Cette traduction est disponible grâce à la contribution volontaire de Mme. Muriel Alapini, Mme. Hariniombonana Andriamampionona, Mme. Melanie Nedelec et M. Arsène Tungali. L'IGF leur en est reconnaissant. Elle ne représente pas une quelconque position de l'organisation.

FORUM SUR LA GOUVERNANCE DE L'INTERNET 2022

Messages IGF d'Addis Abeba

Ce document est le résumé des points soulevés lors de la 17e réunion annuelle du Forum sur la gouvernance de l'Internet qui s'est tenue à Addis- Abeba du 28 novembre au 2 décembre 2022.

Les points de vue et les opinions exprimés ici ne reflètent pas nécessairement ceux du Secrétariat des Nations Unies. Les appellations et la terminologie employées peuvent ne pas être conformes à la pratique des Nations Unies et n'impliquent pas l'expression d'une quelconque opinion de la part de l'Organisation.

Les discussions lors de l'IGF 2022 se sont concentrées sur cinq thèmes clés identifiés pour le Pacte numérique mondial (GDC). Ce dernier a été lui-même proposé dans le rapport 2021 du Secrétaire général des Nations Unies lors du 75e anniversaire des Nations Unies, notre Programme Commun, et sera examiné par l'Assemblée générale des Nations Unies en 2023. Il s'inscrira dans le cadre de l'élaboration du Sommet du Futur prévu en 2024

Les thèmes considérés par l'IGF étaient :

- Connecter toutes les personnes et protéger les droits de l'homme
- Éviter la fragmentation d'Internet
- Gouverner les données et protéger la vie privée
- Assurer la sûreté, la sécurité et la responsabilité
- Aborder les technologies avancées, y compris l'intelligence artificielle (IA)

La communauté multipartite de l'IGF a exprimé son soutien à la proposition du Secrétaire général pour un Pacte numérique mondial. Les messages présentés dans ce document représentent les contributions de l'IGF à l'élaboration du Pacte. Les Coalitions Dynamiques de l'IGF qui traitent déjà les défis et les opportunités spécifiques en rapport avec les domaines thématiques proposés pour le GDC, ont également exprimé leur intention de contribuer aux phases préparatoires et au processus de mise en œuvre par les Nations Unies.

Connecter toutes les personnes et protéger les droits de l'homme

Thème

Le Pacte numérique mondial (GDC) proposé par le Secrétaire général des Nations Unies a pour premier principe de « Connecter tous les individus à Internet, y compris toutes les écoles ». Ce principe reconnaît que la connectivité et l'accès à Internet sont devenus des conditions préalables pour garantir les moyens de subsistance, la sécurité et l'éducation des personnes partout dans le monde, - et que la présence d'Internet dans les écoles fournit des points d'accès cruciaux, met des ressources d'information à la disposition de tous les élèves et permet l'acquisition de la culture numérique dès la petite enfance.

Pourtant, aujourd'hui, 2.7 milliards de personnes ne sont toujours pas connectées dont les plus défavorisées proviennent des pays les moins avancés et des communautés rurales Un accès significatif va au--delà de la simple connectivité et est indissociable de la protection des droits de l'homme en ligne. Un accès qui contribue au bien--être de la société doit être axé sur les droits de l'homme.

Il s'agit, entre autres,de la possibilité pour les utilisateurs de s'exprimer librement, de l'exercice sans entrave à la participation démocratique et politique, de la possibilité pour les personnes de tous horizons de faire l'expérience d'Internet sans crainte de harcèlement ou de discrimination, et de la possibilité pour les enfants de jouir des mêmes droits et protections en ligne comme hors ligne. Internet est à la fois un catalyseur de droits et doit intégrer de manière transparente les droits de l'homme établis, puisque nous augmentons notre dépendance numérique pour les fonctions de routine, et que les frontières entre la vie « en ligne » et « hors ligne » deviennent de moins en moins importantes.

Messages

Fracture numérique

- Les fractures numériques entre les différents pays et régions restent un facteur important qui affecte le développement national et international, y compris les progrès vers les objectifs de développement durable (ODD). Les pays les moins avancés et les petits États insulaires en développement (SIDS) sont particulièrement concernés. Les fractures numériques sont bien plus que des fractures de connectivité. Un accès significatif comprend les questions d'accessibilité, de prix, de contenu, de services, de culture numérique et d'autres capacités ainsi que de connectivité. L'accessibilité financière est un problème particulier pour de nombreuses personnes, notamment dans les pays du Sud.

- La pandémie de COVID-19 a démontré le rôle que joue l'Internet dans la résilience individuelle et économique, mais a aussi illustré à quel point ceux qui ne sont pas connectés ou n'ont pas un accès significatif sont désavantagés, exacerbant potentiellement d'autres inégalités. Il faudra du temps pour comprendre tout l'impact et les implications des interventions liées au COVID concernant l'accès, l'utilisation et les droits de l'homme.

- Dans toutes les sociétés, certains groupes connaissent des fractures numériques plus profondes ou ont un accès moins significatif que d'autres. Dans de nombreuses sociétés, les femmes sont moins connectées que les hommes et utilisent moins la connectivité. Le désavantage numérique est plus important dans les communautés vulnérables et marginalisées, et de nombreuses personnes subissent de multiples désavantages en raison de la combinaison de facteurs liés à l'âge, au sexe, à l'origine ethnique, à la langue, à la classe sociale et à d'autres facteurs. Des initiatives ciblées dans les infrastructures, dispositifs et services peuvent contribuer à améliorer les taux d'accès pour les groupes sociaux moins connectés, mais elles doivent être accompagnés de mesures visant à remédier à d'autres lacunes en matière d'accès significatif et doivent être associés à d'autres mesures visant à lutter contre les désavantages et la discrimination.

