance croissante aux géants du numérique suscitent de sérieuses inquiétudes quant à la capacité des sociétés à préserver des espaces d'information sains, la liberté d'expression et l'accès à l'information. Pour garantir que les technologies de l'information servent les valeurs démocratiques et éthiques, et pour soutenir la pérennité de sociétés de l'information ouvertes, il pourrait être nécessaire de s'éloigner de la déréglementation, de la non-intervention et de la consolidation des entreprises, pour privilégier une gouvernance et une régulation responsables et collectives, axées sur la transparence et la responsabilité.
- Il est nécessaire d'explorer des modèles économiques durables pour garantir un accès généralisé. Des mécanismes juridiques ou institutionnels internationaux devraient être renforcés ou mis en place pour empêcher les fournisseurs privés de haut débit par satellite d'exercer une influence disproportionnée ou non réglementée sur l'accès et la connectivité à Internet dans les juridictions étrangères.
- Il est important de renforcer la coopération multilatérale et multipartite pour garantir que les avantages de la transformation numérique soient largement partagés et que personne ne soit laissé pour compte.
- Les normes techniques peuvent avoir des implications concrètes importantes en matière de droits humains, affectant l'accès aux services essentiels et augmentant le risque de surveillance ou d'exclusion. Par conséquent, l'inclusion dans l'élaboration des normes

### Messages du FGI de Lillestrøm

techniques est essentielle. Cela nécessite des mécanismes de soutien et des efforts de renforcement des capacités pour permettre une participation significative de diverses communautés, y compris la société civile et les non-ingénieurs, et pour l'intégration des cadres internationaux des droits humains à toutes les étapes de l'élaboration des normes afin de garantir des résultats éthiques et inclusifs.

- Le FGI devrait servir d'espace de confiance et de renforcement des capacités pour approfondir les discussions sur la fragmentation de l'Internet, notamment compte tenu du manque actuel de coordination entre les différents groupes d'acteurs sur les questions de fragmentation. La participation inclusive de tous les groupes d'acteurs est essentielle, car l'environnement numérique mondial est confronté à une territorialisation croissante, à un recours croissant aux approches fondées sur la souveraineté et à la normalisation du contrôle des réseaux.
- Il convient de promouvoir le développement de modèles de gouvernance numérique inclusifs et innovants qui s'attaquent aux obstacles structurels contribuant aux inégalités numériques. Il est important de privilégier l'investissement dans le renforcement des capacités numériques, en particulier dans les régions mal desservies et en développement, afin de garantir un accès équitable aux technologies émergentes.

### **FGI, Pacte numérique mondial et SMSI**

- La communauté internationale devrait éviter le chevauchement ou la fragmentation des mandats au sein du système des Nations Unies. Il est important d'exploiter les plateformes et espaces existants, tels que le FGI, d'améliorer les capacités de collaboration et de redoubler d'efforts pour inclure divers acteurs afin de renforcer le dialogue multisectoriel.
- Au sein du FGI, les efforts devraient renforcer davantage l'inclusion des communautés mal desservies et des parties prenantes de toutes les générations, entre autres, en renforçant les liens entre et avec les initiatives nationales et régionales du FGI.
- Pour favoriser la coopération numérique, il est nécessaire de renforcer les engagements et les mécanismes existants en accordant une attention particulière aux pays du Sud et aux populations marginalisées.
- Le SMSI devrait réformer son cadre multipartite afin de relever les défis contemporains de la souveraineté numérique, de la consolidation des plateformes et des technologies émergentes. Cela nécessite de renforcer les mécanismes de responsabilisation institutionnelle, d'élargir la participation des pays du Sud, d'accroître la coordination régionale et de donner plus de pouvoir au FGI.
- Il est communément admis que les lignes d'action du SMSI ont été élaborées de manière globale et neutre sur le plan technologique, afin de pouvoir être adaptées et appliquées aux innovations technologiques constantes. La principale lacune au sein du Cadre du SMSI et entre ses différentes parties (comme le FGI et le Forum du SMSI) réside dans le manque de coordination, tant sur les aspects procéduraux que sur les sujets abordés dans chacun de ces forums.
- Certains aspects sur lesquels il faut travailler pour renforcer le FGI incluent (i) la nécessité d'une coordination avec d'autres espaces de gouvernance numérique ; (ii) repenser les aspects procéduraux, y compris le fonctionnement du MAG (afin de créer des connaissances institutionnelles solides et permanentes, par exemple) ; (iii) obtenir un financement plus

