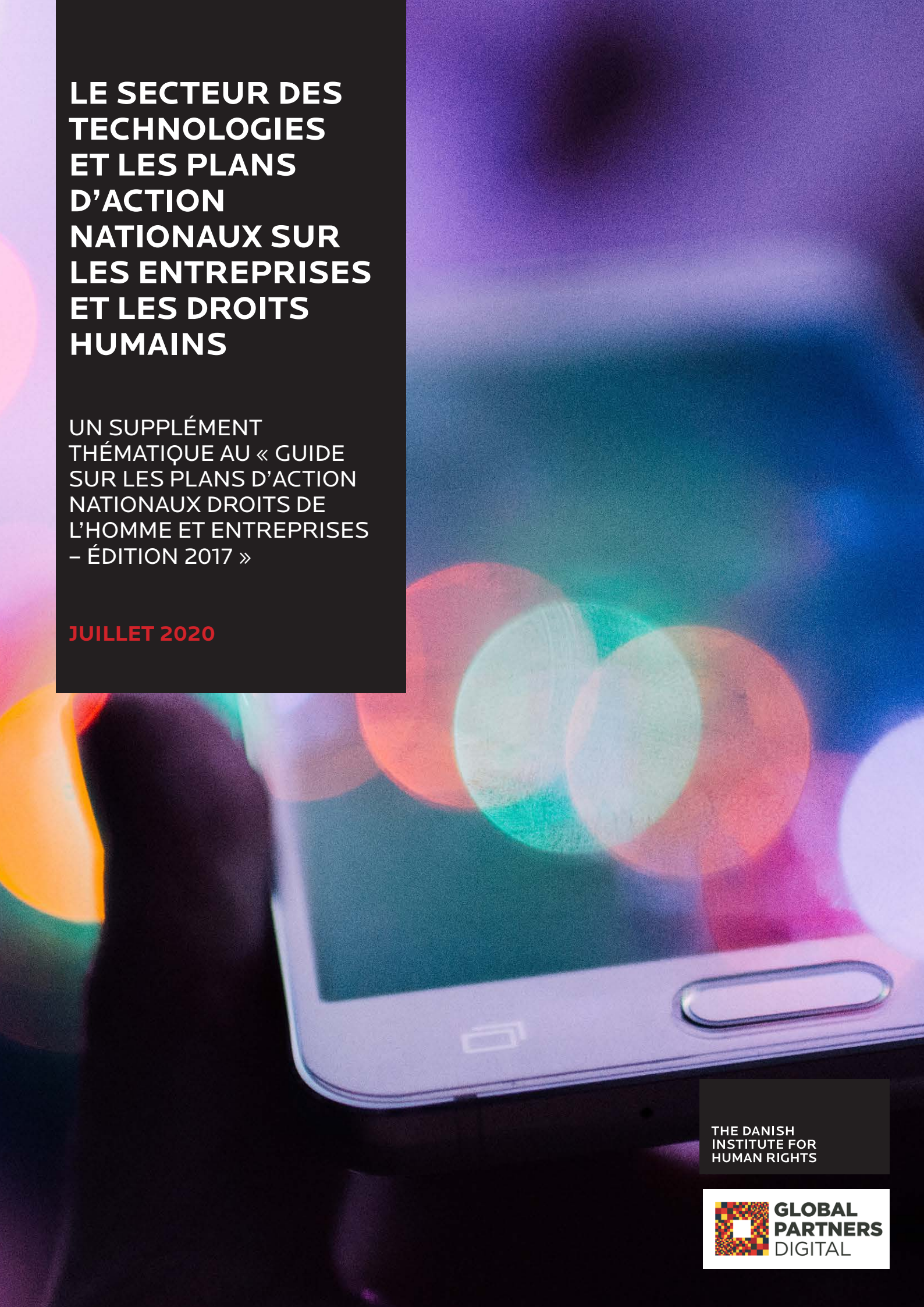
LE SECTEUR DES TECHNOLOGIES ET LES PLANS D'ACTION NATIONAUX SUR LES ENTREPRISES ET LES DROITS HUMAINS

UN SUPPLÉMENT THÉMATIQUE AU « GUIDE SUR LES PLANS D'ACTION NATIONAUX DROITS DE L'HOMME ET ENTREPRISES – ÉDITION 2017 »

JUILLET 2020



THE DANISH INSTITUTE FOR HUMAN RIGHTS

GLOBAL PARTNERS DIGITAL

Le secteur des technologies et les Plans d'action nationaux sur les entreprises et les droits humains
Un supplément thématique au « Guide sur les plans d'action nationaux droits de l'homme et entreprises - Édition 2017 »

THE DANISH INSTITUTE FOR HUMAN RIGHTS

L'**Institut danois des droits de l'homme** (IDDH) est l'institution nationale des droits humains du Danemark. Son mandat est de promouvoir et de protéger les droits humains et l'égalité de traitement au Danemark et à l'étranger. Le Département droits humains et entreprises est une unité spécialisée de l'IDDH qui met l'accent sur le rôle du secteur privé pour le respect des droits humains.

GLOBAL PARTNERS DIGITAL

Global Partners Digital (GPD) est une entreprise à but social qui se consacre à la promotion d'un environnement numérique étayé par les droits humains et des valeurs démocratiques. Nous parvenons à cet objectif en créant des espaces et des processus politiques plus ouverts, inclusifs et transparents, et en facilitant un engagement stratégique, éclairé et coordonné des acteurs ayant un intérêt public dans ces processus.

Auteurs du rapport

Richard Wingfield
Directeur des affaires juridiques chez Global Partners Digital

Ioana Tuta
Conseillère, Droits humains et entreprises auprès de l'Institut danois des droits de l'homme

Tulika Bansal
Conseillère senior, Droits humains et entreprises auprès de l'Institut danois des droits de l'homme

Remerciements

Les auteurs souhaitent remercier tous ceux qui ont contribué à l'élaboration de ce supplément thématique. Leurs remerciements s'adressent en particulier à Sebastian Smart, qui a contribué à la rédaction de la première version du supplément. Les auteurs souhaitent également saluer la contribution de Equal Rights Trust et remercient sa Directrice des affaires juridiques et des programmes, Ariane Adam, pour sa contribution ayant permis de mettre en évidence les effets discriminatoires des activités du secteur des technologies, en soulignant les obligations de non-discrimination des acteurs publics et privés et les responsabilités des acteurs privés, et en proposant des indications concernant la prise en compte de ces obligations et responsabilités dans les processus et les contenus des plans d'action nationaux.

Les auteurs remercient également les nombreux relecteurs de la première version de ce supplément thématique, dont les remarques, commentaires et suggestions ont été précieux : Dunstan Allison-Hope, Rémy Friedmann, Nora Götzmann, Emil Lindblad Kernell, Rikke Frank Jørgensen, Peter Micek, Daniel Morris, Isedua Oribhabor, Jason Pielemeier, Dr. Roxana Radu, Sabrina Rau, Elin Wrzoncki et la Commission australienne des droits humains.

TABLE DES MATIÈRES

Introduction

Au cours des dernières décennies, des bouleversements de grande ampleur se sont produits dans presque tous les domaines de l'activité humaine du fait de l'innovation et du développement technologiques numériques, avec des conséquences significatives pour l'exercice et la jouissance des droits humains sur un pied d'égalité. Il ne fait aucun doute que la technologie numérique offre un vaste éventail de possibilités quant à l'amélioration de la réalisation d'un grand nombre de droits humains. La technologie numérique permet d'assurer un meilleur accès à l'éducation et aux soins de santé, et rend la fourniture de ces services et d'autres services publics plus efficace. De nouvelles plateformes en ligne ont permis aux personnes d'accéder à l'actualité, à l'information et à des idées, et de les échanger plus facilement, et aux groupes et communautés de se mobiliser et de se rassembler.

Alors que ce supplément thématique était en cours de rédaction, le monde était presque à l'arrêt à cause de la pandémie de COVID-19. Cette dernière nous a montré que la société était de plus en plus tributaire de la technologie numérique : pour garder le contact avec notre famille et nos amis, pour l'éducation, pour parler à des collègues de travail et, ce qui est peut-être plus important encore, recevoir des informations.

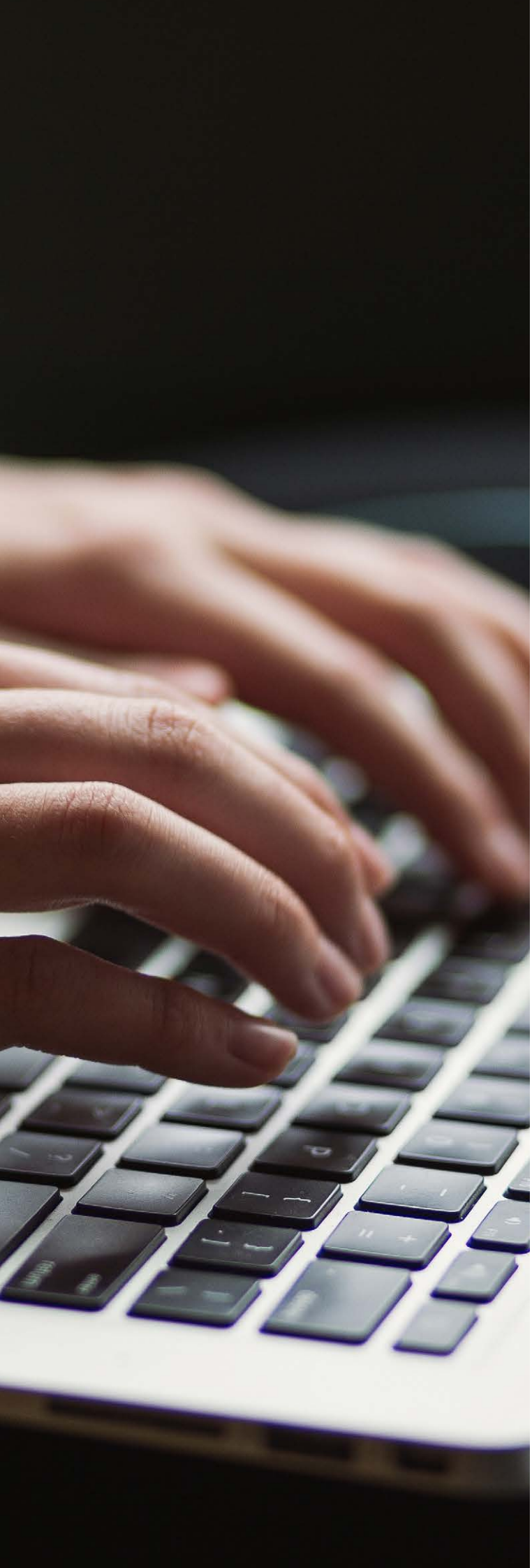
Néanmoins, certaines applications des technologies numériques peuvent poser de graves risques pour les droits humains. Les activités des entreprises de technologie en particulier, telles que les concepteurs de logiciels, les plateformes de réseaux sociaux, les moteurs de recherche et les fournisseurs de services Internet ont été associés à des effets négatifs sur les droits au respect de la vie privée, à la liberté d'expression, à la liberté d'association, à la non-discrimination et même au droit à la vie.[1] Si les périodes de crise ont mis en lumière les avantages des technologies, elles ont aussi souvent révélé leurs risques. Avec la COVID-19, les informations trompeuses sur le virus se sont répandues sur les plateformes en ligne, et des entreprises de technologie au bilan douteux en matière de protection des données et de respect de la vie privée ont proposé des « solutions » aux gouvernements pour surveiller les personnes et les populations.

Les effets en termes de droits humains associés au développement et au déploiement des technologies numériques sont à l'ordre du jour des débats publics depuis près de vingt ans, une attention accrue étant accordée aux activités et aux modèles d'entreprise des « big tech companies », ces entreprises qui dominent le secteur des technologies. Toutefois, les caractéristiques de l'utilisation à grande échelle des technologies numériques posent des défis sans précédent pour la protection et le respect des droits humains :

- les effets se font sentir aux niveaux tantnational, régional que mondial, du fait de l'infrastructure mondialement interconnectée d'Internet, ce qui signifie que les réponses nationales sont souvent inefficaces ou insuffisantes ;

- la portée des effets est large, avec des millions d'utilisateurs (et d'autres individus) qui s'exposent à des risques en termes de droits humains;

- le lien entre les entreprises de technologie et les violations des droits humains n'est pas toujours évident, à cause de la nature hautement spécialisée de leurs activités, et du manque de transparence dans le développement des technologies numériques, telles que la prise de décisions automatisée et l'intelligence artificielle;



©Kaitly Baker

- l'identification des risques pour les droits humains peut être compliquée par le rythme rapide du développement et de l'innovation dans ce domaine;

- certains des problèmes soulevés sont nouveaux et n'ont été abordés que dans une moindre mesure par la jurisprudence internationale et les spécialistes du droit des droits humains. (Il est à noter que récemment l'accent mis sur le lien entre droits humains et secteur des technologies et l'attention qui y a été accordée, notamment par plusieurs Rapporteurs spéciaux des Nations Unies, ont été plus importants).

Le secteur des affaires comprend mieux le lien entre droits humains et technologies numériques et y est davantage sensible. Des affaires très médiatisées, comme l'affaire Cambridge Analytica et les révélations d'Edward Snowden, ont été au centre de l'attention, et ont contribué à un débat politique vif sur les responsabilités en matière de droits humains tant des États que des entreprises à l'ère des big data et des plateformes sociales. Pourtant le secteur des technologies n'est que très peu abordé, voire pas du tout (voir la section 1.3), dans les Plans d'action nationaux sur les entreprises et les droits humains (PAN) existants, malgré le fait que les PAN constituent des occasions primordiales pour les États d'élaborer et exposer les mesures qui seront adoptées pour garantir la protection et le respect des droits humains en lien avec les activités des entreprises de technologie. Plus largement, il est nécessaire de renforcer les synergies entre l'entreprise et les droits humains et les communautés des technologies, comme une étape cruciale vers plus de responsabilité pour les entreprises de technologie, et la conception de cadres réglementaires et

politiques adaptés à l'objectif et conformes aux normes internationales des droits humains.

1.1. À propos de ce supplément thématique

Dans le contexte des défis identifiés en introduction, ce supplément thématique a été conçu comme outil pour assister les acteurs étatiques et les autres parties prenantes dans l'élaboration de PAN, et vise à proposer des conseils concernant l'intégration des risques relatifs au secteur des technologies. Il complète le guide élaboré par l'International Corporate Accountability Roundtable et l'Institut danois des droits de l'homme sur les PAN (le Guide ICAR-IDDH).[2]

Ce supplément thématique vise principalement les pays qui effectuent un processus de lancement, consultation, rédaction, mise en œuvre ou mise à jour de PAN, et les pays qui font usage des technologies numériques élaborées par des entreprises de technologie (pays hôtes), ainsi que ceux dans lesquels des multinationales des technologies ont leur domicile ou leur siège (pays d'origine). Mais il peut également s'avérer utile pour des organisations de la société civile, des entreprises de technologie ou d'autres acteurs impliqués dans le processus de PAN.

Au 1er juin 2020, des PAN avaient été adoptés dans 24 pays, marquant une étape importante vers la diffusion et la mise en œuvre des Principes directeurs relatifs aux entreprises et aux droits de l'homme des Nations Unies (PDNU).[3] Approuvés par le Conseil des droits de l'homme en 2011, les PDNU précisent que les entreprises ont la responsabilité de respecter les droits humains où qu'elles opèrent, indépendamment de la capacité des États de remplir leurs propres obligations en matière de droits humains (principe 11).

Les PDNU réitèrent également le devoir de protection de l'État contre les atteintes causées par des entreprises en adoptant des mesures appropriées pour empêcher ces atteintes, enquêter, punir et réparer par le biais de politiques, de lois, de règles et de procédures judiciaires (principe 1). Les PDNU constituent une solide base normative pour évaluer les effets du secteur des technologies sur les droits humains et élaborer des actions et mesures politiques concrètes pour combler les lacunes en matière de protection. Certains des PAN adoptés font déjà référence aux technologies numériques et au secteur des technologies[4], mais la plupart de ces références sont vagues et n'ont pas le niveau d'ambition requis pour affronter l'ampleur et la portée des effets négatifs du secteur sur les droits humains.

Même si tous les droits humains peuvent être affectés par les technologies numériques développées par les entreprises de technologie, ce supplément thématique se concentre sur trois des droits les plus touchés : les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination. Ce supplément sera mis à jour à l'avenir afin d'inclure d'autres questions en matière de droits humains relatives aux technologies et au secteur des technologies, afin d'en faire un point de convergence pour des organisations qui travaillent au croisement des technologies et des droits humains.

Ce supplément thématique est structuré en trois sections.

Le reste de la **section 1** fournit des informations concernant la portée de ce supplément thématique, et une réflexion sur les références existantes au secteur des technologies dans des PAN.

La **section 2** se penche sur la relation entre le secteur des technologies et les droits humains, en se concentrant sur les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination, avec une vue d'ensemble des effets du secteur des technologies sur ces droits, ainsi que des tendances en matière de réglementation.

La **section 3** commence par examiner comment les considérations relatives au secteur des technologies peuvent être incluses dans le processus de PAN, avec une liste de contrôle des éléments à prendre en considération pour les pays qui souhaitent aborder les effets relatifs au secteur des technologies sur les droits humains dans leurs PAN. La section analyse ensuite comment les considérations relatives au secteur des technologies peuvent être incluses dans le contenu des PAN, et comprend un « Modèle d'évaluation de référence nationale (ERN) pour le secteur des technologies et les PAN » avec des questions indicatives visant à évaluer les protections existantes en matière de droits humains en lien avec le secteur des technologies et à mettre en évidence les lacunes dans la mise en œuvre des PDNU à cet égard. Les deux outils, la liste de contrôle et le modèle d'évaluation de référence nationale, devraient être utilisés conjointement avec le Guide ICAR-IDDH, plus complet, pour élaborer, évaluer et réviser des PAN.

