livre blanc 16

défis du numérique pour le droit international

coordinateurs

Anne-Thida Norodom

Professeur de droit public à l'Université Paris Cité, France

Aude Géry

Chercheuse postdoctorale à GEODE, Université Paris 8, France

François Delerue

Professeur assistant en droit, IE University, Espagne

assistant / rapporteur

Stefanos Argyros

Assistant de recherche à GEODE, Université Paris 8, France

comité de pilotage

(par ordre alphabétique)

Eyal Benvenisti

Professeur Whewell de droit international et Directeur du Centre Lauterpacht de droit international, Université de Cambridge, Royaume-Uni

Nehal Bhuta

Professeur et titulaire de la chaire de droit international public, Université d'Édimbourg ; codirecteur du Centre d'Édimbourg pour le droit international et mondial, Royaume-Uni

informations auteurs

Duncan B. Hollis
Professeur de droit Laura H. Carnell à la Temple Law School et chercheur non résident à la Carnegie Endowment for International Peace, États-Unis

Zhixiong Huang
Changjiang Outstanding Young Scholar, professeur et vice-doyen de la faculté de droit ainsi que directeur exécutif de l'Institut de la cyber-gouvernance, Université de Wuhan, Chine

Nnenna Ifeanyi-Ajufo
Senior lecturer en droit et technologie à la faculté de droit de l'université de Swansea, Royaume-Uni

Eduard Ivanov
Professeur de droit international à la National Research University Higher School of Economics, Moscou, Russie ;

Joanna Kulesza
Professeur de droit international et de gouvernance de l'Internet, Université de Lodz, Pologne

Clea Strydom
Chercheuse indépendante, Etudiante en troisième cycle, Université de Johannesburg, Afrique du Sud

Jennifer Tridgell
Chercheuse principale pour le rapporteur spécial des Nations unies sur la liberté de religion ou de croyance (bureau externe), Responsable des médias de l'Association de droit international (comité de gestion), Royaume-Uni

Robert Young
Conseiller juridique, division du droit pénal, sécuritaire et diplomatique, Affaires mondiales, Canada

Introduction

Objectifs et structure

Les célébrations du 150ème anniversaire de l'ILA/ADI s'articulent autour de deux questions centrales : premièrement, dans quelle société internationale voulons-nous vivre en 2050 ? Et, deuxièmement, pour réaliser cette société internationale, de quel droit international avons-nous besoin ? La branche française de l'ILA/ADI, responsable de l'organisation de ces célébrations, a choisi une variété de sujets pour explorer ces questions, parmi lesquels les défis que représentent les technologies numériques émergentes pour le droit international. Le Livre blanc sur les défis du numérique pour le droit international vise à fournir une vue d'ensemble des règles et principes de droit international existants concernant les données numériques, la sécurité numérique et l'intelligence artificielle (IA) (Partie 1, Exposé des faits), à identifier certains des principaux défis factuels susceptibles d'émerger à l'avenir (Partie 2, Défis) et à réfléchir à la question de savoir si et comment le droit international peut ou doit être utilisé pour y répondre (Partie 3, Questions). Le Livre blanc n'est pas un exercice académique, mais vise plutôt à mettre en lumière certains des principaux défis présents et à venir du numérique et leurs implications potentielles pour le droit international[1]. L'objectif est d'anticiper certaines des questions de droit international qui seront soulevées par les développements technologiques à venir, et de les rendre intelligibles à toutes les parties prenantes intéressées, qu'elles soient ou non spécialisées dans le droit international ou le droit du numérique.

Les thèmes du livre blanc

Le comité a articulé ses travaux sur les défis du numérique autour de trois sujets interdépendants - les données, la sécurité et l'intelligence artificielle - sur la base d'un double raisonnement : d'une part, ces sujets englobent certains des principaux défis qui émergent à l'aube des technologies de l'information et de la communication (TIC) et, d'autre part, ils soulèvent diverses questions de droit international qui intéressent les juristes internationaux et d'autres acteurs clés. Le comité n'a pas pour objectif de fournir une liste exhaustive des défis. Les sujets sont abordés principalement sous l'angle du droit public, bien que

Note 1 Les exigences académiques classiques, notamment en termes de référencement doctrinal, ne seront donc pas respectées. Une bibliographie sera mise à disposition sur le site internet du 150ème anniversaire de l'ILA/ADI.

certaines utilisations privées et commerciales des technologies émergentes (par exemple, la commercialisation des données) puissent également être envisagées. De nombreuses tendances technologiques émergentes, telles que le métavers ou le développement de monnaies numériques par exemple, ne seront discutées que dans la mesure où elles sont liées aux trois principaux sujets identifiés ci-dessus. Certains de ces nouveaux développements peuvent également être abordés dans les livres blancs d'autres comités, eu égard à l'utilisation dominante des technologies numériques et leur impact sur une variété de domaines juridiques internationaux.