- Une infrastructure numérique résiliente et sécurisée est essentielle à l'inclusion numérique. Les gouvernements doivent protéger et promouvoir les infrastructures nécessaires, notamment l'électricité en réseau et hors réseau ainsi que les réseaux de communication. Dans certaines régions d' Afrique et d'autres continents, l'éloignement des communautés rurales et leur enclavement, y compris celles des SIDS, rendent la connectivité du dernier kilomètre commercialement peu attrayante pour le secteur privé. La connectivité, la rapidité et la fiabilité sont des aspects importants de la fourniture d'infrastructures. Il faudra du temps et des investissements pour améliorer la capacité des infrastructures et remédier aux déséquilibres régionaux, en particulier dans les zones rurales.

- La coopération entre les groupes de parties prenantes est importante pour garantir et permettre l'accès. Les gouvernements et les partenaires multipartites devraient soutenir la mise en place et le travail des organismes de régulation et de cadres réglementaires efficaces, relever les défis dans les zones commercialement peu attrayantes et encourager des approches innovantes en matière de connectivité, y compris les réseaux communautaires, l'attribution appropriée du spectre, l'accès fourni par les satellites en orbite terrestre basse et la disponibilité de contenu local, y compris le contenu dans les langues locales.

La fracture numérique entre les sexes et les droits des femmes

- Les hommes sont nettement plus susceptibles d'être en ligne ou d'avoir une connexion mobile que les femmes. La fracture numérique entre les sexes est particulièrement important dans les pays les moins avancés. La cible 9c des ODD, qui vise à parvenir à un accès Internet universel et abordable, ne pourra être atteinte tant que cet écart ne sera pas comblé.

- La menace de violence et de harcèlement a un effet dissuasif pour la participation des femmes en ligne. La violence sexiste en ligne est un facteur important qui entraîne et renforce l'inégalité entre les sexes en matière d'accès et d'utilisation d'Internet, ce qui conduit certaines femmes à quitter les espaces en ligne. Le rôle des services et plateformes technologiques dans la propagation de la violence sexiste doit être reconnu et traité. Les femmes devraient bénéficier de conseils pour résister à la violence sexiste en ligne et y remédier, y compris par le biais de lignes d'assistance communautaires. Les ressources, les directives communautaires et les rapports sur les plateformes doivent être disponibles dans les langues locales.

- Les concepts d'égalité des sexes, d'inclusion et de droits et de protection des femmes doivent être intégrés dans le Pacte Numérique Mondial (GDC), comme cela a été proposé par ONU Femmes.

Droits de l'homme et développement numérique

- L'accès universel doit respecter les droits de l'homme, afin de garantir qu'Internet est à la fois accessible et sûr pour tous. Il s'agit notamment de la liberté d'expression et d'association, du droit à la vie privée et d'autres droits civils, politiques, économiques, sociaux et culturels énoncés dans les accords internationaux sur les droits. Les structures de gouvernance de l'internet et la conception des technologies numériques doivent respecter ces droits. Les organismes d'élaboration de normes devraient envisager d'inviter des experts en droit de l'homme en ligne, issus de toutes les communautés de parties prenantes, afin de participer à leurs travaux.

- La transparence, la responsabilité et la diligence raisonnable en matière de droits de l'homme incombent à tous les groupes de parties prenantes, y compris les organisations intergouvernementales et internationales, les gouvernements, le secteur privé, la communauté technique et la société civile. Cela nécessitera un alignement des pratiques commerciales avec les droits numériques et la coopération entre les parties prenantes pour traiter des questions telles que la désinformation, la discrimination et les discours de haine, en particulier en période de troubles politiques, d'élections et de transferts de pouvoir.

- L'accès à Internet offre une opportunité cruciale d'accès à l'information et à l'expression. Les gouvernements devraient éviter de recourir aux coupures d'Internet en raison de leur impact négatif tant sur les droits de l'homme que sur le bien-être économique. Les médias sociaux et les entreprises de technologie devraient soutenir les citoyens dans leurs efforts de plaidoyer concernant les coupures.

*Il est important d'améliorer le suivi et la mise en œuvre des droits numériques. Un certain nombre de suggestions ont été faites pour mettre en place des dispositifs de suivi internationaux au sein du système des Nations Unies, avec un engagement multipartite. Ces dispositifs pourraient compléter et

s'appuyer sur les mécanismes existants, y compris ceux qui concernent le développement et les droits numériques et ceux qui concernent d'autres domaines tels que le changement climatique.

- Internet offre des possibilités de renforcer les droits à l'éducation, dans le cadre de politiques plus larges d'amélioration de l'éducation. La qualité de l'éducation dans les pays du Sud, en particulier pendant la pandémie, a souffert d'un manque de connectivité. Alors que les TIC peuvent permettre un accès significatif pour les étudiants, les différences dans les taux d'adoption mondiaux et locaux ont exacerbé les inégalités pré-pandémiques. L'expérience acquise pendant la pandémie peut être utilisée pour améliorer l'utilisation des ressources numériques à l'avenir.