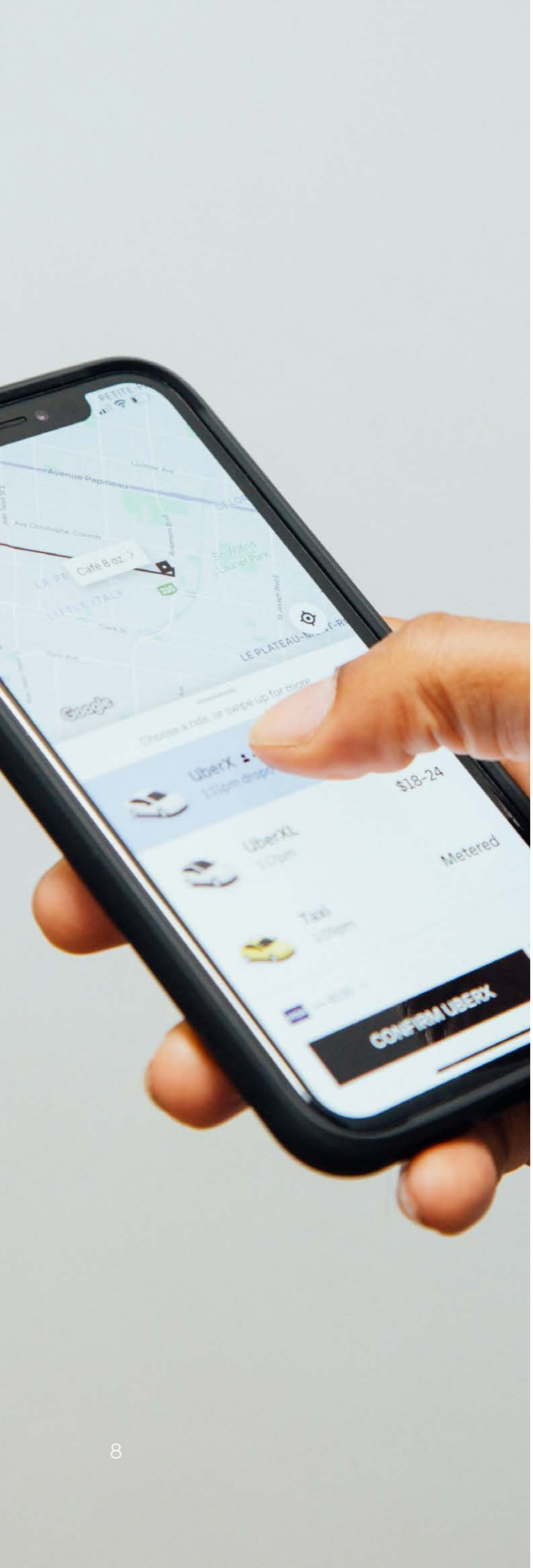
Ce supplément thématique devrait être considéré comme un ensemble minimal d'éléments à prendre en considération pour l'élaboration d'un PAN. Les acteurs étatiques devraient toujours consulter les parties prenantes concernées actives dans le secteur des technologies et/ou qui peuvent être affectées par ce secteur tout au long de l'élaboration et de la mise en œuvre des PAN, afin de garantir qu'il soit aussi efficace que possible.

1.2. Portée de ce supplément thématique

1.2.1. ENTREPRISES VISÉES

La portée de ce supplément thématique est le « secteur des technologies ». Il n'existe pas de définition unique ou généralement acceptée du type d'industries et d'entreprises visées par cette catégorie. Parvenir à une définition claire est compliqué par le fait qu'aujourd'hui presque toutes les entreprises, quel que soit leur secteur, leur taille ou leur emplacement, utilisent Internet et la technologie numérique pour développer et distribuer leurs produits et services. Une entreprise de logistique peut utiliser un logiciel de gestion spécifique, un détaillant peut fournir des biens à travers une plateforme en ligne ou peut commercialiser ses produits en ligne, une institution financière peut utiliser des services d'informatique en nuage pour conserver et gérer de grandes quantités de données.

De plus, la définition du secteur peut être controversée lorsqu'elle a des implications sur l'application de la réglementation. Par exemple, des entreprises « à la tâche » comme Uber et Airbnb ont été contestées pour s'être auto-catégorisées comme des entreprises de gestion de plateforme, ce qui leur permet de se soustraire au respect d'exigences réglementaires plus strictes qui s'appliquent aux entreprises traditionnelles de transport et d'hôtellerie-restauration. Plusieurs tribunaux à travers le monde ont examiné des affaires afin de déterminer si Uber est un service numérique ou simplement une entreprise traditionnelle qui emploie les technologies numériques[5]. Dans un arrêt de 2017 qui a fait date, la Cour de justice européenne a estimé que Uber est une entreprise de transport, et non un service de la société de l'information, et qu'elle est donc sujette aux règles en matière de licences pour les taxis.



©Charles Deluvio

Dans ce contexte dynamique, ce rapport ne propose pas de définition spécifique du « secteur des technologies », mais note que, au sens le plus large, on peut considérer qu'il comprend l'ensemble des entreprises dont le modèle d'affaires permet l'accès à Internet et aux technologies numériques ainsi que leur fonctionnement, y compris le développement et la distribution de produits, services et contenus numériques. Cette large définition signifierait que le secteur des technologies inclut les entreprises de télécommunication, les fournisseurs de service Internet, les entreprises de gestion des noms de domaine telles que registres et bureaux d'enregistrement, les sociétés fournissant du contenu sur Internet, la communication et les services tels que moteurs de recherche, plateformes de réseaux sociaux, applications de messagerie, et les entreprises de matériel informatique et de logiciels, y compris les fournisseurs d'équipement de réseau.

Étant donné que ce supplément thématique met spécifiquement l'accent sur des droits humains, à savoir les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination (voir la section 1.2.2), le rapport se concentre principalement (également à l'aide d'exemples) sur les domaines et les entreprises au sujet desquels ces problèmes relatifs aux droits humains ont été largement attestés et sont particulièrement importants.

Malgré cet examen ciblé, bon nombre des éléments de ce supplément thématique, en particulier les aspects relatifs à la confidentialité et à la protection des données, s'appliqueront également à de nombreuses autres entreprises qui utilisent la technologie numérique d'une manière ou d'une autre, et par conséquent les effets d'un PAN élaboré conformément à ces indications auront une portée plus large.

L'APPROCHE DU SUSTAINABILITY ACCOUNTING STANDARDS BOARD POUR DÉFINIR LE SECTEUR DES TECHNOLOGIES

Le Sustainability Accounting Standards Board (SASB) est un organisme indépendant de normalisation dans le domaine des normes comptables pour la durabilité. Le SASB identifie cinq domaines du secteur des technologies et de la communication : les services de fabrication d'équipement électronique et la création de modèles originaux, le matériel informatique, les médias et services Internet, les semi-conducteurs, les logiciels et services des technologies de l'information, et les télécommunications. Au vu de l'intégration et de la convergence accrues au sein de ce secteur, une entreprise peut appartenir en même temps à plus d'un de ces domaines. Par exemple, une entreprise comme Google, qui opère dans plusieurs segments commerciaux, est à la fois un moteur de recherche, un concepteur de logiciels et une entreprise d'infrastructure Internet.

EFFETS SUR LES DROITS HUMAINS AU-DELÀ DU SECTEUR DES TECHNOLOGIES

Bien que ce supplément thématique mette l'accent sur les effets des entreprises de technologie sur les droits humains, toute entreprise qui utilise, déploie ou dépend des technologies numériques peut, ce faisant, avoir des effets néfastes sur les droits humains des individus.

Un exemple est l'utilisation des technologies de surveillance par des entreprises afin de contrôler leurs employés au travail, ce qui peut constituer une violation du droit au respect de la vie privée. Une enquête menée en 2018 par Gartner a constaté que près d'un quart des organisations à travers le monde utilisent des données concernant les mouvements des employés, et 17 % font un suivi des données d'utilisation des ordinateurs professionnels. Certaines entreprises font un suivi de l'utilisation des réseaux sociaux par leurs employés même lorsqu'ils ne travaillent pas, et des employés ont été licenciés pour avoir exprimé leur avis sur les réseaux sociaux.

L'augmentation du télétravail due à la COVID-19 a poussé certains employeurs à utiliser de nouveaux outils numériques pour surveiller leur personnel à distance, notamment les sites web qu'ils consultent. Des produits numériques tels que Sneek, qui prend des photos au moyen des appareils photo des ordinateurs portables toutes les quelques minutes, sont utilisés par certains employeurs afin de vérifier que leurs employés utilisent leurs ordinateurs portables pendant les heures de travail.

Un autre exemple est l'utilisation accrue de l'intelligence artificielle par un grand nombre de secteurs différents, tels que le secteur des services financiers, afin de prendre des décisions au sujet de l'éligibilité d'une personne à un prêt, ou de définir le taux d'intérêt. Des preuves solides attestent l'utilisation de la prise de décisions automatisée dans des cas ayant abouti à une discrimination, notamment fondée sur la race et l'appartenance ethnique.

1.2.2. DROITS HUMAINS VISÉS

La première édition de ce supplément thématique se concentre sur trois des droits humains qui ont été les plus fréquemment examinés sous l'angle des effets du secteur des technologies : les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination. Tel qu'indiqué précédemment, ce supplément thématique sera mis à jour afin d'inclure d'autres questions des droits humains relatives au secteur des technologies, en vue d'en faire une ressource plus complète.

Les droits au respect de la vie privée et à la liberté d'expression sont particulièrement importants, puisqu'ils sont souvent considérés comme des droits permettant la jouissance d'autres droits humains. Par exemple, le droit au respect de la vie privée peut permettre le développement libre de la personnalité et de l'identité d'un individu, et sa capacité à participer à la vie politique, économique, sociale et culturelle[6]. En jouissant de l'anonymat qu'offrent certaines plateformes en ligne, ou des outils de cryptage qui garantissent la confidentialité, les personnes peuvent se sentir plus libres de discuter de questions personnelles ou sensibles, et de débattre de questions controversées lorsque parler ouvertement pourrait susciter harcèlement et violence.

La jouissance de la liberté d'expression, qui comprend la capacité de transmettre, demander et recevoir des informations, est un moteur pour la réalisation de droits associés tels que les droits à la liberté d'association et de réunion pacifique, le droit de prendre part à la direction des affaires publiques, le droit à l'éducation, le droit de participer à la vie culturelle, et le droit de jouir des avantages du progrès scientifique et de ses applications. Par exemple, c'est souvent à travers des plateformes en ligne que les personnes ont pu non seulement communiquer, mais aussi organiser des manifestations ou d'autres mouvements de masse. Différentes plateformes et outils de formation en ligne sont désormais accessibles à ceux dont les possibilités de recourir à des formes d'éducation plus traditionnelles sont limitées.

La non-discrimination constitue un principe essentiel et fondamental relatif à la protection de tous les droits humains[7]. Le droit international des droits humains reconnaît que le respect et la garantie des droits humains doivent être assurés sans discrimination. Les PDNU soulignent également qu'ils devraient être mis en œuvre de manière non-discriminatoire et, dans le commentaire au principe 3, indiquent que l'incapacité à faire appliquer les lois existantes portant sur la non-discrimination qui régissent directement ou indirectement le respect des droits humains par les entreprises constitue souvent une importante lacune juridique dans la pratique des États.

Le caractère interdépendant de tous les droits humains va par ailleurs dans les deux sens, ainsi des effets négatifs sur les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination peuvent également restreindre d'autres droits humains.

LES DROITS AU RESPECT DE LA VIE PRIVÉE, À LA LIBERTÉ D'EXPRESSION ET À L'ÉGALITÉ/À LA NON-DISCRIMINATION

Le **droit au respect de la vie privée** est reconnu de longue date par le droit international des droits humains. S'inspirant du libellé de l'article 12 de la Déclaration universelle des droits de l'homme (DUDH), le Pacte international relatif aux droits civils et politiques (PIDCP) stipule dans son article 17 que « Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation ». Il précise en outre que « Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes ».

Le **droit à la liberté d'expression** peut être défini au sens large comme le droit d'un individu d'être libre d'exprimer des opinions sans être inquiété et de rechercher, recevoir et répandre des informations et des idées par quelque moyen que ce soit, indépendamment des frontières. L'article 19(2) du PIDCP, qui reprend en grande partie le libellé de l'article 19 de la DUDH, stipule que « Toute personne a droit à la liberté d'expression ; ce droit comprend la liberté de rechercher, de recevoir et de répandre des informations et des idées de toute espèce, sans considération de frontières, sous une forme orale, écrite, imprimée ou artistique, ou par tout autre moyen de son choix ».

Le droit à la liberté d'expression est étroitement lié au droit à la liberté d'opinion. L'article 19(1) du PIDCP (qui reprend là encore le libellé de l'article 19 de la DUDH), dispose que « Nul ne peut être inquiété pour ses opinions ».

Alors que le droit à la liberté d'opinion est un droit absolu (c'est-à-dire qu'aucune ingérence dans ce droit ne peut être justifiée), il n'en est pas de même pour les droits au respect de la vie privée et à la liberté d'expression, qui sont tous deux des droits non-absolus. Néanmoins, des limitations ou restrictions peuvent être imposées uniquement dans certains circonstances, lorsque :

- il existe une base juridique claire ;
- elles poursuivent un objectif légitime ; et
- elles constituent une réponse nécessaire et proportionnée à cet objectif.

Les **droits à l'égalité et à la non-discrimination** sont également reconnus de longue date dans le droit international des droits humains. En effet, le droit à la non-discrimination sous-tend le droit international des droits humains, l'article 2(1) du PIDCP exigeant que les droits reconnus par le Pacte soient respectés « sans distinction aucune », interdisant ainsi la discrimination dans la jouissance de tous les droits humains (et reflétant, en partie, les articles 2 et 7 de la DUDH). Toutefois, l'article 26 consacre un droit à l'égalité à part entière, en s'appuyant sur l'article 7 de la DUDH, en stipulant que :

- toutes les personnes sont égales devant la loi ;
- toutes les personnes ont droit sans discrimination à une égale protection de la loi ; et
- les États doivent veiller à ce que la loi interdise toute discrimination et garantisse à toutes les personnes une protection égale et efficace contre toute discrimination, quel qu'en soit le motif.

Le Comité des droits de l'homme des Nations Unies note que l'article 26 du PIDCP « interdit toute discrimination en droit ou en fait dans tout domaine » et ne se limite donc pas aux droits consacrés dans le Pacte. Le Comité des droits de l'homme a également noté qu'afin de remplir leurs obligations en matière de non-discrimination, les États doivent adopter une législation globale de lutte contre la discrimination. Ainsi, lorsque les États ont dûment réalisé le droit à la non-discrimination, les entreprises du secteur des technologies (et plus généralement le secteur privé) auront des obligations contraignantes de non-discrimination, quel que soit le domaine d'activité.

Comme pour les droits au respect de la vie privée et à la liberté d'expression, les droits à l'égalité et à la non-discrimination ne sont pas des droits absolus. Un traitement différencié ne sera toutefois admissible que si les critères de différenciation sont raisonnables et objectifs et si le but est la poursuite d'un objectif légitime.

1.3. Réflexions sur les effets de la technologie dans les PAN existants

Au 1er juin 2020, des PAN avaient été adoptés dans 24 pays[8]. Dix de ces PAN font référence au secteur des technologies. Parmi eux, cinq contiennent des actions et des engagements spécifiques relatifs au secteur des technologies. Les cinq autres se limitent à noter qu'il existe des effets sur les droits humains relatifs au secteur des technologies. Le texte des dix PAN qui mentionnent le secteur des technologies est reproduit dans l'annexe 1 de ce supplément thématique, avec les détails de la mise en œuvre des actions, lorsqu'ils sont disponibles et pertinents.

En résumé, les mesures des cinq PAN qui prennent des engagements relatifs au secteur des technologies sont diverses : une porte sur une table ronde consacrée à la protection des données (Finlande), l'une sur la réglementation de la responsabilité des intermédiaires (Pologne), l'une sur des orientations concernant l'exportation des technologies de l'information et de la communication (Royaume-Uni), l'une sur un mécanisme pour aider à identifier les enseignements tirés et les meilleures pratiques relatifs aux entreprises qui promeuvent les droits humains en ligne (États-Unis), et l'une sur l'élaboration de plans et de mesures pour aider les travailleurs remplacés par la technologie (Thaïlande). Dans l'un de ces cas seulement (le Royaume-Uni), l'État a fourni des détails sur la façon dont l'engagement a été mis en œuvre[9].

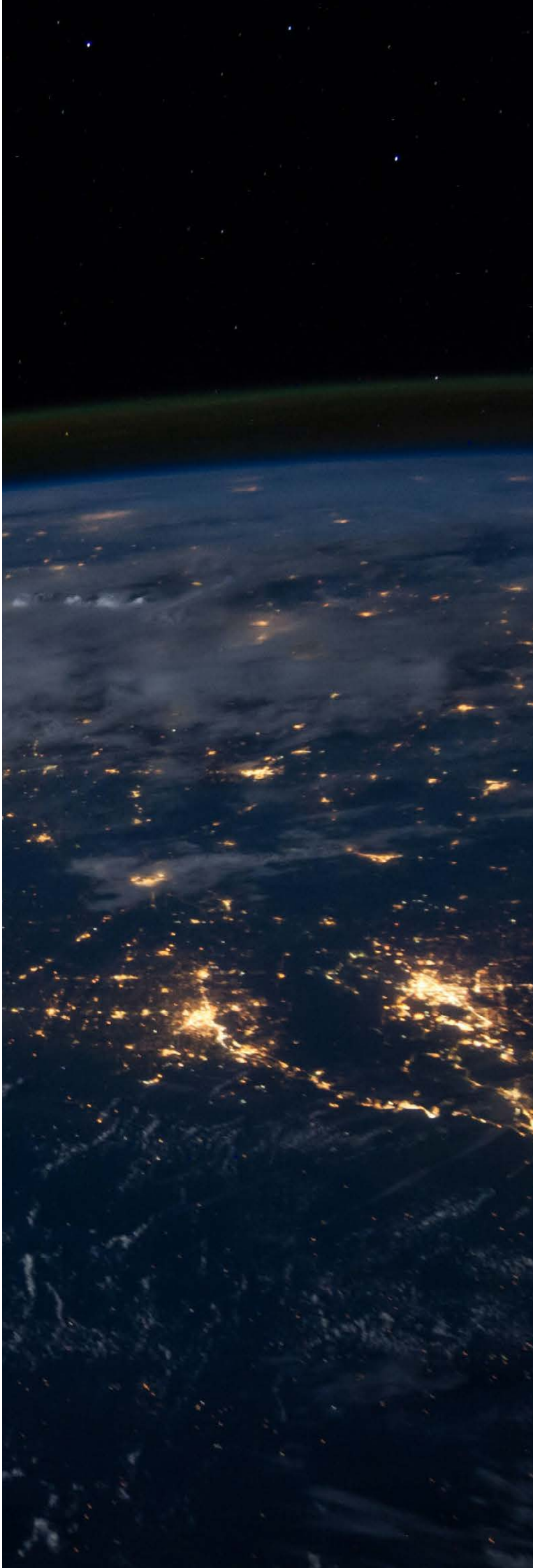
Trois observations peuvent être proposées concernant la formulation et les engagements dans les PAN existants.