1. Les données numériques

Les données numériques sont sans aucun doute l'une des questions les plus importantes du cyberespace mais aussi du droit international du numérique. Elles constituent tout d'abord la base indispensable de nombreuses technologies et innovations numériques, comme l'IA par exemple. C'est sur elles que les acteurs privés tels que les plateformes numériques ou les réseaux sociaux ont bâti leur modèle économique. La puissance de ces acteurs privés a fait des données numériques un enjeu politique, car elles sont considérées comme une ressource exploitable mais qui doit aussi être protégée. Les données sont devenues un enjeu stratégique dans la mesure où elles se situent au cœur des rapports de force entre acteurs privés et acteurs publics mais aussi au sein de chacune de ces catégories. L'importance des données numériques, notamment pour la protection de la vie privée, justifie qu'elles soient un objet de droit et notamment de droit international. Les données numériques peuvent également être un outil pour le droit facilitant la collecte de preuves de la pratique étatique ou de l'*opinio juris*, par exemple. Les données numériques sont plurielles de par leur nature (personnelles, sensibles, publiques, etc.) et surtout par les usages qui peuvent en être faits (*open data*, finalités commerciales, recherche, etc.).

2. La sécurité numérique

Même si le développement des technologies de l'information et de la communication est présenté comme un moyen d'accroître la sécurité des États et des citoyens, il a rapidement conduit à leur exploitation à des activités malveillantes par des États et des acteurs non étatiques, allant de la diffusion d'informations manipulées à des cyberopérations destructrices. En effet, l'ubiquité et la capacité d'agir tout en cachant son

identité ont été exploitées à différentes fins : espionnage, déstabilisation, sabotage, profit économique. Les relations entre les États et les acteurs non étatiques sont aussi parfois difficiles à distinguer. L'interconnexion des réseaux et le rôle des acteurs non étatiques dans leur développement et leur gestion font donc de la sécurité numérique une question internationale par nature, qui intéresse les citoyens, le secteur privé et les États. A ce titre, la sécurité numérique est devenue une préoccupation majeure pour la sécurité internationale, le développement économique et social ainsi que la sécurité humaine. Elle constitue également une condition pour atteindre les Objectifs de Développement Durable (ODD).

3. L'intelligence artificielle

L'intelligence artificielle peut être comprise comme une méthode d'apprentissage qui sous-tend une variété de technologies hétérogènes (reconnaissance faciale, armes autonomes létales, etc.) et d'usages (à des fins commerciales ou militaires). L'un des aspects importants de l'IA est l'apprentissage automatique, grâce auquel les algorithmes s'améliorent automatiquement par l'expérience. Cette dimension évolutive peut créer un certain défi quant à la conformité de ces algorithmes avec le droit international. Le développement rapide de l'intelligence artificielle s'accompagne de nombreux défis, dont certains concernent également le droit international et les relations internationales. Contrairement au développement du cyberespace, l'intelligence artificielle n'est pas perçue comme un nouveau domaine en soi et l'applicabilité du droit international en général n'est donc pas remise en question. Néanmoins, elle soulève de nombreuses questions, notamment en termes d'attribution, de responsabilité et de respect des règles et principes du droit international. Il est intéressant de noter que certains aspects de l'IA ont reçu beaucoup d'attention alors que d'autres restent relativement inexplorés. Par exemple, les systèmes d'armes létaux autonomes (SALA, LAWS en anglais) ont été largement discutés dans la littérature et ont également fait l'objet de divers processus interétatiques, alors que l'impact de l'intelligence artificielle sur les actes et les comportements dans le cyberespace a été moins traité. Il existe des chevauchements et une fertilisation croisée entre les approches éthiques et juridiques de la réglementation de l'IA. Pourtant, une distinction claire paraît pertinente dans de nombreux cas. En outre, les technologies de l'IA offrent de nouveaux moyens de contribuer au développement et à l'application du droit international. Elles sont donc susceptibles d'avoir un impact sur la substance du droit.