- Des efforts doivent être faits pour aider les entreprises plus petites et locales à tirer le meilleur parti d'Internet. L'utilisation des outils numériques par les petites et moyennes entreprises a considérablement augmenté depuis 2020, mais les micro-entreprises sont toujours confrontées à des défis importants dans leur capacité à numériser leurs activités.

L'évolution du marché du travail autour des plateformes en ligne présente à la fois des opportunités et des défis pour la création d'emplois et la qualité des emplois, en particulier pour les femmes qui jouent un rôle plus important que les hommes dans le secteur informel dans la plupart des pays. Le manque de formation reste, pour beaucoup, un obstacle à la maximisation de leur potentiel d'emploi.

Les compétences numériques doivent être améliorées et des adaptations des méthodologies d'enseignement, d'apprentissage et de formation sont nécessaires pour s'adapter aux nouveaux paradigmes de l'éducation et de l'emploi. Il est important d'identifier et de combler l'écart entre les besoins de l'industrie et l'enseignement supérieur.

Éviter la fragmentation d'Internet

Thème

Le maintien d'un Internet mondial, ouvert et interopérable est une valeur fondamentale de l'IGF. Cela implique que des normes et protocoles techniques communs continuent d'être déployés pour créer un réseau de réseaux interconnectés entre les pays et les régions, et que les normes relatives au contenu et aux services soient conformes aux droits de l'homme et à l'État de droit. L'appel en ce sens, appliquer un cadre à Internet qui donne la priorité aux droits et libertés des utilisateurs ainsi qu'à la cohérence infrastructurelle de bout en bout, -a été repris dans les plans de la GDC.

Le risque de fragmentation est réel et croissant. Si la fragmentation technique et commerciale -- où le fonctionnement d'Internet est affecté par un mélange de conditions volontaires et involontaires et de pratiques commerciales - -doit être abordée, la fragmentation par la politique gouvernementale affectant le caractère ouvert et interopérable d'Internet est également préoccupante.

Messages

Comprendre les enjeux

Le Pacte numérique mondial est l'occasion de réaffirmer la valeur d'un Internet interconnecté ouvert pour la réalisation de la Charte des Nations Unies, la réalisation des objectifs de développement durable et l'exercice des droits de l'homme. Il existe un large consensus au sein de la communauté Internet sur la valeur d'un Internet mondial non fragmenté en tant que plate-forme pour l'activité humaine.

Les questions soulevées dans les discussions sur la fragmentation d'Internet sont multiples et les différentes parties prenantes donnent une variété de significations et d'interprétations au terme. Certains sont plus concernés par les aspects techniques et infrastructurels d'Internet, tandis que d'autres se concentrent sur les questions de politique publique, y compris l'accès, les droits et les impacts sur l'expérience de l'utilisateur. Ces questions sont examinées dans un projet de cadre préparé par le Réseau politique du FGI sur la fragmentation d'Internet. Le respect et la compréhension des perceptions et de l'expérience de la fragmentation des différentes personnes sont essentiels si nous voulons parvenir à des réponses efficaces et coordonnées.

Un large éventail de facteurs politiques, économiques et techniques peuvent potentiellement favoriser la fragmentation. Cependant, il ne faut pas confondre la diversité et la décentralisation avec la fragmentation. Ce sont des aspects fondamentalement positifs de l'architecture et du fonctionnement d'Internet.

Faire face au risque de fragmentation

Des mécanismes de gouvernance multipartite efficaces sont essentiels à la gouvernance de l'Internet mondial non fragmenté. Il est nécessaire de renforcer la confiance dans ces mécanismes, de veiller à ce qu'ils soient solides et durables, et de favoriser la cohérence entre les structures de gouvernance à mesure qu'elles évoluent pour relever de nouveaux défis.

Il convient d'être vigilant face aux risques de fragmentation nouveaux ou en développement. La coopération et la coordination à l'échelle mondiale seront essentielles pour identifier les signes avant-coureurs, cartographier l'impact des politiques et autres développements, et se préparer à faire face aux implications de ces changements. Une approche multipartite est la mieux adaptée pour évaluer et surveiller les conséquences involontaires potentielles des mesures qui affectent Internet et pour proposer des alternatives efficaces qui évitent ou atténuent les risques de fragmentation. Le Réseau politique IGF sur la fragmentation d'Internet est un exemple positif de cette approche.

L'ouverture d'Internet permet de favoriser l'exercice des droits de l'homme des internautes, de promouvoir la concurrence et l'égalité des chances et de préserver la nature générative d'internet de pair à pair. Les débats sur la neutralité du réseau et la gestion non discriminatoire du trafic ne sont qu'une partie des discussions plus larges dans ce contexte. La neutralité du réseau est nécessaire mais

pas suffisante pour garantir l'ouverture d'Internet. L'interopérabilité des infrastructures et des données, ainsi que la neutralité des plateformes et des appareils, sont également nécessaires.

Si les approches juridiques, réglementaires et politiques diffèrent dans le monde, une coordination active au-delà des frontières internationales est essentielle pour garantir que les approches fragmentées ne menacent pas la portée mondiale et l'interopérabilité d'Internet. Le maintien de l'intégrité du réseau mondial nécessite une collaboration réglementaire internationale et un consensus sur les principes de base.