1. Le vaste éventail des risques pour les droits humains, en particulier pour les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination, qui résultent des activités du secteur des technologies, ne sont pleinement pris en compte dans aucun PAN publié à ce jour. Les PAN qui se penchent sur le secteur des technologies tendent à examiner uniquement un aspect limité des risques pour les droits humains posés par le secteur, tel

que la confidentialité (Finlande), la liberté d'expression (Pologne) ou le droit de travailler (Thaïlande). Le droit à la non-discrimination est examiné principalement en lien avec l'emploi, et les effets discriminatoires larges de l'utilisation des nouvelles technologies numériques ne sont pas abordés. Bien que cela reflète peut-être l'état des priorités des questions les plus pressantes dans le PAN, cela peut également représenter l'échec de la pleine prise en compte du vaste éventail des effets sur les droits humains qui résultent du secteur des technologies.

2. Aucun des engagements pris dans les quatre PAN contenant des engagements relatifs au secteur des technologies ne peut être considéré comme pleinement SMART (spécifique, mesurable, acceptable, réaliste, et situé dans le temps)[10]. Aucun des cinq PAN ne fournit de détails sur les échéances fixées pour la réalisation de l'engagement ou le financement à octroyer. Aucun des quatre ne fournit de détails sur la façon dont les résultats seraient publiés et leur effet surveillé.

3. Aucun des engagements des PAN relatifs au secteur des technologies n'aborde le troisième axe des PDNU, qui se concentre sur l'accès à des voies de recours. Ces cinq PAN mettent l'accent sur le premier axe (la réglementation de la responsabilité des intermédiaires) et le deuxième axe (indications concernant la prise en compte des droits humains pour l'exportation de produits technologiques, et le partage de bonnes pratiques des politiques d'entreprise qui promeuvent les droits humains en ligne).



© Nasa - Unsplash

2. Le secteur des technologies et les effets sur les droits humains

Tel qu'indiqué à la section 1, les entreprises de technologie, et les produits et services numériques qu'elles élaborent et distribuent, offrent de nombreuses possibilités d'appuyer la réalisation et la jouissance des droits humains. Le développement de produits de cryptage puissants aide à protéger le droit au respect de la vie privée, en préservant la sécurité des données personnelles et des communications des individus. Cela est particulièrement important pour les groupes exposés au risque de traitement discriminatoire par l'État ou des acteurs privés. Les plateformes de réseaux sociaux ont offert de nouvelles possibilités à des milliards de personnes à travers le monde, notamment aux groupes marginalisés, de faire entendre leurs voix, facilitant plus que jamais la communication, et le partage d'informations et d'idées, en renforçant la jouissance, sur un pied d'égalité, de leur droit à la liberté d'expression. Et, tel qu'indiqué à la section 1.2.2., les droits au respect de la vie privée et à la liberté d'expression sont les « garants » de la jouissance sur un pied d'égalité d'autres droits qui y sont associés. Ces produits et services ont également des avantages plus larges pour les droits humains, ils permettent aux victimes de violations des droits humains de mieux révéler les violations, et de sensibiliser à ces violations, ainsi que d'exercer[11] un droit de recours et obtenir réparation.

Néanmoins, les produits et services de ces entreprises peuvent également poser des risques pour les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination. Un PAN qui tient compte du secteur des technologies peut contribuer à éviter ou atténuer ces risques.

2.1. Le droit au respect de la vie privée (y compris les effets discriminatoires)

Le modèle d'affaires de nombreuses entreprises de technologie repose sur la collecte et le traitement de grandes quantités de données personnelles au sujet du comportement en ligne et hors ligne des individus. Ces données sont fréquemment utilisées pour créer des profils hautement sophistiqués, qui couvrent de nombreux aspects personnels et sensibles de l'identité d'une personne. Bien que souvent utilisées à des fins commerciales, comme pour la publicité micro-ciblée (une pratique qui, en soit, a soulevé des préoccupations concernant le respect de la vie privée, la liberté d'expression et l'égalité/la non-discrimination)[12], elles ont également été utilisées par les entreprises elles-mêmes pour suivre et surveiller des individus, et parfois fournies ou détournées par des acteurs étatiques, tels que les organes chargés de l'application des lois. Avec l'avènement de nouvelles technologies telles que la 5G, l'internet des objets et l'intelligence artificielle (IA), la quantité de données collectées ne fera qu'augmenter, et par conséquent également la prévalence de ces utilisations des données.

Ce type de modèle d'entreprise est de plus en plus passé au crible à cause de ses effets négatifs effectifs et potentiels sur les droits au respect de la vie privée et à l'égalité/à la non-discrimination. Les données personnelles (y compris les

métadonnées), qu'elles soient collectées et partagées avec ou sans le consentement des personnes concernées, ne sont pas uniquement utilisées seules, mais elles sont aussi partagées et corrélées avec d'autres sources de données afin de créer des profils personnels et de groupe encore plus détaillés. La consolidation des différents points de données dans des ensembles de données, même s'ils sont apparemment anonymisés, soulève des questions fondamentales au sujet des droits des utilisateurs de savoir, de donner leur consentement et d'exercer un contrôle sur leurs données à caractère personnel, en conformité avec leur droit au respect de la vie privée. Et alors que la technologie devient plus puissante, il devient plus aisé de recueillir et de traiter des « big data », c'est-à-dire des ensembles de données extrêmement volumineux. Selon le Rapporteur spécial des Nations Unies sur le droit à la vie privée « La tendance des mégadonnées à s'immiscer dans la vie des individus en révélant les moindres détails de leur soi virtuel à ceux qui collectent et analysent leurs données heurte de plein fouet le droit au respect de la vie privée et les principes consacrés pour protéger ce droit »[13].

Le Rapporteur spécial a également souligné la reconnaissance du droit au respect de la vie privée dans les instruments internationaux comme « un droit étroitement lié aux notions de dignité humaine et de libre et plein développement de la personnalité »[14]. La capacité de préserver des contextes distincts dans lesquels une personne divulgue ou cache son identité sans surveillance des données peut être cruciale pour des groupes exposés à des risques de discrimination ; par exemple, elle peut s'avérer essentielle pour des personnes LGBTI qui vivent dans un pays où les pratiques intimes entre personnes du même sexe sont stigmatisées ou illégales[15].

© Ev - Unsplash

Les ensembles de données sont analysés de plus en plus fréquemment par des algorithmes et d'autres formes d'IA, des nouvelles technologies qui deviennent rapidement partie intégrante de l'infrastructure essentielle de nos sociétés. Néanmoins, nous commençons seulement à comprendre les effets sur les droits humains de l'IA, des mégadonnées, et des technologies associées[16]. Ces technologies peuvent engendrer différentes discriminations[17], y compris le fait d'être entraînées sur des données biaisées ou des échantillons biaisés, et donc de reproduire des schémas de discrimination existants[18].

À titre d'exemple, en 2018 Reuters faisait état du fait qu'Amazon avait cessé d'utiliser un système d'IA pour sélectionner des candidats à un poste de travail parce que le système avait un préjugé contre les femmes : selon le rapport, « l'entreprise a réalisé que son nouveau système n'évaluait pas les candidats pour les postes de concepteurs de logiciels et d'autres postes techniques sans distinction de sexe »[19]. Sur la base des données traitées, « le système d'Amazon avait appris par lui-même que les candidats de sexe masculin étaient préférables »[20].

L'achat et la vente de données par des « courtiers en données » à des fins commerciales, comme la publicité, l'évaluation du risque de crédit et l'analyse des risques d'assurance sont liés à un manque de transparence, à la rétention des données de manière indéfinie, et à des résultats discriminatoires par des algorithmes[21]. Une étude de ProPublica de 2017 a révélé que les publicitaires de Facebook pouvaient exclure certains groupes des annonces d'offres de logements en location, notamment les afro-américains, les personnes intéressées par des rampes pour fauteuil roulant, et les hispanophones, malgré le fait que l'entreprise avait annoncé avoir bâti un système permettant de détecter et éliminer les annonces discriminatoires[22].

Aux États-Unis, les systèmes de justice pénale de certaines régions utilisent un système appelé COMPAS (Correctional Offender Management Profiling for Alternative Sanctions - Profilage pour la gestion des criminels à des fins de sanctions alternatives) afin d'aider les juges à déterminer si une personne condamnée pour une infraction pénale devrait être autorisée à être surveillée hors de prison plutôt qu'incarcérée. Des recherches menées par des journalistes d'investigation en 2016 ont montré que COMPAS intégrait un préjugé fondé sur la race : les personnes noires étaient au moins deux fois plus susceptibles que les personnes blanches d'être catégorisées comme à haut risque, sans toutefois commettre un autre délit par la suite, et les personnes blanches étaient beaucoup plus susceptibles d'être catégorisées comme représentant un risque faible, alors qu'elles commettaient par la suite d'autres délits[23].

La récolte massive et opaque de grandes quantités de renseignements, y compris des données personnelles, peut également poser des risques de violations des données, d'utilisation inappropriée de ces données et de discrimination. Le scandale Cambridge Analytica a révélé que Facebook autorisait la récolte de données de 87 millions d'utilisateurs, qui furent ensuite utilisées pour tenter d'influencer le résultat de la campagne présidentielle de 2016 aux États-Unis[24]. La violation des données de Yahoo en 2013 a affecté les trois milliards de comptes d'utilisateurs de Yahoo, mettant en péril les données à caractère personnel de millions de ses utilisateurs, des rapports ayant fait état de l'utilisation des données volées par des gouvernements afin de cibler des individus[25].

Les entreprises de technologie, y compris les fournisseurs de service Internet et les points d'échange Internet, sont désormais soumises à des pressions significatives afin qu'elles partagent des données

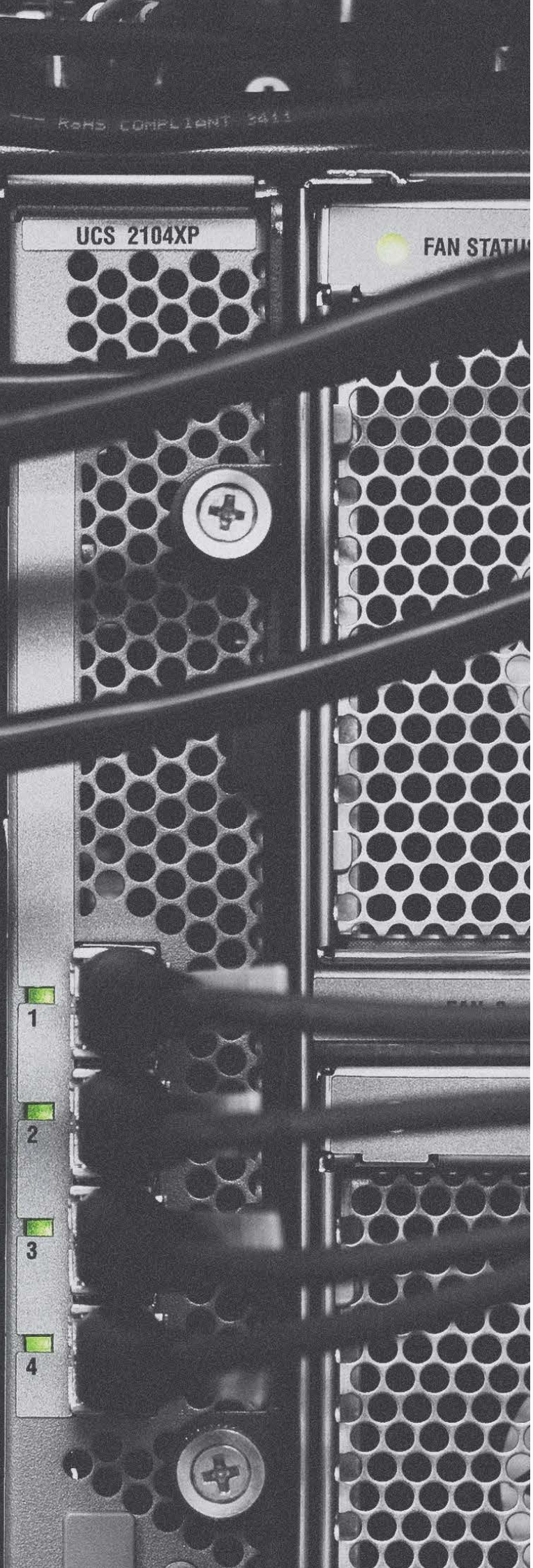
personnelles avec des organismes chargés de la sécurité nationale qui mènent des activités de surveillance numérique, avec des effets néfastes sur les droits au respect de la vie privée, à l'égalité/à la non-discrimination et d'autres droits humains. Par exemple, le programme de surveillance PRISM des États-Unis, mis en lumière suite aux révélations Snowden de 2013, a été critiqué pour avoir accumulé de grandes quantités de données sur des Américains qui n'étaient ni des cibles d'espions ni ne représentaient de menace pour la sécurité. De plus, les données recueillies de la sorte ont été utilisées pour identifier des suspects et enquêter sur leur compte en violation du droit à un procès équitable[26]. Plusieurs procédures en justice contre ces entreprises de technologie sont actuellement en cours dans différentes juridictions pour leur rôle dans la facilitation des violations des droits humains commises par des États suite à la collecte de données par des techniques de surveillance numérique[27]. Les groupes exposés au risque de discrimination sont particulièrement vulnérables au partage de grandes séries de données à des fins de surveillance étatique. Par exemple, les mégadonnées ont alimenté la répression de l'État chinois contre les Ouïghours et d'autres minorités ethniques dans la région de Xinjiang[28].

Cadres et initiatives

Le rapport « Freedom on the Net » de 2018 de Freedom House indiquait que, depuis juin 2017, les gouvernements de 18 États sur 65 avaient révisé ou promulgué de nouvelles lois ou directives visant à accroître la surveillance étatique en ligne[29]. Certains États ont exigé des entreprises de technologie qu'elles stockent les données de leurs citoyens sur des serveurs locaux, avec l'objectif de rendre les registres plus accessibles aux organismes nationaux en charge de la sécurité ou de les protéger contre le vol ou l'exploitation[30]. Dans ce contexte, les Principes internationaux sur l'application des droits humains à la surveillance des communications ont été élaborés par un groupe multipartite afin de préciser comment le droit international des droits humains s'applique aux technologies et techniques actuelles de surveillance des communications[31]. Les entreprises de technologie ont progressivement uni leurs forces pour repousser les demandes des gouvernements de collecter des données concernant leurs utilisateurs. Par l'intermédiaire de la Coalition pour la réforme de la surveillance des gouvernements, des entreprises comme Google, Apple, Facebook, Dropbox, Twitter et LinkedIn ont demandé la réforme des lois et pratiques sur la surveillance gouvernementale et l'accès aux informations par des gouvernements à travers le monde[32].

Certains États ont soulevé des préoccupations concernant les défis que des outils et produits de cryptage sophistiqués développés par des entreprises de technologie pour protéger la sécurité des utilisateurs en ligne posent pour l'application de la loi. En 2018 par exemple, les États appartenant à Five Eyes, une alliance du renseignement constituée par le Royaume-Uni, les États-Unis, le Canada, l'Australie et la Nouvelle-Zélande, ont publié une déclaration conjointe appelant les entreprises de technologie à « établir sur une base volontaire des solutions d'accès licites » au contenu crypté[33].

La prolifération des risques numériques pour la sécurité et la protection des données a mis en évidence les défauts de bon nombre des cadres de protection des données. Globalement, la plupart des lois en matière de protection et de confidentialité des données tiennent compte des principes relatifs à la protection des données énoncés dans les Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel adoptées en 1980 (et mises à jour en 2013) et la Convention du Conseil de l'Europe pour la protection



© Kvistholt

des personnes à l'égard du traitement automatisé des données à caractère personnel adoptée en 1981 (Traité n° 108). En conséquence, de nombreux États révisent ou adoptent de nouvelles lois en matière de protection des données et de confidentialité.

Alors que plus de 100 pays ont adopté une législation, sous l'une ou l'autre forme, en matière de protection des données, le Règlement général sur la protection des données de l'UE (RGPD) est le règlement ayant la portée la plus large adopté à ce jour (voir l'encadré 4). Salué pour le potentiel qu'il renferme de consolider la protection des données et le droit au respect de la vie privée, le RGPD s'inscrit dans un ensemble réglementaire plus large développé par l'UE qui inclut le Règlement sur la cybersécurité et la révision de la Directive relative à la vie privée et aux communications électroniques[34]. Cela inclut également une directive sur la police portant sur le traitement des données personnelles par les autorités chargées de prévenir, enquêter, détecter et poursuivre les délits[35].

Selon le Comité européen de la protection des données, plus de 89 000 violations de données ont été enregistrées par les autorités nationales de supervision lors de la première année ayant suivi l'entrée en vigueur du RGPD en mai 2018[36]. Une amende record de 50 millions d'euros a été infligée à Google par l'organisme national français de protection des données pour avoir violé la nouvelle loi[37].