robuste ; (iv) établir un mandat plus long ou permanent, pour permettre des améliorations continues ; (v) améliorer les mécanismes de partage des résultats du FGI, afin d'atteindre davantage de personnes et de publics, y compris les décideurs ; (vi) accroître la coordination entre la gouvernance mondiale et la gouvernance locale et régionale, comme une plus grande interaction avec les NRI.

- Des mécanismes d'intégration et de coordination devraient être établis entre le Forum du SMSI et le FGI, ce qui contribuerait à une meilleure harmonisation entre les lignes d'action du SMSI et les ODD.
- Les plateformes multipartites comme le FGI doivent être préservées et renforcées. Toutes les parties prenantes, y compris les gouvernements, les entreprises, la communauté technique et la société civile, doivent soutenir activement le FGI en tant que bien public mondial, tant sur le plan politique qu'opérationnel.
- Le FGI constitue une précieuse plateforme mondiale de collaboration transfrontalière et intersectorielle. Il permet aux petites et grandes nations d'influencer l'avenir numérique. à travers les générations, les industries et les intérêts.
- Le prochain examen du SMSI+20 offre une occasion cruciale de réévaluer les structures de gouvernance mondiale et de mieux intégrer les approches juridiques et techniques. Il invite à réfléchir aux progrès accomplis dans les processus multipartites et aux domaines dans lesquels l'alignement avec le droit international pourrait être renforcé.
- La définition « large » de la gouvernance de l'Internet formulée par le GTGI et adoptée à Tunis reste d'actualité malgré les évolutions technologiques et les nouveaux enjeux apparus ces vingt dernières années. Le GTGI a démontré l'intérêt et la viabilité d'un véritable processus décisionnel multipartite dans le contexte onusien. Son modèle pourrait être utilisé pour aborder d'autres questions sur lesquelles les gouvernements sont incertains ou dans l'impasse et pour lesquelles une nouvelle approche est nécessaire, comme la gouvernance des données et de l'IA.
- L'examen du SMSI devrait faciliter un véritable engagement multipartite (y compris entre les parties prenantes et les gouvernements) et établir des accords multipartites plus solides pour les efforts futurs de suivi et de mise en œuvre.
- Le FGI doit être préservé comme un lieu de discussion efficace sur la gouvernance de la couche technique de l'Internet, tout en créant un espace d'engagement multipartite sur les nouveaux défis de la gouvernance numérique.

### **Coopération mondiale en matière d'IA**

- La collaboration multipartite et intersectorielle est essentielle pour garantir que l'IA contribue aux Objectifs de développement durable (ODD) . L'IA doit être régie en plaçant les droits humains au cœur de ses préoccupations. Les systèmes d'IA doivent soutenir le développement durable, promouvoir l'égalité des sexes et refléter la diversité culturelle.
- Les approches inclusives et multipartites de la gouvernance de l'IA devraient impliquer la société civile, les experts indépendants et les communautés sous-représentées afin de garantir que les modèles de gouvernance ne soient pas dominés par des intérêts autoritaires ou purement commerciaux.

- Les écosystèmes locaux d'IA joueront un rôle essentiel pour donner aux diverses communautés les moyens de façonner l'avenir technologique. Les efforts mondiaux doivent privilégier le développement d'une IA en langues locales et d'ensembles de données culturellement pertinents afin de permettre aux communautés sous-représentées de contribuer à l'élaboration des cadres internationaux de gouvernance de l'IA.
- Les partenariats multipartites doivent être renforcés pour améliorer les compétences numériques et développer des systèmes d'IA fiables, favorisant ainsi une adoption inclusive dans divers contextes mondiaux.