De nombreux facteurs différents affectent l'expérience d'Internet dans différentes juridictions, notamment des contextes sociaux, démographiques, économiques, culturels et politiques différents, ainsi que des questions techniques et d'infrastructure. La poursuite de certaines formes de gouvernance numérique au niveau national peut accroître le risque de fragmentation au niveau technique de l'Internet. Toutefois, les cadres réglementaires doivent également tenir compte des exigences différentes selon les contextes et suivre le rythme de l'évolution rapide des technologies et des services.

Il est nécessaire de renforcer le partage des connaissances et des informations entre les parties prenantes, d'approfondir le débat sur la cyber-diplomatie en tant que phénomène évolutif et d'examiner les possibilités d'interventions appropriées. Les organismes de normalisation devraient continuer à améliorer la sensibilisation et l'engagement avec les parties prenantes et à améliorer la compréhension entre les communautés politiques et techniques. Les décisions techniques qui ont des implications politiques devraient être discutées par les organismes de normalisation avec la participation directe de toutes les parties prenantes concernées.

Gouvernance des données et protection de la vie privée

Thème

Les données sont la ressource clé de l'ère numérique mondialisée. Le mouvement des données stimule les économies, tandis que l'analyse des données, y compris l'analyse des mégadonnées, a été à la base d'innovations remarquables dans toutes les disciplines, de la finance à la santé en passant par l'application de la loi.

Mais l'utilisation généralisée, le flux routinier à travers les frontières et la fongibilité des données restent des sujets sensibles et non résolus. En tant qu'actif commercial transnational, les flux de données s'effectuent dans un environnement où il existe peu de cohérence entre les régimes juridiques nationaux où les défis en matière d'application sont importants. La confidentialité des données personnelles est trop souvent sacrifiée au cours des échanges de données, du point de collecte à l'application et au stockage, avec de graves conséquences pour la confiance et la sécurité.

Pour exploiter la promesse importante des données, économiquement et à des fins de recherche, il faut relancer les discussions autour de la gouvernance, de l'intégrité et de la protection de la vie privée des personnes.

Messages

La centralité des données

Les données sont devenues une ressource essentielle dans une ère de plus en plus numérique. Les flux de données sont cruciaux pour la coopération internationale dans de nombreux domaines, notamment la recherche scientifique, l'application de la loi et la sécurité nationale et mondiale. Les données, la sécurité des données et la protection des données sont des catalyseurs essentiels du développement durable. L'utilisation et le partage efficaces des données à l'échelle mondiale peuvent aider à surmonter les défis communs et les menaces posées par les crises en cascade telles que les pandémies et le changement climatique.

Les données peuvent générer à la fois des bénéfices et une importante valeur sociale. Toutefois, les avantages de l'économie fondée sur les données ont jusqu'à présent été inégalement répartis. De nombreuses personnes craignent de devenir principalement des fournisseurs de données plutôt que des bénéficiaires.

La relation entre ceux qui génèrent et ceux qui utilisent les données est importante. La pauvreté des données est un problème important, en particulier dans les communautés locales et parmi les segments vulnérables de la population. Le manque de confidentialité des données et leur protection inadéquate sapent la confiance dans la gestion des données. Il est important de développer la culture et les capacités en matière de données à tous les niveaux de gouvernement dans les programmes d'enseignement et pour le grand public.

La gestion et la gouvernance des données sont des questions complexes dans la gouvernance nationale et internationale. L'évolution des données - y compris l'analyse des mégadonnées, les innovations dans l'intelligence artificielle et l'apprentissage automatique, et les innovations dans les dimensions des politiques publiques et les ODD - démontrent la nécessité d'une prise en compte appropriée des impacts politiques, économiques et sociaux et d'une approche nuancée des interventions politiques.

Les institutions gouvernementales et réglementaires ont besoin de l'infrastructure et des capacités nécessaires pour mettre en œuvre des cadres nationaux de gouvernance des données efficaces et intégrés. Les développeurs d'applications ont la responsabilité d'assurer une conception éthique et sûre.

Confidentialité des données et justice des données

La confidentialité des données n'est pas une question de commodité ou de bonnes pratiques, mais des droits de l'homme. Outre les droits à la vie privée, à l'égalité de traitement et à la non-

-discrimination, elle affecte l'accès à d'autres droits de l'homme tels que ceux à la santé, à l'éducation et aux services publics, ainsi qu'aux droits démocratiques tels que la liberté d'expression et d'association. Les lois sur la protection de la vie privée doivent être substantielles, fondées sur des preuves claires. Les personnes concernées doivent être en mesure de comprendre clairement leurs implications.

Les flux et l'échange de données doivent se faire sans compromettre la confidentialité des données. La confidentialité des données personnelles a souvent été sacrifiée dans les processus d'échange entre la collecte d'informations et leur application, avec des risques intentionnels et non intentionnels pour la confiance et la sécurité.

L'accès et l'utilisation d'Internet ne devraient pas dépendre du suivi des données : les utilisateurs devraient avoir le droit de choisir la mesure dans laquelle leurs informations sont partagées, y compris les informations dérivées de leur activité en ligne. Les données personnelles ne doivent pas être exportées vers des juridictions qui n'offrent pas les garanties adéquates.

Les politiques doivent aller au delà de la protection des données pour aboutir à une justice des données, dans laquelle les personnes ont le choix de l'utilisation de leurs données personnelles et peuvent partager les retours et les avantages de l'innovation apportés par les ensembles de données dérivés de leurs données. Les protections de la vie privée devraient ainsi contribuer à une économie numérique plus sûre et plus prospère.