Le RGPD a alimenté des lois similaires dans d'autres juridictions, notamment la loi californienne sur la protection de la vie privée des consommateurs (Californian Consumer Privacy Act) et des lois en matière de protection des données en Argentine, au Brésil et en Indonésie. Tel que noté au début de cette section, des nouvelles technologies telles que la 5G, l'internet des objets et l'IA ne feront

qu'accélérer la portée et l'ampleur de la collecte des données et rendront encore plus floue la distinction entre données à caractère personnel et non-personnel. Afin de se maintenir à l'avant-garde de l'innovation numérique, les organismes de régulation et les décideurs politiques examinent de plus en plus des solutions qui couvrent des domaines réglementaires autrefois distincts, tels que la protection du consommateur, les règles en matière de concurrence, et la protection des données.

RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES DE L'UE (RÈGLEMENT (UE) 2016/679)

Le Règlement général sur la protection des données (RGPD) est entré en vigueur en mai 2018 et s'applique à tous les individus, organisations et entreprises qui collectent, stockent et traitent des données à caractère personnel concernant des individus dans l'UE. Les données personnelles sont définies comme toute information concernant une personne physique identifiée ou identifiable. Les données personnelles sont protégées quelle que soit la technologie employée pour leur traitement ou conservation, que le traitement soit automatisé ou manuel. Le RGPD exige des entreprises qu'elles obtiennent le consentement explicite des personnes (« personnes concernées ») au sujet desquelles elles détiennent des données et rédigent une politique en matière de protection de la vie privée « sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples ». Chose importante, afin de se conformer aux dispositions du RGPD, le consentement ne devrait pas être caché dans les conditions, et lorsque le traitement est effectué à différentes fins, le consentement doit être obtenu pour toutes ces fins.

Le RGPD crée également plus de transparence en exigeant des entreprises qu'elles informent les utilisateurs si des données sont transférées hors de l'UE, si les données recueillies sont utilisées pour une fin différente de celle prévue initialement, et si les décisions prises à l'aide de leurs données sont automatisées, notamment en leur donnant la possibilité de le contester. Il accorde aux personnes des droits plus solides d'accès aux données les concernant, de notification rapide en cas de violation, et un « droit à l'oubli » (un droit à la suppression des données personnelles).

Le RGPD créé également des mécanismes de mise en œuvre plus solides en accordant aux autorités nationales de protection des données le pouvoir de condamner à une amende une entreprise pour un montant allant jusqu'à 4 % de son chiffre d'affaires mondial en cas de violations, et en favorisant leur coopération à travers le Comité européen de la protection des données, avec le pouvoir de fournir des indications et une interprétation et d'adopter des décisions contraignantes dans les cas présentant une dimension transfrontalière.

Le RGPD introduit également quelques dispositions nouvelles, telles qu'une exigence d'une analyse des effets de la protection des données dans des situations susceptibles d'engendrer un risque élevé pour les droits et les libertés des personnes, ainsi que des droits à la portabilité des données et à ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, qui produit des effets juridiques ou d'autres effets significatifs qui les concernent.

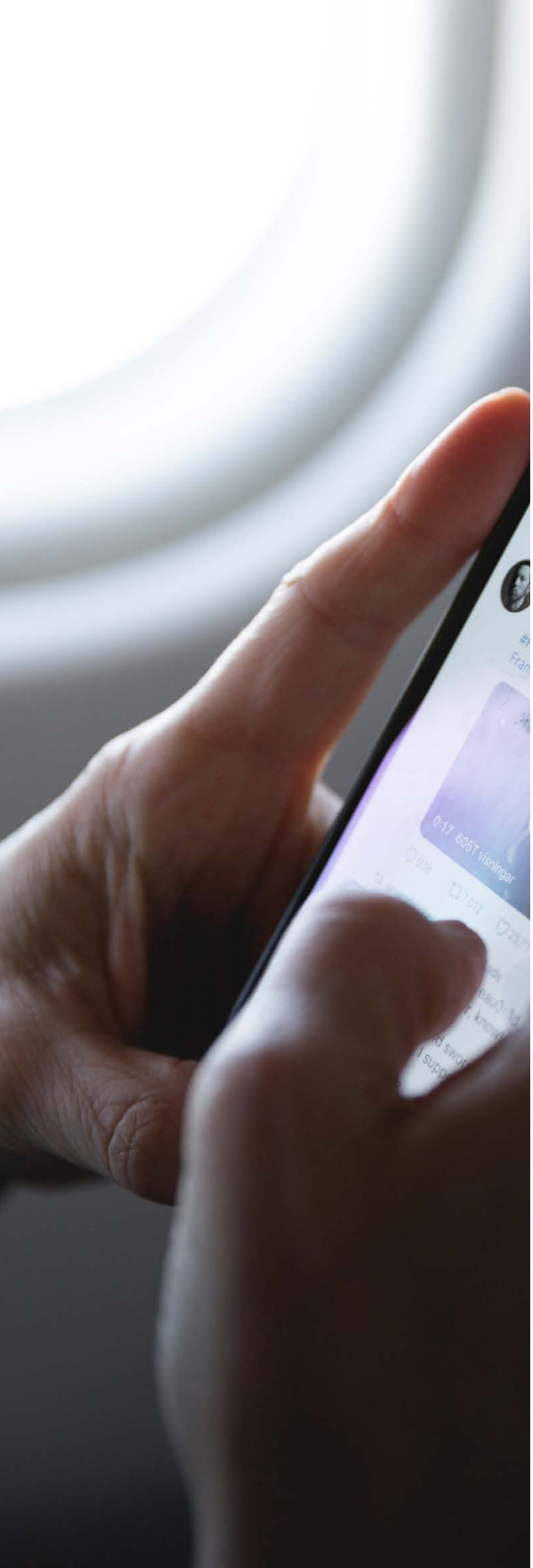
Bien que les lois et politiques en matière de protection des données contribuent dans une certaine mesure à atténuer les effets néfastes sur les droits humains des nouvelles technologies, y compris l'IA et les mégadonnées, bon nombre de ces technologies sont de plus en plus utilisées dans des pays qui n'ont pas encore adopté de lois générales de lutte contre la discrimination, ce qui signifie que le cadre juridique pour empêcher une application discriminatoire est inadéquat.[38]

En réponse aux préoccupations concernant spécifiquement les risques de discrimination, la Déclaration de Toronto : protéger le droit à l'égalité et à la non-discrimination dans les systèmes reposant sur l'apprentissage automatique a été promulguée par un groupe d'organisations non-gouvernementales en 2018. La Déclaration de Toronto appelle les gouvernements et les entreprises à s'assurer que les applications d'apprentissage automatique respectent les principes d'égalité et de non-discrimination[39].

2.2. Le droit à la liberté d'expression (y compris les effets discriminatoires)

Bien que les plateformes de réseaux sociaux, les services de messagerie et les moteurs de recherche offrent de nouveaux espaces pour que les personnes exercent leur droit à la liberté d'expression, ces espaces, et donc ce que les personnes peuvent dire et faire en ligne, sont régis presque entièrement par un petit nombre d'entreprises de technologie. Les politiques de modération des contenus dictent ce qui peut et ne peut pas être vu, dit et fait sur ces plateformes, et ces décisions reposent de plus en plus sur des algorithmes et l'IA, également employés pour sélectionner les informations que les personnes voient en ligne. Dans son rapport de 2018 à l'Assemblée générale des Nations Unies, le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression a mis en évidence comment l'utilisation d'algorithmes et de l'IA pour filtrer et personnaliser le contenu auquel les personnes peuvent accéder en ligne sape la capacité des titulaires de droits à se forger des opinions indépendantes en faisant appel à des idées diverses qui transcendent les divisions idéologiques et politiques[40].

Des préoccupations en matière de liberté d'expression ont été évoquées au sujet des lois et des projets de loi élaborés par des gouvernements et des instances réglementaires afin de s'attaquer à certaines formes de contenu, d'expression et de comportement en ligne. Cette tendance réglementaire s'est développée suite à l'accumulation croissante de



© Marten Bjork

preuves de l'utilisation de plateformes en ligne pour diffuser de la désinformation et de la propagande politique[41], la violence et des abus à l'égard des femmes[42], et la haine et l'incitation à la violence contre des groupes minoritaires[43]. Des incidents violents tels que les attaques de Christchurch en 2019 en Nouvelle-Zélande, le nombre croissant d'attaques perpétrées par des suprémacistes blancs à travers le monde et la campagne de nettoyage ethnique contre la minorité musulmane Rohingya au Myanmar[44], ont mis en lumière un continuum déconcertant entre la prolifération en ligne de contenu haineux et la perpétration de la violence hors ligne.

Un autre risque fondamental pour la liberté d'expression en ligne découle des différentes restrictions d'accès à Internet, et aux plateformes qui utilisent Internet, imposées par des gouvernements qui cherchent à contrôler les flux d'information. Rien qu'en 2018, 196 interruptions d'Internet ont empêché l'accès des utilisateurs aux informations dans 25 pays, un chiffre qui est passé à 213 interruptions dans 33 pays en 2019[45]. Les groupes exposés au risque de discrimination sont particulièrement vulnérables à ces restrictions d'accès arbitraires, qui constituent souvent des mesures illégales prises par des gouvernements pour faire taire les voix dissidentes[46]. Des coupures à grande échelle ont fréquemment lieu dans des régions où un groupe ethno-linguistique ou religieux constitue une part importante de la population[47]. Des recherches récentes identifient la discrimination numérique dans l'accès aux technologies de la communication comme une tendance mondiale qui affecte fortement les groupes ethniques laissés pour compte.[48]

Le Conseil des droits de l'homme des Nations Unies a condamné les mesures visant à empêcher ou perturber intentionnellement l'accès aux

informations en ligne ou leur diffusion, en violation du droit international des droits humains, et a appelé tous les États à s'abstenir d'adopter de telles mesures et à les éliminer[49]. Ces interruptions d'Internet et d'autres techniques visant à contrôler l'accès au monde numérique sont tributaires de l'implication des entreprises, tant par des moyens coercitifs que par des moyens non-coercitifs, qui font fonctionner et gèrent l'infrastructure Internet, notamment les fournisseurs de services de télécommunications et d'Internet, les points d'échange Internet et les réseaux de fourniture de contenus[50].

Les risques pour la liberté d'expression peuvent également émaner des décisions des organismes de normalisation dans le domaine d'Internet. En 2019 par exemple, une coalition d'organisations de défense des droits numériques a appelé publiquement la Société pour l'attribution des noms de domaines et des numéros sur Internet (ICANN) à empêcher la vente du nom de domaine de premier niveau « .org », utilisé principalement par des organisations caritatives et sans but lucratif, à un fonds d'investissement privé. La coalition affirmait que la gestion du nom de domaine par une organisation à but lucratif pourrait avoir des implications financières et politiques qui exacerberaient la diminution de l'espace à disposition de la société civile à travers le monde[51].

Dernier point mais non des moindres, la société civile et les défenseurs des droits numériques ont souligné que la réalisation de la liberté d'expression en ligne exige que les États et les acteurs privés adoptent des mesures visant à donner accès à une connexion Internet de qualité à un prix abordable. Dans un contexte où environ 40 % des habitants de la planète ne sont pas des utilisateurs actifs d'Internet[52], combler la fracture numérique entre les pays et au sein des pays est devenu une question cruciale de droits humains. De plus, le Rapporteur spécial des Nations Unies sur la promotion et la protection du droit à la liberté d'opinion et d'expression a souligné que la qualité et le type d'accès à Internet peuvent également avoir des effets négatifs sur le droit à la liberté d'expression. Par exemple, les menaces au principe de « neutralité du réseau » et les systèmes à taux zéro peuvent restreindre et limiter excessivement le type de contenu et d'information auxquels certains utilisateurs peuvent accéder en ligne[53].

Cadres et initiatives

Dans ce contexte, de plus en plus de pays adoptent des législations exigeant des entreprises de technologie ou les encourageant à identifier et supprimer différentes formes de contenus « préjudiciables » générés et téléchargés par des utilisateurs, notamment en établissant des régimes de responsabilité des intermédiaires. En 2018 par exemple, l'Allemagne a adopté une loi sur l'application du réseau (NetzDG), qui exige des entreprises de technologie qu'elles suppriment les discours de haine et les publications « manifestement illicites » dans un délai de 24 heures à compter de la réception d'une notification, ces entreprises s'exposant à des amendes allant jusqu'à 50 millions d'euros en cas d'inaction. En avril 2019, l'Australie a modifié son code pénal afin d'ériger en infraction la publication de « matériel violent haineux » et exige des entreprises de technologie qu'elles suppriment le matériel violent en ligne « diligemment ». En cas de non-conformité, les sanctions sont élevées : les entreprises peuvent être condamnées à une amende allant jusqu'à 10 % de leurs bénéfices annuels, et leurs dirigeants risquent une peine de prison.

Des évolutions réglementaires similaires sont envisagées également dans d'autres pays. En 2019, le Royaume-Uni a dévoilé un plan pour un nouveau régime réglementaire qui établirait un « devoir de diligence » pour les entreprises de technologie concernant la sécurité de leurs utilisateurs, ainsi qu'un régulateur indépendant afin d'assurer la conformité[54]. Au niveau de l'Union européenne, le Parlement européen a approuvé un projet de règles qui exigeraient des plateformes

en ligne qu'elles suppriment le contenu terroriste dans un délai d'une heure à compter de la notification par les autorités nationales. Une enquête menée par Freedom House a constaté qu'au moins 17 pays avaient approuvé ou proposé des lois en 2017 qui appliqueraient des restrictions aux médias en ligne au nom de la lutte contre les « fake news » et la manipulation en ligne[55].

Bien que les gouvernements qui proposent de telles lois déclarent généralement que toute restriction imposée à la liberté d'expression serait justifiée, des experts des droits humains ont contesté la sécurité juridique, la proportionnalité et la nécessité de certaines de ces lois et propositions à cause de leurs définitions vagues, des sanctions importantes et des délais courts. Nombreuses sont les préoccupations évoquées quant au fait que ces lois encouragent fortement le retrait excessif de contenu qui représente des formes d'expression licites et légitimes.

Au-delà du respect des lois nationales, les entreprises de technologie appliquent leurs propres règles (qu'elles soient décrites sous formes de conditions, de normes communautaires ou autre) concernant les modalités et les types d'expression et de comportement acceptables sur leurs plateformes. Il a été allégué que l'application arbitraire de ces règles et leur alignement limité sur les normes des droits humains restreignent de manière disproportionnée la liberté d'expression, souvent de manière discriminatoire[56].

Des organisations de la société civile ont identifié plusieurs cas de répression de la liberté d'expression sur des plateformes de réseaux sociaux, y compris concernant l'activisme LGBTI, des faits rapportant des cas de nettoyage ethnique et la dénonciation du racisme et des structures de pouvoir[57]. Une analyse des conditions d'utilisation de Facebook et de Twitter a conclu que leurs définitions et pratiques doivent s'aligner davantage sur les

© John Schnobrich

normes internationales en matière de liberté d'expression[58]. L'identification d'un contenu inapproprié au moyen d'algorithmes a été contestée pour n'avoir pas interprété correctement des indices langagiers propres à une culture et à un contexte. Le Rapporteur spécial des Nations Unies sur la liberté d'opinion et d'expression a noté qu'il existe un risque élevé que les systèmes de modération des contenus par l'intelligence artificielle ne suppriment des contenus sur la base de préjugés discriminatoires et que, par conséquent, les groupes vulnérables sont les plus susceptibles d'être désavantagés[59].

Plusieurs experts et défenseurs ont avancé des principes des droits humains pour la modération des contenus afin d'aborder les fermetures de comptes et le retrait de contenus inappropriés et excessifs. Par exemple, les Principes de Santa Clara sur la transparence et la responsabilité dans la modération des contenus sont des lignes directrices à l'intention des entreprises visant à garantir que la modération des contenus suive une procédure régulière, telle qu'un préavis et une possibilité de faire dûment appel à chaque utilisateur dont du contenu est supprimé ou le compte est suspendu[60]. Une coalition d'experts de la société civile a élaboré les Principes de Manille sur la responsabilité des intermédiaires dans le cadre d'efforts plus larges pour intégrer les principes des droits humains dans les cadres réglementaires relatifs aux contenus en ligne[61].

Dans son rapport de 2018 au Conseil des droits de l'homme, le Rapporteur spécial des Nations Unies sur le droit à la liberté d'opinion et d'expression proposait une série de principes des droits humains afin d'orienter la modération des contenus en ligne[62], en soulignant, entre autres, que lorsque des entreprises élaborent ou modifient des politiques ou produits, elles devraient recueillir activement et tenir compte des préoccupations des communautés historiquement exposées à un risque de censure et de discrimination[63].

De plus, de nouveaux modèles de gouvernance de la modération de contenus émergent en réponse à des appels à plus de responsabilité et de transparence sur les réseaux sociaux. En 2019, l'organisation de la société civile Article 19 a lancé une consultation publique mondiale sur l'établissement de Conseils sur les réseaux sociaux en tant qu'instances multipartites chargées des questions de modération des contenus sur les plateformes de réseaux sociaux sur la base des normes internationales relatives aux droits humains[64]. En 2020, Facebook a mis en place un Conseil de surveillance indépendant chargé d'examiner les recours contre les décisions de modération des contenus de l'entreprise[65].

En plus d'une approche fondée sur les règles de modération des contenus, des organes publics et des entreprises de technologie ont créé des partenariats visant à élaborer des programmes sociaux qui aborderaient la manipulation et les fausses informations en ligne. À titre d'exemple, des responsables politiques en Italie ont coopéré avec des journalistes et des entreprises des technologies en vue d'élaborer et de tester un programme à l'échelon national de repérage des manipulations en ligne, notamment les « fake news » et les théories du complot[66]. Apple a lancé une initiative d'éducation aux médias afin d'encourager la pensée critique et de donner aux étudiants les moyens d'être mieux informés. Aux États-Unis, l'entreprise a travaillé en partenariat avec plusieurs organisations sans but lucratif telles que News Literacy Project et Common Sense qui offrent des programmes indépendants d'éducation aux médias non-partisans[67]. WhatsApp a collaboré avec des organisations en Inde pour concevoir un programme de formation sur l'alphabétisation numérique pour ses utilisateurs[68]. Des entreprises de technologie ont travaillé en partenariat avec la société civile afin de lutter contre la désinformation sur leurs plateformes. L'organisation argentine Chequeado exploite une application logicielle en partenariat avec Facebook afin d'établir une correspondance automatique sur le réseau avec des recherches visant à vérifier des faits[69].