Les gouvernements et les régulateurs devraient veiller à ce que les données personnelles soient protégées, en identifiant les responsabilités différenciées des différentes parties prenantes et sans imposer de charges ou de responsabilités excessives aux utilisateurs individuels. Les politiques de gouvernance des données doivent être élaborées avec la contribution de plusieurs parties prenantes pour garantir que les défis de mise en œuvre sont compris.

La confidentialité et la protection des données sont particulièrement essentielles à la gouvernance de l'intelligence artificielle et de l'apprentissage automatique. Toutes les parties prenantes de la chaîne d'approvisionnement de l'IA ont un rôle à jouer dans le respect des droits à la vie privée.

Il est nécessaire de disposer d'organes de contrôle indépendants dotés de ressources appropriées. Les bureaux de protection des données devraient avoir pour mandat de gérer l'enregistrement des données, de fournir des conseils, de mener des enquêtes et de résoudre les plaintes des personnes concernées.

Gouvernance des données

Les questions relatives à la gouvernance des données ne doivent pas être traitées en silos ou isolément de leurs impacts.

Le paysage actuel de la gouvernance des données est un patchwork fragmenté de règles nationales, régionales et internationales impliquant des responsabilités pour les gouvernements nationaux, les entreprises du secteur privé et les particuliers.

Une plus grande cohérence est nécessaire au niveau mondial pour parvenir à une approche équilibrée dans laquelle les données sont au service des personnes et de la planète. La législation et les cadres réglementaires existants aux niveaux national, régional et international sont souvent insuffisants et ne parviennent pas à suivre le rythme de l'évolution des technologies et des applications. Ils doivent viser à garantir des normes de sécurité élevées pour les entreprises et autres organisations responsables de la détention de données.

En raison de la diversité des contextes et des défis, des histoires, des cultures, des traditions juridiques et des structures réglementaires, il ne peut y avoir un ensemble rigide de règles pour tous. Différentes personnes et organisations interprètent également des approches largement similaires de différentes manières. Cependant, si les pays et les régions doivent développer leurs approches personnalisées de la gouvernance des données, il doit y avoir cohérence et interopérabilité pour faciliter les flux de données et garantir des conditions de concurrence équitables.

La transparence, la participation et la responsabilité sont des aspects importants d'une bonne gouvernance des données.

Les éléments importants à porendre en compte dans la gouvernance des données sont notamment les suivants (liste non exhaustive) : les normes et la classification des données ; partage, échange et interopérabilité des données ; la sécurité des données et la confidentialité des données ; infrastructures de données ; données et identité numérique ; la justice et l'équité des données ; traçabilité, transparence et explicabilité des données ; minimisation et limitation des données ; exactitude et qualité des données ; biais de données, marginalisation et discrimination ; le cycle de vie des données, la spécificité et la conservation de l'utilisation des données ; la responsabilité des données et l'éthique des données ; dommages aux données, sécurité des données et protection des données.

Dans ce contexte, de nombreuses parties prenantes ont un rôle à jouer et devraient exercer leur pouvoir et influence pour promouvoir une gouvernance des données efficace, notamment les régulateurs, les chercheurs, les organismes de normalisation, les organisations de consommateurs et les utilisateurs finaux. Des politiques de gouvernance des données devraient être élaborées avec la contribution de cette communauté multipartite qui possède une expertise à la fois dans les débats juridiques sur la confidentialité et les défis du « monde réel » de la mise en œuvre de solutions efficaces de confidentialité des données.

Les économies en développement doivent renforcer leurs capacités institutionnelles pour gouverner, utiliser et gérer les données de manière globale, objective et fondée sur des données probantes, notamment par le biais de la coopération régionale et mondiale. Pour ce faire, il faut mieux comprendre les capacités institutionnelles des responsables gouvernementaux et des parties prenantes.

Flux de données transfrontaliers

Les flux de données transfrontaliers sont essentiels à de nombreux aspects du commerce électronique et du commerce numérique. Une gestion efficace du commerce intra-régional et de la chaîne d'approvisionnement repose sur la fluidité des flux de données ainsi que des biens, des services et des capitaux. Cependant, tous ces éléments nécessitent des considérations transversales complexes en matière de réglementation, de convergence, d'harmonisation des cadres juridiques, la gouvernance de l'internet, la réforme de la politique en matière de technologies de l'information et de la communication et l'infrastructure régionale stratégique

Les accords commerciaux multilatéraux, régionaux et bilatéraux actuels sont insuffisants pour les flux de données transfrontaliers actuels et futurs. Ceux-ci opèrent dans un environnement largement non réglementé avec peu de cohérence entre les régimes juridiques nationaux. Les approches diffèrent et sont contextuelles, générant des obstacles au commerce, alors que de nombreux pays ne disposent pas actuellement d'une législation ou d'une capacité d'application adéquates. Il y a un besoin croissant de développer et d'harmoniser des mesures de gestion des flux transfrontaliers qui facilitent le développement et la création de valeur économique, dans différents contextes, tout en respectant la souveraineté nationale et la vie privée des utilisateurs.