3. Le secteur des technologies dans les PAN

Cette section s'appuie sur les indications relatives au cycle de vie des PAN qui figurent dans le Guide IDDH-ICAR, et indique comment les États peuvent garantir que les aspects spécifiques relatifs au secteur des technologies sont pris en compte dans le processus et le contenu des PAN.

3.1. Cartographie et participation des parties prenantes

Comme l'indique le Guide IDDH-ICAR, il est essentiel que toutes les parties prenantes concernées soient dûment cartographiées et participent à l'élaboration d'un PAN.Leur consultation devrait se dérouler de manière ouverte, inclusive et transparente. Des institutions publiques chargées de traiter des questions relatives aux activités du secteur des technologies devraient être incluses dans la conception et la mise en œuvre du processus, notamment au moyen de l'attribution de ressources pour le renforcement des capacités, la participation à la collecte des données et les consultations du public et des experts. Il est essentiel que la cartographie des parties prenantes inclue des personnes et des groupes dont les droits au respect de la vie privée, à la liberté d'expression et à la non-discrimination sont les plus à risque, tels que les défenseurs des droits humains, les femmes et les filles, les minorités ethniques ou religieuses ou les personnes victimes de discriminations fondées sur leur orientation sexuelle et leur identité de genre. Des stratégies pour la participation de ces personnes et ces groupes devraient être élaborées spécialement afin de garantir que leurs droits soient protégés et que leurs voix soient entendues dans le cadre du processus.

Plusieurs catégories générales de parties prenantes devraient être prises en compte dans le processus de PAN, quel que soit le secteur d'activité ou le domaine politique. Afin d'aider les acteurs étatiques dans l'utilisation du Guide IDDH-ICAR, les catégories identifiées dans le Guide sont énumérées ci-dessous et accompagnées, le cas échéant, des parties prenantes spécifiques qui devraient être prises en compte pour le secteur des technologies.

CATÉGORIE DE PARTIES PRENANTES	PARTIES PRENANTES SPÉCIFIQUES AU SECTEUR DES TECHNOLOGIES
L'exécutif gouvernemental, et notamment l'ensemble des services, agences, bureaux gouvernementaux pertinents, les entreprises publiques, ainsi que la police et d'autres agences de maintien de l'ordre.	• Les Ministères des communications et/ou des TIC • Les Ministères de la justice • Les bureaux chargés des technologies au sein d'autres ministères, par ex. un « ambassadeur des technologies » auprès du Ministère des affaires étrangères ou un « bureau des technologies et de l'innovation » auprès d'un Ministère de l'économie • La police et les agences de maintien de l'ordre chargées de la cybercriminalité • Les autorités compétentes en matière de marchés publics et les acheteurs publics • Les instances réglementaires dont les mandats comprennent l'internet et les technologies numériques • Les instances réglementaires dont le mandat inclut les médias traditionnels et les nouveaux médias
Les tribunaux judiciaires et administratifs, les mécanismes alternatifs de résolution des différends, et les acteurs de justice informelle	• Le médiateur pour la transformation numérique (ou similaire) • Le médiateur pour l'égalité (ou similaire) • Les ordres des avocats

Le parlement, y compris les comités pertinents	• Les comités parlementaires dont le mandat couvre les communications et/ou les TIC • Les comités parlementaires dont le mandat couvre la justice, la criminalité et/ou la cybercriminalité • Les comités parlementaires dont le mandat couvre l'égalité et la non-discrimination
Les entreprises, et notamment les secteurs industriels importants, les associations d'entreprises, les petites et moyennes entreprises (PME), les auto-entrepreneurs, les entreprises individuelles, les coopératives, les structures sans but lucratif, et les acteurs du secteur informel	• Les organes sectoriels compétents en matière de technologies • Les entreprises des technologies exerçant leurs activités dans le pays ou y étant établies
Les syndicats de travailleurs et autres associations de représentation des travailleurs	• Les syndicats nationaux et sectoriels qui s'occupent de la question de la collecte des données des employés, de la répression des voix des travailleurs grâce à la surveillance des réseaux sociaux, de la non-discrimination, etc.
Les représentants de groupes ou communautés de titulaires de droits et les défenseurs des droits de l'homme, tant à l'intérieur qu'à l'extérieur de la juridiction territoriale d'un État, susceptibles d'être affectés par les activités d'entreprises basées dans l'État, ou contrôlées par l'État	• Les représentants des titulaires de droits qui pourraient être particulièrement marginalisés, par ex. les femmes et les filles, les personnes LGBTI, les minorités ethniques et religieuses, etc. • Les organisations des droits humains principalement actives sur les questions de respect de la vie privée, de liberté d'expression et/ou d'Internet et des technologies

	numériques (y compris les organisations de défense des droits numériques) • Les défenseurs de l'égalité (organisations de la société civile, juristes et autres acteurs travaillant sur des questions d'égalité et de non-discrimination) • Les organisations de défense des consommateurs qui représentent les droits des consommateurs/utilisateurs dont les droits pourraient être violés • Les organisations de défense de la liberté des médias
Les INDH, institutions de médiation, organes chargés de l'égalité statutaire, et autres mécanismes nationaux dotés d'un mandat relatif aux droits de l'homme	• Les institutions nationales des droits humains • Les autorités compétentes en matière de protection des données • Les organes nationaux chargés de l'égalité
Les OSC dotées de mandats traitant de sujets pertinents	• Les organisations des droits humains principalement actives sur les questions de respect de la vie privée, de liberté d'expression et/ou d'Internet et des technologies numériques (y compris les organisations de défense des droits numériques) • Les défenseurs de l'égalité (organisations de la société civile, juristes et autres acteurs travaillant sur des questions d'égalité et de non-discrimination)

	• Là où ces organisations n'existent pas au niveau national, des organisations internationales (telles que Global Partners Digital, Equal Rights Trust, Access Now, Association for Progressive Communications, Article 19 et Privacy International) pourraient être impliquées
Les médias, y compris les sources d'information généralistes et spécialisées	• Les entreprises de médias en ligne • Les forums en ligne
Les universités, y compris les instituts de recherche, experts individuels, et institutions académiques pertinentes, comme les écoles de commerce	• Les institutions académiques et de recherche spécialisées dans l'internet et les technologies numériques
Les acteurs internationaux et régionaux, y compris les agences pertinentes de l'ONU, la Banque mondiale, les banques régionales de développement, et l'OCDE	• L'Union internationale des télécommunications • La Commission de la science et de la technique au service du développement des Nations Unies • L'UNICEF, Équipe chargée des entreprises et des droits des enfants • Le Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH) • Le Conseil de l'Europe, Service de l'antidiscrimination

INSTANCES RÉGLEMENTAIRES

En matière de réglementation du secteur des technologies (et plus généralement des technologies), les approches adoptées varient selon les pays. Certaines accordent de nouvelles fonctions et pouvoirs aux instances réglementaires existantes. D'autres commencent à instituer de nouvelles instances réglementaires dont les mandats portent sur différents aspects d'Internet et des technologies.

Australie : en 2015, l'Australie a institué le Commissaire chargé de la sécurité électronique des enfants (Children's eSafety Commissioner), dont le mandat consiste à protéger la sécurité des enfants en ligne. Depuis lors, le mandat de l'instance (désormais appelée Commissaire de la sécurité électronique (eSafety Commissioner)) a été étendu en vue d'agir pour empêcher les abus liés aux images et d'autres formes de contenus interdits.

Danemark : le Conseil danois pour l'éthique des données, un organe indépendant, est composé de membres représentant un vaste éventail de compétences, des secteurs tant public que privé. Le Conseil consulte et conseille le gouvernement danois, le parlement et les autorités publiques sur des questions relatives à l'éthique des données dans l'utilisation des données et des nouvelles technologies, et promeut une culture de l'utilisation responsable des données par les entreprises et le public.

Royaume-Uni : le Centre pour l'éthique et l'innovation en matière de données a été établi en 2018 avec pour mandat « d'analyser et d'anticiper les occasions et les risques posés par les technologies alimentées par les données » (en mettant l'accent en particulier sur l'intelligence artificielle) et « proposer des conseils pratiques et fondés sur des faits pour y faire face ».

INSTITUTIONS NATIONALES DES DROITS HUMAINS

Les institutions nationales des droits humains (INDH) s'intéressent de plus en plus aux technologies et à leurs effets sur les droits humains, parfois dans le cadre de leurs activités générales en matière d'entreprises et de droits humains. À ce titre, au cours de l'élaboration d'un PAN, elles peuvent faire part de perspectives spécifiques concernant la façon dont les droits humains tels que les droits au respect de la vie privée et à la liberté d'expression sont affectés par le secteur des technologies.

Australie : en 2018, la Commission australienne des droits humains (AHRC) a lancé un projet sur la relation entre droits humains et technologie. Avec les conseils d'un Groupe de référence spécialisé constitué de représentants du milieu universitaire, d'entreprises et des États, le projet examine les questions relatives aux droits humains en lien avec l'intelligence artificielle, les préjugés, les mégadonnées, la technologie inclusive et l'intersection entre technologie, liberté d'expression et démocratie. L'AHRC prévoit de formuler des recommandations concernant la façon de garantir que les droits humains soient prioritaires dans la conception et la gouvernance des technologies émergentes en 2020.

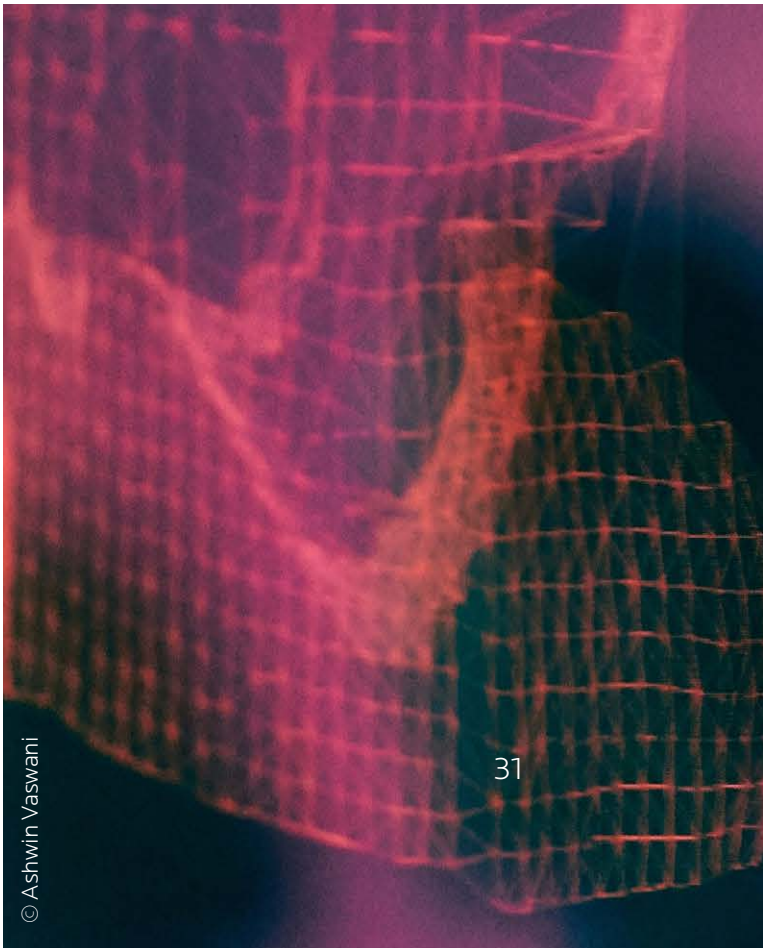
Danemark : l'Institut danois des droits de l'homme mène des recherches spécifiques sur les technologies et leurs effets sur les droits humains depuis 2003. Il a contribué

à l'élaboration de normes dans ce domaine aux Nations Unies, à l'Union européenne et au Conseil de l'Europe. L'Institut collabore avec des entreprises de technologie et élabore actuellement un guide sur la réalisation d'évaluations des effets des activités des entreprises du numérique sur les droits humains.

Kenya : en février 2019, la Commission nationale des droits humains du Kenya (KNCHR), en collaboration avec la Commission des droits humains du Kenya et le Forum des droits de Nubie, a déposé une pétition devant la Haute Cour de Nairobi, qui contestait la mise en place d'un système national numérique obligatoire d'enregistrement de l'identité, le National Integrated Identity Management System (NIIMS). La KNCHR a soutenu les autres pétitionnaires en affirmant entre autres que le NIIMS violait le droit au respect de la vie privée parce qu'aucune protection adéquate n'avait été assurée et les droits à l'égalité et à la non-discrimination concernant la communauté nubienne et d'autres groupes marginalisés qui seraient confrontés à une aggravation de leur exclusion. Le 30 janvier 2020, la Haute Cour a jugé que le gouvernement kenyan devait interrompre la mise en place du système jusqu'à ce qu'il existe « un cadre réglementaire complet et approprié de mise en œuvre du NIIMS ». Le jugement soulignait l'importance de disposer d'un cadre de protection des données et d'un cadre réglementaire clair qui tienne compte de la possibilité de cas d'exclusion.

3.2. Groupes á risque

Comme pour les autres secteurs d'activité et domaines politiques, il est important de tenir compte des besoins et des expériences de différents groupes, en particulier des groupes à risque, et de répondre à ces besoins et expériences, lors de la cartographie des parties prenantes (et de leur implication). Pour ce qui est du secteur des technologies, certains titulaires de droits et groupes sont particulièrement exposés au risque de violations des droits humains, et l'État devrait donc identifier les personnes, organes et organisations qui représentent légitimement les intérêts de ces groupes, en garantissant que leur participation n'entraînera pas de représailles ou une forme quelconque de harcèlement. Le tableau ci-dessous présente des exemples d'effets néfastes et discriminatoires sur les droits au respect de la vie privée et à la liberté d'expression asur des personnes possédant certaines caractéristiques. Il s'agit d'une liste non-exhaustive et les États devraient garantir que tous les groupes qui pourraient être affectés de manière disproportionnée par des politiques relatives au secteur des technologies soient encouragés et habilités à participer à des consultations.



© Ashwin Vaswani

© Kelly Sikkema

CARACTÉRISTIQUE/GROUPE	EXEMPLES D'EFFETS NÉGATIFS ET DISCRIMINATOIRES SUR LES DROITS AU RESPECT DE LA VIE PRIVÉE ET À LA LIBERTÉ D'EXPRESSION
ÂGE/ENFANTS	
Les enfants sont exposés à un risque disproportionné de collecte excessive de données, de manipulation et d'abus en ligne à cause de leurs capacités cognitives, sociales et affectives en développement. Des entreprises recueillent des données sur des enfants dès la naissance sans leur consentement et sans qu'ils en soient informés, à travers les informations partagées par leurs parents et l'utilisation des dispositifs de contrôle parental. La publicité ciblée et les modèles des moteurs de recherche peuvent s'avérer préjudiciables pour le développement des enfants en influençant leurs préférences en tant que consommateurs et leur capacité à formuler des avis autonomes. La présence croissante des enfants sur les réseaux sociaux et d'autres plateformes numériques a accru les risques d'abus sexuels, de harcèlement et de cyberintimidation.	• La Commission fédérale du commerce des États-Unis a imposé plusieurs amendes à des entreprises de technologie pour avoir collecté des données personnelles concernant des enfants sans le consentement de leurs parents. • Selon Human Rights Watch, la « loi sur la propagande homosexuelle » de la Russie de 2013 interdit la « promotion des relations sexuelles non-traditionnelles auprès des mineurs », ce qui a eu des effets préjudiciables sur la jeunesse LGBTI qui essaie d'accéder à des sites web proposant une éducation en ligne et des services de soutien. • Selon une récente étude portant sur la distribution des captures d'abus sexuels d'enfants diffusés en direct, 98 % des images représentaient des enfants dont l'âge était évalué à 13 ans ou moins, et 96 % des images représentaient des filles. • Aux États-Unis, des écoles ont engagé des entreprises de surveillance des

réseaux sociaux afin de prévenir la violence et les fusillades dans les écoles. Néanmoins, les programmes de surveillance ont été contestés à cause de leur interférence disproportionnée avec l'exercice de la liberté d'expression des adolescents en ligne.

GENRE/FEMMES

La discrimination à laquelle les femmes sont confrontées hors ligne a envahi les espaces numériques. En 2018, le Conseil des droits de l'homme des Nations Unies a adopté une résolution reconnaissant le problème de la discrimination et de la violence à l'égard des femmes dans les contextes numériques. De nouveaux termes ont été introduits afin de comprendre les nouvelles formes de violence en ligne telles que « doxing », « sextorsion », « trolling », harcèlement moral en ligne, cyberprédation et « vengeance pornographique » (la distribution non-consensuelle de contenus intimes). La publication sans consentement de photographies intimes constitue une forme de violence fondée sur le genre qui viole les droits des femmes et des filles au respect de la vie privée. Les menaces et les abus en ligne empêchent les femmes d'exercer leur droit à la liberté d'expression, y compris par leur retrait des plateformes numériques, des débats publics et des fonctions publiques. Les défenseures des droits humains, les femmes actives en politique et les journalistes, sont exposées à un risque accru de violence en ligne.

Par ailleurs, la discrimination, les inégalités et les stéréotypes en ligne ont engendré une fracture numérique entre les hommes et les femmes qui fait que les femmes et les filles sont beaucoup moins

- Une étude d'Amnesty International de 2018 constatait que les femmes sont davantage susceptibles d'être victimes de harcèlement et d'abus sur Twitter, y compris au moyen de violations de la vie privée telles que le doxing ou le partage d'images à caractère sexuel ou intime sans consentement. Le harcèlement en ligne a souvent entraîné une auto-censure par les femmes de leurs publications, et l'abandon complet de Twitter. Selon le rapport, Twitter a enquêté et répondu de manière inadéquate à des signalements de violence et d'abus.