Permettre la sûreté, la sécurité et la responsabilité

Thème

La sécurité d'Internet est menacée à plusieurs égards. La cybersécurité traditionnelle concerne la protection des réseaux, des appareils et des données contre les accès non autorisés ou les utilisations criminelles. Elle englobe le problème permanent des cyberattaques, qu'elles soient perpétrées par des individus ou sanctionnées par l'État, et que les cibles soient civiles, commerciales ou gouvernementales. Des facteurs tels que l'absence d'accords de cybersécurité larges et contraignants et des réseaux insuffisamment sécurisés contribuent à la perte de possibilités de tirer pleinement parti des avantages économiques des technologies numériques, en particulier pour les pays en développement.

Les questions de sûreté, de sécurité et de responsabilité sont multiples, et comprennent des problèmes distincts concernant l'infrastructure, les services, le contenu et d'autres aspects d'Internet. Notre compréhension de la sûreté et de la sécurité, par exemple, inclut désormais les défis persistants de la mauvaise information et de la désinformation en ligne. Ces dernières années, ces facteurs ont aggravé les effets de la pandémie de COVID-19 et ont fait poser des risques importants sur les processus électoraux dans le monde. Cela a souligné la nécessité d'une responsabilité et de critères clairs pour les contenus trompeurs.

Le concept de « sécurité » peut être encore élargi à la sécurité environnementale, compte tenu des efforts visant à « écologiser » l'Internet et à réduire les émissions de carbone liées à la consommation numérique. La nécessité de traiter l'impact environnemental de la numérisation est un thème de plus en plus important dans les discussions de l'IGF.

Messages

Le rôle des décideurs politiques

La cybersécurité doit être considérée comme un défi central pour la politique Internet. Les considérations de confiance et de sécurité devraient faire partie intégrante du développement d'un accès sûr et sécurisé, y compris le respect des droits de l'homme, l'ouverture et la transparence dans l'élaboration des politiques, et une approche multipartite qui sert les intérêts des utilisateurs finaux.

La garantie de la cybersécurité et la prévention de la cybercriminalité sont deux domaines politiques importants qui nécessitent une attention sérieuse et le développement d'une expertise. Leur objectif diffère toutefois, et l'approche requise pour chacun est différente. Une approche efficace dans l'un ne le sera pas dans l'autre sans adaptation et reformulation.

Les problèmes de cybersécurité et de cybercriminalité ont des dimensions inter organisationnelles et transfrontalières. Pour y faire face, il faut :

a) des approches pangouvernementales et pansociétales qui incluent des partenariats solides et des efforts coordonnés, impliquant les parlements, les régulateurs et autres autorités et agences gouvernementales compétentes, le secteur privé, la communauté technique, les universités et la société civile ; et

b) une coopération régionale et internationale efficiente et efficace qui soit intergouvernementale, multilatérale et multipartite.

Les gouvernements, le secteur privé et la communauté technique doivent veiller à éviter d'adopter des lois sur la cybercriminalité et d'établir des normes qui affectent négativement le travail des défenseurs de la cybersécurité. Ils devraient inviter toutes les parties prenantes à participer à l'élaboration des politiques et faciliter l'interaction et le partage d'expérience et d'expertise entre leurs différentes.groupes

La société civile devrait participer aux discussions sur la cybercriminalité et la cybersécurité. Pour le faire efficacement, les parties prenantes de la société civile doivent se former aux différentes approches et questions en jeu, et travailler avec d'autres parties prenantes pour rassembler les informations et les ressources nécessaires pour participer pleinement à l'élaboration des politiques.

La cyber-sécurité

La communauté internationale devrait explorer des moyens pratiques d'intégrer le renforcement des capacités en matière de cybersécurité dans les efforts de développement numérique plus larges. Les tensions entre le désir de faire progresser la transformation numérique et la nécessité de permettre une cybersécurité efficace posent des problèmes pour permettre un environnement en ligne sûr et sécurisé et atteindre les objectifs de développement durable. S'il est nécessaire d'en faire plus pour accroître la résilience de l'infrastructure numérique, ce n'est pas suffisant. Il est grand temps de traduire les accords internationaux existants en actions réalisables.

Les normes permettant d'assurer la cybersécurité sont essentielles pour un Internet ouvert, sûr et résilient qui permet le progrès social et la croissance économique, et sont particulièrement importantes pour protéger ceux qui ne sont pas encore connectés. De telles normes ont été élaborées, mais leur utilisation doit se développer de manière significative pour qu'elles soient pleinement efficaces. Les Nations Unies pourraient aider à accélérer l'adoption mondiale des normes clés en incluant leur promotion dans le Pacte numérique mondial, en soutenant le plaidoyer et le renforcement des capacités et en encourageant les initiatives pour tester et surveiller le déploiement. La sensibilisation précoce et le renforcement des capacités sur les normes ne doivent pas être oubliés en tant que priorités dans des domaines où beaucoup doivent encore se connecter et où Internet se développe.

Il faut faire davantage pour améliorer la sensibilisation des décideurs politiques nationaux et des autres parties prenantes aux défis de la cybersécurité et aux normes et principes internationaux. Il s'agit notamment de sensibiliser et de renforcer les capacités concernant les liens entre le développement durable et la cybersécurité, en réunissant diverses parties prenantes pour mobiliser une gestion efficace, durable et inclusive de la coopération internationale pour la cyber résilience. Un certain nombre d'initiatives internationales ont été mises en place pour soutenir cela. Les opportunités de financement de la cyber résilience doivent également être abordées par les agences de financement et les autres parties prenantes.