- En 2019, une députée élue à la Chambre des représentants des États-Unis a démissionné après la publication en ligne sans son consentement de photos nues par des médias en ligne.

- Une enquête menée en 2018 par l'Union interparlementaire constatait qu'un nombre important de femmes parlementaires européennes avaient été victimes de contenus abusifs, sexuels et violents sur les réseaux sociaux.

- En 2016, Al Jazeera rendait compte de l'existence d'un marché d'échange de vidéos de viol dans l'État d'Uttar Pradesh, en Inde.

susceptibles que les hommes d'utiliser Internet et de tirer parti des possibilités financières, formatives et de connectivité sociales en ligne qu'il offre.

- Selon une enquête de 2019 menée auprès de femmes journalistes au Pakistan, les femmes indiquaient que la violence en ligne avait eu des répercussions importantes sur leur santé mentale et qu'elles s'étaient auto-censurées afin de contrer la violence en ligne.
- Des activistes ont exprimé leur préoccupation quant au fait que des données personnelles recueillies au moyen de dispositifs intelligents pour la maison et des technologies numériques peuvent être utilisées pour contrôler et intimider des victimes de violence domestique.
- Selon l'Union internationale des télécommunications, en 2017 dans le monde, la proportion de femmes qui utilisaient Internet était de 12 % inférieure à celle des hommes utilisant Internet. L'écart se creusait en Afrique, où la proportion des femmes utilisant Internet était de 25 % inférieure à celle des hommes.

DÉFENSEURS DES DROITS HUMAINS

Les défenseurs des droits humains à travers le monde ont compté sur la technologie pour s'organiser, mobiliser et défendre les droits humains. Leur présence numérique a augmenté leur exposition à la surveillance et au contrôle en ligne à l'aide de logiciels espion avec des conséquences préjudiciables pour leur sécurité et le respect de leur vie privée. Des gouvernements décrètent de plus en plus fréquemment des interruptions d'Internet afin de faire taire des défenseurs des droits humains.

- Selon Amnesty International, l'entreprise israélienne NSO Group a développé une technologie de logiciel espion visant à réduire au silence des défenseurs des droits humains dans des pays comme le Mexique, le Maroc et l'Arabie saoudite. WhatsApp a poursuivi NSO Group en justice en octobre 2019, l'accusant d'avoir aidé le gouvernement à pénétrer dans les téléphones de quelques 1 400 utilisateurs, dont des journalistes et des dissidents politiques.
- En 2019, un groupe d'organisations de la société civile a fait part de

sa préoccupation au sujet de la tendance globale à la persécution des défenseurs des droits humains.

- Selon Human Rights Watch, l'interruption d'Internet imposée par le Conseil militaire de transition du Soudan en 2019 a empêché des activistes de rendre compte d'informations critiques dans le contexte instable d'une crise politique.

RACE ; APPARTENANCE ETHNIQUE ET RELIGION

La discrimination fondée sur la race, l'appartenance ethnique et la religion s'est étendue à l'espace en ligne à travers la surveillance numérique, des restrictions illégitimes à la liberté d'expression, ainsi que la modération inadéquate de contenus de discours haineux.

- Une fuite de données de 2019 a révélé que la Chine surveillait les déplacements de près de 2,6 millions de personnes dans la région du Xinjiang, où vivent les Ouïghours et d'autres minorités musulmanes, au moyen d'une société spécialisée dans la reconnaissance faciale et d'une entreprise travaillant pour le compte de la police, appelée SenseNet.
- Vox faisait état de deux études scientifiques qui démontrent que les modèles d'intelligence artificielle employés par les entreprises de réseaux sociaux ont 1,5 fois plus de probabilité de signaler des tweets rédigés par des Afro-américains comme étant « injurieux » comparé à d'autres tweets.
- Une étude menée en 2019 par l'Université de Cardiff a constaté une corrélation entre les discours haineux sur Twitter qui ciblent la race et la religion, et les infractions aggravées par des motivations raciales et religieuses qui se produisaient hors ligne à la même période.

- En 2020, dans le cadre des manifestations mondiales du mouvement Black Lives Matter, une plus grande attention a été accordée aux politiques de modération des contenus des principaux réseaux sociaux pour ce qui avait trait aux discours haineux et à l'incitation à la violence, ainsi qu'à la nécessité d'agir davantage pour lutter contre l'utilisation des plateformes des réseaux sociaux par des individus pour violer les droits humains.

- En 2019, la Société pour l'attribution des noms de domaines et des numéros sur Internet (ICANN) a octroyé à la société Amazon le droit exclusif d'administrer le nom de domaine de premier niveau général « .amazon ». Des spécialistes des droits humains ont affirmé que cette décision privera les Autochtones de la région amazonienne de possibilités de développement économique, et qu'en vertu du droit international des droits humains, la société Amazon avait la responsabilité de s'assurer que les Autochtones soient consultés avant de présenter sa demande.

- En février 2020, le gouvernement de Myanmar a réinstauré une interruption du trafic Internet mobile dans cinq communes de l'État de Rakhine et de l'État Chin. Elles s'ajoutent aux quatre communes de l'État de Rakhine où le réseau était interrompu depuis juin 2019, causant un embargo sur l'information qui affecte environ un million de personnes, dont la majorité appartiennent à la minorité ethnique musulmane rohingya. Entraver leur capacité à communiquer rend l'obtention d'aide en période de conflit difficile, tout comme la fourniture d'une assistance par les organismes humanitaires.

3.3. Réalisation d'une évaluation de référence nationale

Une étape importante dans le cycle de vie d'un PAN est la réalisation d'une évaluation de référence nationale (ERN). Comme l'indique le Guide IDDH-ICAR, « L'objectif principal d'une ERN relative aux entreprises et aux droits de l'homme est d'évaluer le niveau existant de mise en œuvre des PDNU dans un État donné. Elle combine une analyse des lacunes d'ordre législatif et politique concernant la mise en œuvre des PDNU avec un aperçu des incidences négatives des entreprises sur les droits de l'homme, afin d'identifier les problématiques les plus saillantes relatives aux droits de l'homme dans un contexte donné. Elle sert ainsi à éclairer la formulation et la priorisation des actions figurant dans un PAN ».

Le « Modèle d'évaluation de référence nationale (ERN) pour le secteur des technologies » devrait être utilisé pour déterminer comment les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/non-discrimination des personnes affectées par le secteur des technologies sont protégés par le cadre juridique et politique relatif aux entreprises et aux droits humains. Il a été élaboré en vue d'être utilisé conjointement avec le Modèle complet d'ERN qui figure dans le Guide IDDH-ICAR.

Alors qu'ils entreprennent une ERN et l'utilisent comme outil pour élaborer un PAN, les États devraient analyser et évaluer des mesures spécifiques qui garantissent à la fois une protection étatique et le respect par les entreprises des droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination, ainsi que des voies de recours efficaces lorsque ces droits ont été violés.

Le modèle ci-dessous contient les questions essentielles permettant de délimiter la problématique de la protection et du respect des droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination dont les États devraient tenir compte lors de l'élaboration d'une ERN. Les questions sont le reflet des dispositions des PDNU sur le devoir de l'État de protection contre les violations des droits humains (pilier I), la responsabilité des entreprises de respecter les droits humains (pilier II) et l'établissement de voies de recours tant par les acteurs étatiques que par les acteurs non-étatiques (pilier III). L'inclusion de ces questions dans une ERN générale permettra aux décideurs politiques d'obtenir des informations détaillées sur les différentes formes d'implication du secteur des technologies ayant des effets négatifs et discriminatoires sur le respect de la vie privée et la liberté d'expression, d'évaluer leur gravité et de décider si et comment en faire des priorités dans le PAN.

Les États devraient envisager de consulter des spécialistes locaux dès le début de l'ERN, ainsi que tout au long de sa rédaction. Comprendre les activités des entreprises de technologie et la façon dont elles peuvent affecter les droits humains exige des connaissances spécialisées. Il est recommandé que l'organisation qui mène l'ERN dispose des capacités adéquates pour analyser des données technologiques, identifier les risques et comprendre l'écosystème complexe dans lequel les entreprises de technologie opèrent.

Dans le cadre de l'ERN, l'État pourrait envisager de mandater une évaluation des effets sur les

droits humains de l'ensemble du secteur. Une évaluation des effets sur les droits humains axée sur le secteur des technologies aidera les acteurs étatiques et d'autres parties prenantes à voir le « tableau d'ensemble » des effets négatifs potentiels des activités du secteur des technologies.

À PROPOS DE L'EXTRATERRITORIALITÉ

Bien que les PDNU indiquent que les États ne sont généralement pas tenus de réglementer les activités extraterritoriales des entreprises domiciliées sur leur territoire et/ou sous leur juridiction, ils reconnaissent également que cela ne leur est généralement pas interdit, pour autant qu'il existe une base juridictionnelle reconnue. Les PDNU reconnaissent qu'il peut exister de très bonnes raisons, politiquement, pour que les États énoncent clairement leurs attentes à l'égard des entreprises à l'étranger. Les États ne jouissent pas d'un pouvoir illimité pour promulguer des lois qui s'appliquent aux activités extraterritoriales et doivent agir dans les limites des contraintes du droit international et de la courtoisie internationale.

Bien que cette considération doive être faite dans de nombreux secteurs, elle est particulièrement pertinente pour le secteur des technologies, étant donné que de nombreuses entreprises de technologie sont actives à l'échelon mondial, et ont des produits et services qui seront disponibles à travers le monde, souvent dans des pays où l'entreprise n'a aucune présence physique. Au vu de la nature immatérielle de certaines activités numériques, il peut s'avérer difficile d'identifier précisément où les activités se produisent et quel régime juridique national s'applique.

Le cadre réglementaire qui s'applique aux entreprises dans un pays, en particulier dans leur pays d'origine, aura souvent des effets dans d'autres pays où la société exerce ses activités. Par exemple, le RGPD de l'UE (voir l'encadré 4) fixe des normes plus strictes que la plupart des autres cadres nationaux de protection des données. Plutôt que d'adopter de nombreuses politiques différentes en matière de protection des données pour différents pays, certaines entreprises de technologie utilisent simplement les prescriptions du RGPD comme politique mondiale de protection des données, une évolution positive sous l'angle du respect de la vie privée.

Néanmoins, dans un nombre croissant de cas, il est demandé à des tribunaux de décider si des contenus en ligne qui violent la législation nationale peuvent être supprimés mondialement par des entreprises de technologie, plutôt que dans un seul pays, ce qui soulève différentes préoccupations, notamment concernant le respect de la vie privée et la liberté d'expression

Il convient donc que les États examinent avec soin l'application extraterritoriale de la législation nationale, y compris à travers des décisions des tribunaux, afin de s'assurer que les PAN, et les cadres juridique et politique qu'ils adoptent, garantissent que les entreprises de technologie respectent les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination dans les pays dans lesquels ils exercent une activité.

Modèle d'évaluation de référence nationale(ERN) pour le secteur des technologies et les PAN

1. CADRE JURIDIQUE ET POLITIQUE

Les États devraient évaluer si leurs cadres juridique et politique offrent une protection adéquate contre les violations des droits humains liées au secteur des technologies. Les États devraient également évaluer dans quelle mesure ces lois et politiques contribuent à la prévention de tels abus.

Bien que les questions ci-dessous se concentrent sur les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination, elles pourraient être élargies pour inclure d'autres droits humains.

1.1. NORMES INTERNATIONALES, RÉGIONALES ET AUTRES NORMES

Normes internationales	L'État a-t-il signé, ratifié et mis en œuvre les instruments internationaux relatifs aux droits humains pertinents qui protègent les droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination, en particulier le Pacte international relatif aux droits civils et politiques ? Depuis 2011, l'État a-t-il reçu des recommandations émanant du Comité des droits de l'homme des Nations Unies (ou de l'organe conventionnel surveillant les instruments respectifs) concernant la protection des droits au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination en lien avec les activités du secteur des technologies ? Le cas échéant, quel est l'état d'avancement de la mise en œuvre des recommandations de cet organe ? Depuis 2011, l'État a-t-il reçu des recommandations émanant des Procédures spéciales des Nations Unies ou de l'Examen périodique universel concernant la protection des droits au respect de la vie privée, à la liberté d'expression ou à l'égalité/à la non-discrimination en lien avec les activités du secteur des technologies ? Le cas échéant, quel est l'état d'avancement de la mise en œuvre des recommandations de ces organes ?

Normes régionales	L'État a-t-il signé, ratifié et mis en œuvre les instruments régionaux des droits humains pertinents, tels que : • la Convention américaine des droits de l'homme • la Charte africaine des droits de l'homme et des peuples • la Convention européenne des droits de l'homme ? Depuis 2011, l'État a-t-il reçu des recommandations émanant d'organes régionaux concernant la protection des droits au respect de la vie privée, à la liberté d'expression ou à l'égalité/à la non-discrimination en lien avec les activités du secteur des technologies ? Le cas échéant, quel est l'état d'avancement de la mise en œuvre des recommandations de cet organe ? Depuis 2011, une cour régionale des droits humains a-t-elle constaté que l'État violait son devoir de protection contre les abus liés au respect de la vie privée, à la liberté d'expression ou à l'égalité/à la non-discrimination par une entreprise de technologie ? Le cas échéant, quel est l'état d'avancement de la mise en œuvre des recommandations de cette cour ?
Autres normes	L'État a-t-il signé, intégré ou approuvé les normes et initiatives suivantes pertinentes pour le secteur des technologies et le respect de la vie privée, la liberté d'expression et l'égalité/la non-discrimination : • Cadre en matière de respect de la vie privée de la Coopération économique Asie-Pacifique • Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du Conseil de l'Europe • Recommandation No. R(99) 5 sur la protection de la vie privée sur Internet du Conseil de l'Europe • Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme du Conseil de l'Europe • Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE

	• Recommandations d'Amsterdam sur la liberté des médias et Internet de l'Organisation pour la sécurité et la coopération en Europe • Déclaration de principes sur la liberté d'expression en Afrique de l'Union africaine • Principes internationaux sur l'application des droits de l'homme à la surveillance des communications • Principes de Manille sur la responsabilité des intermédiaires • Déclaration de Toronto : protéger le droit à l'égalité et à la non-discrimination dans les systèmes reposant sur l'apprentissage automatique • Freedom Online Coalition • Plan d'action de Rabat ?

1.2. LOIS ET POLITIQUES NATIONALES

Droit au respect de la vie privée	La constitution ou la législation garantit-elle le droit au respect de la vie privée ? Des exceptions sont-elles prévues dans la législation qui restreignent le droit au respect de la vie privée ? Si tel est le cas : • Sont-elles conformes aux limitations autorisées énoncées par le droit international et régional des droits humains, et donc existe-t-il une base juridique claire et non-discriminatoire, et sont-elles nécessaires et proportionnées pour atteindre un objectif légitime ?
Protection des données	La protection des données est-elle réglementée, y compris la collecte, le stockage, l'utilisation et le partage des données personnelles ? Si tel est le cas : • Est-elle conforme aux bonnes pratiques internationales, telles que le Règlement général sur la protection des données de l'UE ? En particulier :

	• Couvre-t-elle toutes les formes de données personnelles ? • Couvre-t-elle tous les utilisateurs/personnes ou uniquement les consommateurs ? • S'applique-t-elle à tous les sous-traitants de données dans le secteur privé et le secteur public ? • Là où le consentement constitue la base juridique du traitement des données, exige-t-il que la demande de consentement soit éclairée, claire, intelligible, accessible et formulée simplement ? • Permet-il aux personnes de demander aux sous-traitants des données des copies de leurs données, et de les faire corriger ou supprimer ? • Prévoit-il un droit à la portabilité des données ? • Inclut-il un droit des individus de ne pas être soumis à des décisions ayant des effets significatifs basées sur un traitement automatisé ? Existe-t-il une loi qui permet aux gouvernements d'accéder aux données stockées par des entreprises de technologie (par ex. lois en matière de conservation des données, de métadonnées) ? Existe-t-il des mécanismes ou organes nationaux de supervision qui peuvent traiter les plaintes au sujet des violations des données et exécuter la législation sur la protection des données, comme l'autorité compétente en matière de protection des données ? Si tel est le cas : • Ces organes disposent-ils de ressources adéquates ? • Combien de violations des données par des entreprises ont-elles été enregistrées au cours des cinq dernières années ?
Cryptage	Existe-t-il une loi ou une politique qui exige ou encourage l'utilisation d'un cryptage solide par des entreprises de technologie pour les données personnelles ou les communications ? Existe-t-il une loi ou une politique qui restreint ou sape la capacité des entreprises de technologie de crypter les données personnelles ou les communications ?

Surveillance	Existe-t-il une loi ou une politique qui réglemente la surveillance, l'interception ou l'interférence en ligne des communications privées ? Si tel est le cas : • Est-elle conforme aux bonnes pratiques internationales, comme les Principes internationaux sur l'application des droits de l'homme à la surveillance des communications ? En particulier : • La loi est-elle suffisamment claire et précise pour que les personnes disposent d'un préavis et puissent prévoir son application ? • La surveillance est-elle autorisée uniquement lorsqu'elle est nécessaire pour atteindre un objectif légitime et est-elle effectuée de manière non-discriminatoire ? • La loi autorise-t-elle la surveillance uniquement lorsqu'elle est permise par une autorité judiciaire compétente impartiale et indépendante ? • Permet-elle aux entreprises de technologie de s'opposer aux demandes ou de contester les demandes qui leur sont adressées par des organismes publics ? • Limite-t-elle la transparence des entreprises concernant les demandes de données émanant du gouvernement ? • Quelle évaluation a été faite de la mise en œuvre de la législation, et de la participation des entreprises de technologie à sa mise en œuvre ?
Liberté d'expression	La constitution ou la législation garantit-elle le droit à la liberté d'expression ? Une loi sur la liberté d'information existe-t-elle ? Des exceptions sont-elles prévues dans la législation qui restreignent le droit à la liberté d'expression ? Si tel est le cas, sont-elles conformes aux limitations autorisées énoncées par le droit international et régional des droits humains, et donc existe-t-il une base juridique claire et non-discriminatoire, et sont-elles nécessaires et proportionnées pour atteindre un objectif légitime ? Une loi permet-elle aux gouvernements de bloquer ou restreindre l'accès à Internet ?