Les normes de cybersécurité doivent faire une différence dans les expériences personnelles passées, présentes et futures des internautes. Dans ce contexte, l'écoute des expériences des victimes individuelles et organisationnelles d'attaques de cybersécurité, et celles des premiers intervenants, est importante, en particulier pour l'élaboration de nouvelles normes.

Cybercriminalité

La cybercriminalité représente une menace croissante pour de nombreux internautes. Les réglementations de lutte contre la cybercriminalité doivent tenir compte de la taille, de la capacité et des ressources des plateformes. Les obligations légales doivent tenir compte de la diversité du secteur technique et reconnaître les besoins et les circonstances des petites entreprises dans le respect de leurs obligations légales, par exemple dans la lutte contre l'exploitation de leurs services par des terroristes et extrémistes violents.

Les gouvernements et les décideurs politiques doivent veiller à ce que les réponses juridiques à l'utilisation criminelle et terroriste d'Internet préservent à la fois l'État de droit et les droits de l'homme, en tenant pleinement compte de la liberté d'expression et en garantissant la transparence et la responsabilité dans la mise en œuvre des mesures contre la cybercriminalité.

Contenu et désinformation

La désinformation peut et doit être traitée par des mécanismes qui répondent aux risques encourus par les individus et les sociétés tout en protégeant la liberté d'expression, le pluralisme et le processus démocratique. Le soutien au journalisme et aux médias professionnels joue un rôle important dans les efforts de lutte contre la désinformation, y compris l'engagement envers les normes journalistiques établies.

Les compétences en matière de médias et d'éducation numérique permettent aux citoyens d'avoir une vision plus critique du contenu ou des informations qu'ils rencontrent, aidant à identifier la désinformation et la mésinformation et à renforcer la participation démocratique. L'éducation à la culture numérique peut contribuer à accroître la sensibilisation à la sécurité en ligne, en particulier pour les personnes et les communautés les plus vulnérables. Les initiatives doivent être sensibles aux besoins et aux risques associés aux différents groupes démographiques. Différentes approches pour les jeunes et les générations plus âgées, par exemple, doivent répondre à différents modes d'utilisation.

Les programmes d'enseignement devraient inclure des compétences en matière de culture numérique aidant les enfants à être en sécurité en ligne. Les initiatives doivent impliquer les parents, les enseignants et les tuteurs. Les législateurs et les plateformes numériques devraient assumer la responsabilité d'assurer la sécurité des enfants dans un cadre des droits de l'enfant en ligne conforme aux accords internationaux sur les droits, y compris la Convention des Nations Unies relative aux droits de l'enfant.

Le système des noms de domaine a une capacité technique limitée dans ce contexte. Un dialogue continu avec les parties prenantes devrait clarifier quand et comment il peut être utilisé pour remédier à des problèmes de contenu spécifiques, et devrait renforcer les normes de procédure régulière.

Le cryptage joue un rôle important dans la construction d'un Internet ouvert, sûr et démocratique et aide les utilisateurs à assurer leur sécurité, leur confidentialité et leur liberté d'expression. Les questions relatives à l'application de la loi et à la capacité de l'utilisateur à gérer l'accès dans des domaines tels que la protection de l'enfance doivent être abordées.

Les problèmes de traduction constituent des obstacles importants qui peuvent empêcher les utilisateurs finaux de s'engager de manière significative après les normes et directives communautaires des plateformes. Les termes clés sont parfois mal traduits, ce qui entraîne des interprétations ambiguës.

Pour permettre aux plateformes et aux utilisateurs de comprendre ce que l'on attend d'eux, il est important de s'engager auprès des différentes communautés linguistiques afin d'améliorer la précision et la pertinence des traductions, y compris la communication de concepts sans équivalents directs dans différentes langues

Aborder les technologies avancées, y compris les Intelligences Artificielles (IA)

Thème

Les technologies numériques avancées façonnent de plus en plus notre économie et notre société, y compris les systèmes d'intelligence artificielle (IA) qui guident nos expériences en ligne, alimentent les appareils intelligents et influencent nos propres décisions et celles que les autres prennent à notre sujet, ainsi que les applications de la robotique et d'internet des objets qui sont déployés dans des domaines aussi divers que la fabrication, la santé et l'agriculture. Au-delà de leurs promesses, ces technologies comportent des écueils. La prise de décision algorithmique, par exemple, peut entraîner des préjugés, de la discrimination, des stéréotypes et des inégalités sociales plus larges, tandis que les systèmes basés sur l'IA peuvent présenter des risques pour la sécurité humaine et les droits de l'homme. Les dispositifs de l'internet des objets présentent des défis en matière de confidentialité et de cybersécurité.La réalité augmentée et virtuelle soulève des questions de sécurité publique, de protection des données et de protection des consommateurs.

Tirer parti des opportunités offertes par les technologies de pointe, tout en relevant les défis et les risques qui y sont liés, est une tâche qu'aucun acteur ne peut assumer seul. Le dialogue et la coopération multipartites - impliquant les gouvernements, les organisations intergouvernementales, les entreprises technologiques, la société civile et d'autres parties prenantes - sont nécessaires pour garantir que ces technologies soient développées et déployées d'une manière centrée sur l'humain et respectueuse des droits de l'homme.

Messages

Gouvernance

Les technologies avancées, y compris l'intelligence artificielle, doivent être conçues de manière à respecter l'état de droit, les droits de l'homme, les valeurs démocratiques et la diversité, et comporter des garanties appropriées.