Réglementation du contenu	Existe-t-il une loi ou une politique qui réglemente le contenu en ligne ou les politiques de modération des contenus des entreprises de technologie ? Si tel est le cas : • Est-elle conforme aux bonnes pratiques internationales, telles que les Principes de Manille sur la responsabilité des intermédiaires ? En particulier : • Les règles qui régissent la responsabilité des intermédiaires sont-elles précises, claires et accessibles ? • Les intermédiaires sont-ils exempts de toute responsabilité pour les contenus de tiers dans les cas où ils n'ont pas été impliqués dans la modification de ces contenus ? • Garantit-elle que les intermédiaires ne peuvent être tenus pour responsables de n'avoir pas restreint des contenus licites ? • Interdit-elle une responsabilité stricte des intermédiaires pour l'hébergement de contenus illicites de tiers ? • Interdit-elle l'obligation pour les intermédiaires de surveiller activement les contenus ? • Garantit-elle que les intermédiaires ont uniquement l'obligation de restreindre les contenus lorsqu'une décision a été prononcée par une autorité judiciaire indépendante et impartiale, qui a déterminé que le matériel en question était illicite ? • Garantit-elle que l'intermédiaire et le fournisseur de contenus pour les utilisateurs sont en mesure d'exercer un droit effectif d'être entendu (excepté dans des circonstances exceptionnelles) ? • Impose-t-elle des délais courts pour le retrait de contenus illicites une fois signalés à l'intermédiaire ? • Impose-t-elle des sanctions financières élevées ou d'autres sanctions disproportionnées en cas de non-conformité ?

	• La transparence prévaut-elle concernant les ordres ou demandes de suppression de contenus reçus par des entreprises de technologie ? Une loi ou une politique exige-t-elle des entreprises de technologie qu'elles publient des politiques de modération des contenus formulées de manière claire et accessible ?
Égalité/non-discrimination	La constitution ou la législation garantit-elle le droit à la non-discrimination ? L'État a-t-il adopté un cadre juridique complet en matière de lutte contre la discrimination ? • Le cadre juridique interdit-il la discrimination sur la base de motifs non-exhaustifs et explicites ? • La discrimination multiple, y compris la discrimination croisée, est-elle interdite ? • Le cadre juridique définit-il et interdit-il de manière adéquate toutes les formes de discrimination reconnues au niveau international, à savoir la discrimination directe, la discrimination indirecte, le harcèlement et le fait de ne pas procéder à des aménagements raisonnables ? • La protection contre la discrimination est-elle prévue dans tous les domaines de la vie réglementés par le droit ? • Le cadre juridique impose-t-il des obligations de non-discrimination aux acteurs privés ? Des justifications à la discrimination indirecte figurent-elles dans le cadre juridique ? Si tel est le cas, sont-elles conformes aux normes internationales, à savoir la poursuite d'un objectif légitime et leur caractère approprié et nécessaire ? Existe-il des justifications à la discrimination directe ? Elles ne peuvent être justifiées que dans des circonstances tout à fait exceptionnelles sur la base de critères stricts étant donné que la discrimination directe poursuit rarement un objectif légitime.

	Le cadre juridique de lutte contre la discrimination de l'État exige-t-il une action positive lorsque des inégalités de fond sont identifiées, y compris dans l'accès et l'utilisation d'Internet et des nouvelles technologies ? • L'État a-t-il mis en œuvre des politiques d'action positive concernant l'accès et l'utilisation d'Internet et des nouvelles technologies ? L'État prévoit-il des évaluations de l'impact sur l'égalité comme élément à part entière de ses politiques ? Les évaluations de l'impact sur l'égalité visent-elles à identifier et éliminer les effets discriminatoires effectifs ou potentiels des politiques publiques ?
Devoir de diligence	Les entreprises, y compris les entreprises de technologie, doivent-elles faire preuve, ou attend-on d'elles qu'elles fassent preuve, d'une diligence raisonnable ou adoptent d'autres formes de procédures de diligence raisonnable, comme la protection des données et des évaluations de l'impact sur l'égalité, y compris pour évaluer et rendre compte de leurs effets négatifs sur les droits humains ? Si tel est le cas : • L'État fournit-il des indications ou exige-t-il une méthode pour les procédures de diligence raisonnable ?

2. LA RESPONSABILITÉ DU SECTEUR DES TECHNOLOGIES DE RESPECTER LES DROITS HUMAINS

Au titre du deuxième pilier des PDNU, les entreprises de technologie ont la responsabilité de respecter les droits humains et de respecter un devoir de diligence adéquat en matière de droits humains. Les États devraient évaluer dans quelle mesure les entreprises de technologie se conforment à cette responsabilité et tiennent compte des droits humains dans leurs politiques et leurs activités.

Les questions ci-dessous peuvent être utilisées pour recueillir des informations auprès des entreprises de technologie concernant les politiques et procédures de gestion pour le respect des droits humains conformément aux attentes énoncées par le deuxième pilier des PDNU. Elles peuvent être modifiées pour s'adapter au type d'entreprise concernée (multinationale, PME, entreprise d'État, société cotée en bourse) et élargies afin d'inclure des aspects relatifs aux droits humains autres que le respect de la vie privée, la liberté d'expression et l'égalité/la non-discrimination.

2.1. GOUVERNANCE	
Engagement public	Les entreprises de technologie du pays ont-elle pris un engagement public en faveur du respect des droits humains ? Si tel est le cas • Cet engagement figure-t-il dans (i) une politique autonome en matière de droits humains, (ii) une autre politique telle que la politique en matière de durabilité ou de responsabilité sociale de l'entreprise ? Les entreprises de technologie du pays ont-elles adhéré à des initiatives multipartites incluant une composante des droits humains comme la Global Network Initiative ou le Pacte mondial des Nations Unies ?
Gouvernance et surveillance de la direction	Les hauts dirigeants des entreprises de technologie exercent-ils un contrôle sur la façon dont leurs politiques et pratiques affectent les droits humains ? L'engagement public de respect des droits humains est-il intégré dans toutes les fonctions et activités commerciales ?
Mise en œuvre interne	Les entreprises de technologie disposent-elles de mécanismes pour mettre en œuvre leurs engagements en faveur des droits humains ?
2.2. DROITS HUMAINS SPÉCIFIQUES	
Droit au respect de la vie privée	Les politiques et les engagements des entreprises de technologie font-ils état de moyens concrets par lesquels elles respectent le droit au respect de la vie privée des utilisateurs ?
Protection des données	Les entreprises de technologie disposent-elles de politiques en matière de protection des données claires et accessibles par les utilisateurs ?

	Les entreprises de technologie délivrent-elles un préavis aux utilisateurs lorsqu'elles modifient leurs politiques en matière de protection de la vie privée ? Est-ce que les politiques en matière de protection des données : • indiquent clairement quelles données personnelles sont recueillies et traitées, et comment ? • demandent le consentement éclairé des utilisateurs pour la collecte, le traitement et le partage des données ? • indiquent clairement quelles données personnelles sont partagées et avec qui ? • indiquent clairement les objectifs de la collecte, du traitement et du partage des données personnelles ? • indiquent clairement la durée de conservation des données personnelles ? • indiquent clairement aux utilisateurs comment ils peuvent exercer un contrôle sur la collecte, le traitement et le partage de leurs données personnelles ? • permettent aux utilisateurs d'obtenir des copies des données personnelles détenues ? • permettent aux utilisateurs de faire corriger ou supprimer leurs données personnelles ?
Sécurité des données	Les entreprises de technologie : • divulguent-elles clairement les informations relatives à leurs processus institutionnels pour garantir la sécurité de leurs produits et services ? • examinent-elles les problèmes de sécurité lorsqu'ils sont découverts ? • divulguent-elles publiquement des informations concernant leurs processus en réponse à des violations des données ? • cryptent-elles les communications des utilisateurs et les contenus privés afin que les utilisateurs puissent contrôler qui y a accès ?

Liberté d'expression	Les politiques et les engagements des entreprises de technologie font-ils état de moyens concrets par lesquels elles respectent le droit à la liberté d'expression des utilisateurs ?
Modération des contenus	Les entreprises de technologie : • publient-elles des politiques de modération des contenus claires et accessibles ? • informent-elles les utilisateurs des changements apportés à leurs politiques de modération des contenus ? • divulguent-elles et publient-elles régulièrement des données concernant le volume et la nature des mesures prises pour imposer des restrictions à des contenus ou des comptes qui violent les politiques de modération des contenus ? • notifient-elles les utilisateurs lorsqu'elles imposent des restrictions à des contenus ou à des comptes ? Les entreprises de technologie : • divulguent-elles leurs processus pour répondre aux demandes du gouvernement (y compris les ordres judiciaires) et aux demandes privées de suppression de contenus ou de comptes ? • publient-elles régulièrement des données concernant les demandes des gouvernements (y compris les ordres judiciaires) et les demandes de particuliers pour supprimer des contenus ou des comptes
Non-discrimination	Les entreprises de technologie adoptent-elles des politiques de lutte contre la discrimination qui couvrent tous les domaines d'activité, y compris la fourniture de services en ligne et d'autres services numériques ? Les entreprises de technologie assurent-elles une formation et une sensibilisation adéquates au droit à la non-discrimination à l'ensemble de leur personnel et autres agents ?

	Les entreprises de technologie intègrent-elles des évaluations de l'impact sur l'égalité dans la conception et le lancement de leurs produits et services ? • Les entreprises de technologie garantissent-elles que les évaluations de l'impact sur l'égalité constituent un élément essentiel de l'évaluation de leurs produits ? Les entreprises de technologie adoptent-elles des politiques pour garantir qu'un compromis raisonnable soit trouvé lorsque cela est nécessaire ? Les entreprises de technologie garantissent-elles et promeuvent-elles l'égalité d'accès à leurs services ?

3. RÉPARATIONS ET VOIES DE RECOURS

Les États devraient évaluer quelles voies de recours judiciaires et non-judiciaires sont disponibles pour les individus affectés par des entreprises de technologie, ainsi que leur efficacité.

3.1. MÉCANISMES ÉTATIQUES

Mécanismes judiciaires	Existe-t-il des recours judiciaires abordables, rapides et efficaces devant des tribunaux indépendants et impartiaux en cas de violations des droits humains liées au secteur des technologies ?
Accessibilité des voies de recours	L'accès à la justice pour les victimes de violations des droits humains relatives au secteur des technologies est-il possible, compte tenu des différentes situations et besoins, notamment, à titre d'exemple, des barrières géographiques, linguistiques et culturelles ? Les règles du droit en matière de preuves garantissent-elles que les victimes de violations des droits humains relatives au secteur des technologies ne sont pas excessivement entravées dans l'obtention de réparations ?

	• Les règles en matière de preuves dans les procédures civiles sont-elles adaptées pour garantir que lorsque des personnes prétendant avoir été victimes de discrimination établissent des faits permettant de présumer qu'il y a eu discrimination (présomption), il incombe au défendeur de prouver qu'il n'y a pas eu violation du droit à la non-discrimination ? Un soutien financier ou d'autres formes de soutien sont-ils fournis aux personnes ou groupes victimes de violations des droits humains relatives au secteur des technologies, par exemple à travers l'aide juridictionnelle ? Si tel est le cas, qui est éligible pour ces aides financières ou autres formes d'aide ? Des conseils et une assistance juridiques sont-ils disponibles pour les personnes ou les groupes victimes de violations des droits humains relatives au secteur des technologies ? Le cas échéant, qui est éligible à ces formes de conseils et assistance juridiques ? Les plaintes collectives, les actions collectives en justice et d'autres formes d'action de groupe sont-elles possibles en cas de violations des droits humains par le secteur des technologies qui affectent plusieurs personnes ? Des mesures appropriées sont-elles en place pour garantir la protection des personnes contre tout traitement ou conséquence préjudiciable en réponse au dépôt d'une plainte alléguant des violations des droits humains commises par le secteur des technologies ?
Accès à l'information	Des politiques sont-elles en place pour promouvoir l'accès aux mécanismes de plainte étatiques non-judiciaires, tels qu'une autorité compétente en matière de protection des données, une institution nationale des droits humains, ou un médiateur ? Si tel est le cas : • Ces mécanismes sont-ils légitimes, indépendants, accessibles, prévisibles, équitables, transparents et compatibles avec les droits ? Des plaintes ont-elles été déposées auprès des points de contact nationaux de l'OCDE, le cas échéant, au sujet d'entreprises de technologie ?

	Des plaintes ou des préoccupations ont-elles été soulevées auprès de l'institution nationale des droits humains, le cas échéavnt, au sujet d'entreprises de technologies ?
Voies de recours et sanctions	Des mécanismes judiciaires et non-judiciaires constituent-ils des voies de recours efficaces, assorties de sanctions, pour les violations des droits humains relatives au secteur des technologies ? • Ces voies de recours et/ou sanctions sont-elles mises en œuvre de manière efficace ?

3.2. MÉCANISMES NON-ÉTATIQUES

Entreprises de technologie	Les entreprises de technologie offrent-elles des mécanismes de plainte et de recours accessibles pour répondre aux préoccupations des utilisateurs en matière de droits humains ? Ces mécanismes sont-ils légitimes, indépendants, accessibles, prévisibles, équitables, transparents et compatibles avec les droits conformément aux critères d'efficacité prévus par les PDNU ?

3.3. EXTRATERRITORIALITÉ

Extraterritorialité	L'État exerce-t-il une juridiction extraterritoriale sur les actions des entreprises qui ont leur siège dans le pays ou y sont établies, ou sur les actions de leurs filiales, pour des violations des droits humains commises à l'étranger, en particulier en lien avec les activités du secteur des technologies ? Inversement, l'État exerce-t-il un contrôle sur les entreprises de technologie sises à l'étranger qui opèrent dans sa juridiction ? Les entreprises de technologie internationales/étrangères sont-elles soumises à la compétence des tribunaux nationaux ?

LE SECTEUR DES TECHNOLOGIES ET LA LISTE DE CONTRÔLE DES PAN

La liste de contrôle suivante contient les éléments minimums nécessaires pour que les États garantissent que les conséquences du secteur des technologies sur les droits humains sont adéquatement prises en compte alors qu'ils entament le processus d'élaboration, d'évaluation ou de révision d'un PAN. Elle a été conçue sur le modèle de la Liste de contrôle relative aux PAN qui figure dans le Guide.

1. GOUVERNANCE ET RESSOURCES

- Identifier tous les départements gouvernementaux, agences et autres organes et institutions publics concernés, disposant d'un mandat relatif aux technologies, au secteur des technologies et/ou au respect de la vie privée, à la liberté d'expression, et à l'égalité/à la non-discrimination, et veiller à ce qu'ils soient impliqués dans toutes les étapes du processus de PAN. Ils devraient inclure, là où ils existent, non seulement les départements gouvernementaux concernés, mais aussi les organes réglementaires, les institutions nationales des droits humains, les médiateurs et les agences de protection des données.

- Doter ces départements, agences, organes et institutions de ressources adéquates afin de garantir qu'ils sont en mesure de jouer un rôle actif dans la cartographie des parties prenantes, leur consultation, la fourniture d'un renforcement des capacités et leur contribution aux politiques.

2. CARTOGRAPHIE ET PARTICIPATION DES PARTIES PRENANTES

- Dans le cadre d'une cartographie étendue des parties prenantes, dresser une carte spécifique de tous les acteurs non-étatiques experts et/ou intéressés par l'élaboration de politiques relatives aux technologies, au secteur des technologies et/ou au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination.

- Faciliter la participation substantielle de ces acteurs, garantir la représentation d'intérêts multiples et divers et attribuer les ressources et le renforcement des capacités adéquats lorsque cela est nécessaire.

- Identifier ceux qui sont les plus exposés aux effets préjudiciables et discriminatoires pour le respect de la vie privée et la liberté d'expression et garantir qu'ils participent au processus en tenant compte de leurs besoins et vulnérabilités spécifiques.

3. ÉVALUATION DE RÉFÉRENCE NATIONALE

- Garantir que l'organisation qui mène l'ERN est spécialiste du secteur des technologies et des questions relatives au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination.
- Inclure dans l'ERN des questions spécifiques au secteur des technologies et au respect de la vie privée, à la liberté d'expression et à l'égalité/à la non-discrimination, en intégrant les résultats de l'ERN pour le secteur des technologies et les PAN de ce supplément thématique.
- Identifier les lacunes politiques et réglementaires et les principaux risques pour le respect de la vie privée, la liberté d'expression et l'égalité/la non-discrimination.

4. PORTÉE, CONTENU ET PRIORITÉS

- Lors de l'examen de l'étendue de la compétence de l'État, tenir compte de l'importance de l'extraterritorialité en lien avec les activités du secteur des technologies.
- Accorder la priorité aux actions relatives aux conséquences les plus graves du secteur des technologies et garantir que tous les engagements relatifs au secteur sont spécifiques, mesurables, acceptables, réalistes et situés dans le temps.

5. RESPONSABILITÉ ET SUIVI

- Publier des renseignements concernant l'ERN et le PAN dans un format accessible et facile à comprendre, dans des langues comprises par toutes les parties prenantes, en garantissant que toutes les parties prenantes affectées par le secteur des technologies qui ont été consultées comprennent comment leur contribution a été prise en compte.
- Intégrer les parties prenantes incluses dans le cadre de surveillance et de compte rendu sur la mise en œuvre des actions relatives au secteur des technologies dans le PAN, en incluant toute nouvelle politique future.