Elles devraient profiter aux personnes et à la planète en stimulant la croissance inclusive, le développement durable et le bien-être. Les mécanismes de surveillance et d'application doivent suivre des principes et des règles, les acteurs de l'IA étant tenus responsables de tout dommage causé.

L'hypothèse selon laquelle la technologie améliore nécessairement l'égalité est erronée. Ceux qui conçoivent les technologies d'apprentissage automatique et les données utilisées pour former les applications d'IA ne sont souvent pas représentatifs de leurs sociétés. Les technologies peuvent amplifier les inégalités et nuire, en particulier aux groupes vulnérables et marginalisés.

Les sociétés doivent s'adapter à la transformation qu'entraîne l'IA en modifiant leur cadre de coopération et leur modèle de gouvernance.

La construction d'une société intelligente centrée sur l'humain nécessite la pleine coopération du gouvernement, des entreprises, des organisations sociales et des universités. Un contrôle humain continu reste essentiel pour s'assurer que les algorithmes n'aboutissent pas à des résultats indésirables ou incontrôlés. Pour y parvenir, il est essentiel de briser les silos entre les ingénieurs et les experts en politiques.

Un accord mondial sur les normes d'IA ne peut être obtenu par un processus simple. Bien qu'il existe certaines normes, il s'agit principalement de lois souples plutôt que de principes contraignants. L'élaboration de normes mondiales significatives nécessitera la participation effective de tous les pays, y compris les pays en développement et les pays développés, et les contributions des initiatives régionales, ainsi que l'engagement de toutes les parties prenantes.

Le renforcement des capacités est important dans les efforts visant à aborder les technologies avancées. Des politiques d'alphabétisation en IA, de développement des compétences et de ressources linguistiques pour les langues minoritaires sont nécessaires afin de formuler une approche véritablement mondiale des technologies de pointe.

Confiance, sécurité et confidentialité

Les cadres réglementaires devraient inclure des principes pour aider les médias sociaux et les autres plateformes à remplir leurs obligations de diligence raisonnable pour la gestion des contenus susceptibles de porter atteinte à la démocratie et aux droits de l'homme. Les cadres devraient contribuer à la conversation mondiale sur la modération du contenu en ligne afin de responsabiliser les utilisateurs, y compris les groupes les plus vulnérables et les utilisateurs de langues minoritaires. Les technologies émergentes telles que l'informatique affective, qui examinent comment les ordinateurs peuvent reconnaître, interpréter et simuler les émotions humaines, nécessitent une évaluation éthique approfondie. La transparence dans le fonctionnement et le reporting des systèmes algorithmiques est essentielle pour les droits de l'homme.

L'IA facilite l'observation et l'analyse constantes des données pour personnaliser et cibler le contenu et la publicité. Les expériences en ligne personnalisées qui en résultent risquent de désagréger les espaces d'information en ligne et de limiter l'exposition des individus à la diversité des informations.

Le manque de pluralisme de l'information peut favoriser la manipulation et la tromperie - aggravant les inégalités, sapant les débats démocratiques et favorisant potentiellement l'autoritarisme numérique, la haine et la violence.

Les parties prenantes des communautés techniques et non techniques doivent partager leur expertise et collaborer au développement de principes, de lignes directrices et de normes suffisamment flexibles pour être appliqués dans divers contextes et pour favoriser la confiance dans les systèmes d'IA.

Il est important de reconnaître et de respecter les différents contextes institutionnels et culturels des divers pays et communautés, ainsi que de promouvoir l'inclusivité et de permettre la coopération internationale en IA.

Droits et modération du contenu

Il est essentiel que les politiques de gouvernance des contenus par les plateformes en ligne, et leur application, soient conformes aux normes internationales des droits de l'homme. L'intelligence artificielle et les technologies d'apprentissage automatique sont déjà utilisées pour décider si le contenu doit être publié ou supprimé, quel contenu est prioritaire et à qui il est diffusé. Ces outils jouent un rôle important dans le façonnement du discours politique et public d'une manière qui affecte à la fois les droits de l'homme individuels et collectifs, y compris les droits sociaux, économiques et culturels et les droits à la paix et à la sécurité mondiales. Ils sont souvent déployés avec peu ou pas de transparence, de responsabilité ou de contrôle public. Il convient de remédier à cette situation.

Les mêmes technologies qui peuvent être utilisées pour promouvoir les droits de l'homme peuvent également être utilisées pour la surveillance, pour promouvoir des programmes violents et d'autres façons qui enfreignent ces droits. Les conséquences imprévues de la gestion automatisée du contenu peuvent être particulièrement préjudiciables en temps de conflit ou de crise lorsqu'elles peuvent faire taire les voix critiques à un moment où elles sont les plus cruciales.

Les normes techniques jouent un rôle important en permettant le développement et l'amélioration de la valeur des technologies numériques et des infrastructures, services, protocoles, applications et dispositifs connexes.

Ils peuvent aussi avoir de fortes répercussions sur les droits de l'homme. Pourtant, les processus d'élaboration des normes techniques au sein des organisations ne prennent pas pleinement en compte des préoccupations relatives aux droits de l'homme. Ces processus sont souvent opaques, complexes et lourds en ressources pour que la société civile et les autres parties prenantes puissent y accéder et les suivre systématiquement. Cela devrait être résolu.