Annexe 1 : le secteur des technologies dans les PAN existants

ÉTAT	ENGAGEMENT(S)
République tchèque (2017) 	Le PAN tchèque ne contient pas d'engagements spécifiques au secteur des technologies. Il fait référence à la technologie uniquement dans le contexte de l'accès à la justice et des tribunaux, notant que le pouvoir judiciaire « pourrait bénéficier des avantages octroyés par les technologies de pointe ».
Finlande (2014) 	Le PAN finlandais note que « [l]a protection de la vie privée qui est particulièrement liée aux communications électroniques a fait l'objet d'une grande attention lors de récents débats publics » et que « [l]es questions liées au respect de la vie privée relatives aux communications électroniques sont particulièrement importantes en Finlande, où les infrastructures de TIC jouissent d'une position solide ». Le PAN s'engage à organiser « une table ronde (...) sur la manière de garantir la protection de la vie privée en Finlande, avec les autorités, les entreprises des TIC et la société civile ».
Irlande (2017) 	Le PAN irlandais ne contient pas d'engagements spécifiques au secteur des technologies. Il fait cependant référence au fait que l'Irlande compte un grand nombre de multinationales des technologies, et que le Commissaire irlandais pour la protection des données est chargé de superviser une grande quantité de données et a été impliqué dans quelques affaires très médiatisées. Le PAN note que le gouvernement s'engage à soutenir le Commissaire pour la protection des données et qu'il a multiplié par quatre les fonds alloués à ses activités.
Luxembourg (2018) 	Le PAN luxembourgeois ne contient pas d'engagements spécifiques au secteur des technologies. Le PAN note simplement « le risque potentiel d'effets négatifs sur les droits humains que les activités du secteur privé peuvent avoir ... – y compris les technologies de l'information et de la communication – y compris le domaine de l'intelligence artificielle – la protection des données ... ».

Pologne (2017) 	Le PAN polonais prend l'engagement de « rédiger un règlement visant à contrebalancer les restrictions à la liberté de parole, d'une part, et à bloquer les contenus illégaux sur Internet, d'autre part ». Un tel règlement clarifierait la procédure pour notifier et supprimer les contenus illégaux en ligne, et renforcer les garanties légales pour la liberté d'expression dans les activités des fournisseurs de services électroniques.
Suède (2015) 	Le PAN suédois ne contient pas d'engagements spécifiques au secteur des technologies. Cependant, il note que : « La liberté d'Internet et le respect de la vie privée figurent parmi les grands enjeux mondiaux de l'avenir. Il est essentiel pour la Suède que les droits humains qui s'appliquent hors ligne s'appliquent également en ligne ». Le PAN note que la Suède a contribué à garantir que les Principes directeurs de l'OCDE à l'intention des entreprises multinationales appellent désormais les entreprises à promouvoir les droits humains sur Internet, et que la Suède appartient à un groupe de pays qui a présenté des résolutions portant sur la liberté d'Internet au Conseil des droits de l'homme des Nations Unies en 2012 et 2014.
Suisse (2016) 	Le PAN suisse ne contient pas d'engagements spécifiques au secteur des technologies. Il fait cependant référence à la possibilité pour les « biens destinés à la surveillance d'Internet et des communications mobiles » de servir à des fins tant civiles que militaires. Il note par ailleurs que « [l']exportation et le courtage de biens destinés à la surveillance d'Internet et des communications mobiles sont réglementés dans le cadre de la législation sur le contrôle des biens » et que « [le] transfert de biens immatériels, y compris le savoir-faire et la concession de droits y afférents, pour autant qu'ils concernent des biens destinés à la surveillance d'Internet et des communications mobiles, est également soumis à autorisation ».
Thaïlande (2019) 	Le PAN thaïlandais se concentre sur la technologie principalement dans le contexte du travail, notant qu'un défi primordial dans ce domaine consiste à « protéger la main d'œuvre contre l'utilisation des technologies pour remplacer la main d'œuvre ».

	Dans la liste des activités planifiées, le PAN inclut « Adopter des plans ou des mesures pour promouvoir les voies de recours et aider les groupes de travailleurs licenciés conformément aux règlements prévus en matière d'aide ». Le Ministère du travail est chargé de cette activité, pour la période 2019-22.
Royaume-Uni (2013 et 2016) 	Le PAN du Royaume-Uni s'est engagé à « élaborer des directives pour affronter les risques posés par les exportations de technologies de l'information et de la communication qui ne sont pas soumises à un contrôle des exportations, mais qui pourraient avoir des effets sur les droits humains, y compris la liberté d'expression en ligne ». En 2014, le gouvernement du Royaume-Uni, avec techUK, une association professionnelle du secteur des technologies, et l'Institut pour les droits humains et les entreprises, ont publié « Assessing Cyber Security Export Risks: Human Rights and National Security » (Évaluer les risques des exportations pour la cyber-sécurité : droits humains et sécurité nationale).
États-Unis (2016) 	Le PAN des États-Unis note que : « L'effet et l'importance de la conduite des entreprises du secteur des TIC ont pris de l'ampleur, alors que les interactions sociales, commerciales, éducatives et de loisirs ont lieu de plus en plus souvent en ligne ». Le PAN engage le gouvernement des États-Unis à « travailler avec d'autres organismes et parties prenantes, [afin de] mettre au point un mécanisme ordinaire permettant d'identifier, de documenter et de rendre publics les enseignements tirés et les bonnes pratiques relatifs aux actions des entreprises qui promeuvent et protègent les droits humains en ligne ». Il engage également le gouvernement à « promouvoir un engagement permanent entre les parties prenantes concernées afin d'appuyer un dialogue et une collaboration continus au sujet du respect des droits humains dans le secteur des TIC ».

NOTES DE FIN

1 Voir, par exemple, Conseil des droits de l'homme des Nations Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Doc. ONU A/HRC/35/22, 30 mars 2017 ; Conseil des droits de l'homme des Nations Unies, Rapport du Rapporteur spécial sur le droit à la vie privée, Doc. ONU A/HRC/40/63, 27 février 2019 ; Conseil des droits de l'homme des Nations Unies, Rapport du Rapporteur spécial sur les droits de l'homme et l'extrême pauvreté, A/74/493, 11 octobre 2019 et Jørgensen, R. F., Human Rights in the Age of Platforms ed., MIT Press, 2019.

2 International Corporate Accountability Roundtable et Institut danois des droits de l'homme, Guide sur les plans d'action nationaux droits de l'homme et entreprises : édition 2017, 2017, disponible sur : https://www.humanrights.dk/publications/national-action- plans-business-human-rights-toolkit-2017-edition.

3 Pour consulter les chiffres les plus récents, voir Global Naps, disponible sur : https:// globalnaps. org/.

4 Voir ci-dessous à la section 1.3.

5 Une base de données de ces procédures en justice est disponible auprès du Digital Watch Observatory de Geneva Internet Platform, disponible sur : https://dig.watch/trends/uber.

6 Conseil des droits de l'homme des Nations Unies, Résolution 34/7. Le droit à la vie privée à l'ère du numérique, Doc. ONU A/HRC/RES/34/7, 7 avril 2017.

7 Comité des droits de l'homme des Nations Unies, Observation générale n° 18 : non-discrimination, DOC. ONU HRI/GEN/1/Rev.9 (Vol. I), 10 novembre 1989.

8 Pour consulter les chiffres les plus récents, voir Global Naps, disponible sur : https:// globalnaps.org/.

9 En mai 2016, le Royaume-Uni a mis à jour son premier PAN (adopté en 2013), et présenté les mesures adoptées afin de respecter les engagements pris dans le premier PAN, notamment les engagements relatifs au secteur des technologies : HM Government, Good Business : Implementing the UN Guiding Principles on Business and Human Rights, Updated May 2016, disponible sur : https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_ data/file/522805/Good_Business_Implementing_the_UN_Guiding_Principles_on_ Business_and_ Human_Rights_updated_May_2016.pdf.

10 L'absence d'engagements et de mesures SMART dans les PAN de manière générale a été souligné. Voir, par exemple, Institut danois des droits de l'homme, National Action Plans & Business and Human Rights: An Analysis of Plans from 2013 - 2018, 2018, pp. 21-23, disponible sur : https:// mk0globalnapshvllfq4.kinstacdn.com/wp-content/uploads/2018/11/nap-analysis-full-report.pdf.

11 Voir, par exemple, Kreps, S. E., « Social Networks and Technology in the Prevention of Crimes against Humanity » in Rotberg, R.R. (éd.), Mass Atrocity Crimes: Preventing Future Outrages, World Peace Foundation, 2010 ; Hargreaves, C. et Hattotuwa, S., ICTs for the Prevention of Mass Atrocity Crimes, ICT for Peace Foundation, octobre 2010, disponible sur : http://ict4peace.org/wp-content/ uploads/2010/11/ICTs-for-the-Prevention-of-Mass-Atrocity-Crimes1.pdf.

12 Voir, par exemple, Amnesty International, Surveillance Giants, 2019, disponible sur : https:// www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/

13 Conseil des droits de l'homme des Nations Unies, Rapport du Rapporteur spécial sur le droit à la vie privée, Doc. ONU A/72/43103, 19 octobre 2017, § 75.

14 Ibid.

15 Voir, par exemple, Amnesty International, Surveillance Giants, 2019, disponible sur : https:// www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/.

16 Voir, par exemple, la recherche menée par le projet Human Rights, Big Data and Technology de la University of Essex, disponible sur : https://www.hrbdt.ac.uk/.

17 Voir Borgesius, F. Z., Discrimination, Artificial Intelligence, and Algorithmic Decision-Making,

Direction générale de la démocratie, Conseil de l'Europe, 2018, disponible sur : https://rm.coe.int/discrimination- artificial-intelligence-and-algorithmic-decision-making/1680925d73.
18 Ibid.
19 Dastin, J., « Amazon scraps secret AI recruiting tool that showed bias against women », Reuters, 10 octobre 2018, disponible sur : https://www.reuters.com/article/us-amazon-com-jobs-automation-in...-ai-recruiting-tool-thatshowed-bias-against-women-idUSKCN1MK08G.
20 Ibid.
21 Commission fédérale du commerce, Data Brokers: A Call for Transparency and Accountability, mai 2014, disponible sur : https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.
22 Angwin, J., Tobin, A. et Varner, M., « Facebook (Still) Letting Housing Advertisers Exclude Users by Race », ProPublica, novembre 2017, disponible sur : https://www.propublica.org/article/facebook-advertising-discrimination-housing- race-sex-national-origin. En mars 2019, Facebook annonçait des restrictions aux options de ciblage pour les annonces concernant des logements, des emplois ou des crédits aux États-Unis, dans le cadre d'un règlement avec des organisations de défense des droits civils.
23 Angwin, J. et al., « Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks », ProPublica, 23 mai 2016, disponible sur : https://www.ProPublica.org/article/machine-bias-riskassessments-in-criminal-sentencing.
24 Confessore, N., « Cambridge Analytica and Facebook: the scandal so far », The New York Times, 4 avril 2018, disponible sur : https://www.nytimes.com/2018/04/04/ us/politics/cambridge-analytica-scandal-fallout.html.
25 Perlroth, N., « All 3 Billion Yahoo Accounts Were Affected by 2013 Attack », The New York Times, 3 octobre 2017, disponible sur : https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.
26 Human Rights Watch, Dark Side Secret Origins of Evidence in US Criminal Cases, 9 janvier 2018, disponible sur https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases.
27 Voir la liste des affaires sur le site du Centre de ressources sur les entreprises et les droits de l'homme, Corporate Legal Accountability Hub, disponible sur https://www.business-humanrights.org/en/corporate-legal-accountability/case-profiles/industry/technology.
28 Human Rights Watch, Chine : Big Data Fuels Crackdown in Minority Region, disponible sur : https://www.hrw.org/news/2018/02/26/china-big-data-fuels-crackdown-minority-region.
29 Freedom House, Freedom on the Net 2018, The Rise of Digital Authoritarianism, disponible sur : https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.
30 Ibid.
31 Voir https://necessaryandproportionate.org/principles.
32 Voir https://www.reformgovernmentsurveillance.com.
33 Five Country Ministerial, Statement of Principles on Access to Evidence and Encryption, disponible sur : https://www.ag.gov.au/About/CommitteesandCouncils/Documents/joint-statement-principles-access-evidence.pdf.
34 Comité européen de la protection des données, Avis 5/2019 relatif aux interactions entre la directive « vie privée et communications électroniques et le RGPD, en particulier en ce qui concerne la compétence, les missions et les pouvoirs des autorités de la protection des données, 12 mars 2019, disponible sur : https://edpb. europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_ interplay_en_0.pdf.
35 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre

circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, disponible sur : https://eur-lex.europa.eu/eli/ dir/2016/680/oj.v

36 Comité européen de la protection des données, 1 year GDPR - taking stock, 22 mai 2019, disponible sur : https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en.

37 Commission Nationale de l'Informatique et des Libertés, The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC, 21 janvier 2019, disponible sur : https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

38 Voir la communication du Equal Rights Trust au Rapporteur spécial des Nations Unies sur les formes contemporaines de racisme, de discrimination raciale, de xénophobie et de l'intolérance qui y est associée au sujet des graves menaces structurelles que les nouvelles technologies de l'information telles que les mégadonnées, l'apprentissage automatique et l'IA posent pour les droits à la non-discrimination et à l'égalité raciale et les principes et normes des droits humains, disponible sur https://www.equalrightstrust.org/news/equal-rights-trusts-submission-un-special-rapporteur-contemporary-forms-racism.

39 Access Now, The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems, disponible sur : https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/.

40 Conseil des droits de l'homme des Nations Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Doc. ONU A/73/348, 29 août 2018, § 12

41 Voir, par exemple, l'étude de 2019 mandatée par le Département thématique des droits des citoyens et des affaires constitutionnelles du Parlement européen, Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States, février 2019, disponible sur : https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf.

42 Amnesty International, Toxic Twitter: A Toxic Place for Women, mars 2018, disponible sur : https://www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

43 Conseil des droits de l'homme des Nations Unies, Rapport de la mission internationale indépendante d'établissement des faits sur le Myanmar, Doc. ONU A/HRC/39/64, 12 septembre 2019, § 74. Le rapport fait référence de manière explicite au rôle de Facebook dans la diffusion de discours de haine à l'égard des Rohingya au Myanmar.

44 Ibid.

45 Access Now, The State of Internet Shutdowns Around the World: #KeepItOn Report, disponible sur : https://www.accessnow.org/keepiton/.

46 Ibid.

47 Global Network Initiative, Disconnected: A Human Rights-Based Approach to Network Disruptions, juin 2018, disponible sur : https://globalnetworkinitiative.org/wp-content/uploads/2018/06/Disconnected-Report-Network-Disruptions.pdf.

48 Weidmann, N. B., Benitez-Baleato, S., Hunziker, P., Glatz, E. et Dimitropoulos, X. (2016), Digital discrimination: Political bias in Internet service provision across ethnic groups. Science, 353(6304), 1151-1155

49 Conseil des droits de l'homme des Nations Unies, Résolution 32/13. La promotion, la protection et l'exercice des droits de l'homme sur Internet, Doc. ONU A/HRC/RES/32/13, 18 juillet 2016.

50 Voir, par exemple, Conseil des droits de l'homme des Nations Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Doc. ONU A/HRC/35/22, 30 mars 2017.

51 Electronic Frontier Foundation, NGO Community Urges ICANN to Scrutinize the .ORG Sale, mars 2020, 9 mars 2020, disponible sur : https://www.eff.org/deeplinks/2020/03/ngo-community-urges-icann-scrutinize-org-sale.

52 Population mondiale ayant accès à Internet en janvier 2020, https://www.statista.com/statistics/617136/digital-population-worldwide/.
53 Conseil des droits de l'homme des Nations Unies, Résolution 32/13. La promotion, la protection et l'exercice des droits de l'homme sur Internet, Doc. ONU A/HRC/RES/32/13, 18 juillet 2016.
54 BBC, Websites to be fined over 'online harms' under new proposals, 8 avril 2019, disponible sur : https://www.bbc.com/news/technology-47826946.
55 Freedom on the Net 2018, The Rise of Digital Authoritarianism, p. 2, disponible sur https://freedomhouse.org/sites/default/files/FOTN_2018_Final%20 Booklet_11_1_2018.pdf
56 Voir, par exemple, Electronic Frontier Foundation, EFF, Human Rights Watch, and Over 70 Civil Society Groups Ask Mark Zuckerberg to Provide All Users with Mechanism to Appeal Content Censorship on Facebook, 13 novembre 2018, disponible sur : https://www.eff.org/press/releases/eff-human-rights-watch-and-over-70-civil-society-groups-ask-mark-zuckerberg-provide.
57 Conseil des droits de l'homme des Nations Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Doc. ONU A/HRC/38/35, 6 avril 2018, § 27.
58 Voir, par exemple, Article 19, Facebook Community Standards: Analysis against international standards on freedom of expression, 30 juillet 2018, disponible sur https://www.article19.org/resources/facebook-community-standards-analysis-against-international-standards-on-freedom-of-expression/ ; Article 19, Twitter Rules: Analysis against international standards on freedom of expression, 6 septembre 2018, disponible sur https://www.article19.org/resources/twitter-rules-analysis-against-international-standards-on-freedom-of-expression.
59 Conseil des droits de l'homme des Nations Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Doc. ONU A/73/348, 29 août 2018, § 15.
60 Voir https://santaclaraprinciples.org.
61 Voir https://www.manilaprinciples.org.
62 Conseil des droits de l'homme des Nations Unies, Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Doc. ONU A/HRC/38/35, 6 avril 2018, § 41-63.
63 Ibid., § 48.
64 Article 19, The Social Media Councils Consultation Paper, juin 2019, disponible sur https://www.article19.org/wp-content/uploads/2019/06/A19-SMC-Consultation-paper-2019-v05.pdf
65 Facebook, Preparing the Way Forward for Facebook's Oversight Board, 28 janvier 2020, disponible sur https://about.fb.com/news/2020/01/facebooks-oversight-board/.
66 Horowitz, J., In Italian Schools, Reading, Writing and Recognizing Fake News, The New York Times, 18 octobre 2017, disponible sur : https://www.nytimes.com/2017/10/18/world/europe/italy-fake-news.html.
67 Apple, Apple teams with media literacy programs in the US and Europe, 19 mars 2019, disponible sur : https://www.apple.com/uk/newsroom/2019/03/apple-teams-with-media-literacy-programs-in-the-us-and-europe/.
68 Freedom House, Freedom on the Net 2018, The Rise of Digital Authoritarianism, disponible sur : https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism.
69 Ibid