1.

état des lieux

Au cours des dernières décennies, les États et les organisations internationales ont de plus en plus concentré leur attention et leurs ressources sur les défis et les opportunités découlant de l'utilisation des nouvelles technologies numériques. Cette première partie présente un aperçu des règles et processus internationaux les plus importants dans les domaines des données numériques, de la sécurité numérique et de l'intelligence artificielle. Pour chacun de ces trois sujets, les principaux règles et processus de droit international applicables sont identifiés, accompagnés d'un bref commentaire sur leurs principales caractéristiques (par exemple, leur répartition géographique, leur statut et contenu juridiques, la branche du droit à laquelle ils appartiennent, etc.). Les exemples que nous abordons ne sont pas exhaustifs et ne visent qu'à fournir un échantillon de certaines des règles existantes les plus pertinentes.

Étant donné que de nombreux débats et processus internationaux actuels portent déjà sur la manière dont le droit international s'applique au cyberespace et sur l'élaboration de normes de comportement responsable des États, il a été décidé de donner un aperçu des controverses existantes sur l'application du droit international (par exemple, les désaccords sur la signification de la souveraineté, de la diligence raisonnable, de la non-ingérence, etc.), en distinguant les concepts globalement acceptés de ceux qui sont encore controversés, sans chercher à les résoudre. L'objectif est de donner aux lecteurs une idée des règles qui existent (le cas échéant) pour chaque sujet, et de prendre note des désaccords existants sur leur application. Compte tenu du grand nombre de règles de droit international applicables aux données numériques, à la sécurité numérique et à l'IA, l'aperçu fourni ici ne vise pas à être exhaustif, mais plutôt à fournir une connaissance générale des débats actuels. L'« état des lieux » qui en résulte constitue une base pour évaluer l'adéquation des règles et processus existants à la lumière des défis et des questions identifiés dans les parties 2 et 3.

La principale conclusion qui se dégage des règles et processus identifiés dans l'exposé des faits est celle d'une fragmentation géographique, technique et juridique. S'il existe un accord substantiel sur l'applicabilité du droit international dans le domaine numérique, des désaccords importants sur le statut, l'interprétation et l'application des règles existantes subsistent. En outre, les règles spécifiques à chacun de ces trois sujets sont souvent non contraignantes, inégalement réparties ou concentrées dans des branches particulières du droit international.

1. Les données numériques

1.1. Les principaux principes et règles du droit international

Par principe, l'ensemble du droit international général s'applique aux données numériques, ainsi que toutes les branches pertinentes du droit international, telles que le droit international humanitaire, le droit international des droits de l'homme (notamment les droits à la vie privée, à la liberté d'expression et à l'accès à l'information) et le droit commercial international.

Divers processus techniques et politiques spécifiquement consacrés aux données numériques ont également été menés à bien ou sont en cours dans de nombreuses organisations internationales. Les Nations unies, l'Union européenne, l'Organisation pour la coopération et le développement économique, l'Union africaine, la Communauté économique des États de l'Afrique de l'Ouest et d'autres organisations sous-régionales en Afrique, le G7 et le G20, l'Organisation mondiale du commerce se penchent tous sur les questions relatives aux données numériques, conformément à leurs mandats respectifs.

Exemples d'instruments adoptés par des organisations ou des processus internationaux

- Union africaine : la Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel ;
- ASEAN : clauses contractuelles types de l'ASEAN pour les flux de données transfrontalier ;
- Accords de libre-échange bilatéraux et multilatéraux : UE-Japon, UE-Canada CETA, etc. ;
- Union européenne : Règlement général sur la protection des données (RGPD)
- Conseil de l'Europe : la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STCE n° 108) ;
- OCDE : Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel ; Déclaration sur les flux transfrontières de données ; Recommandation du Conseil sur la gouvernance des

données de santé ; Déclaration de Séoul sur le futur de l'économie Internet ;

- G7 : Declarations on the free flow of data, including the UK 2021 G7 Roadmap for Cooperation on Data Free Flow with Trust, the UK 2021 G7 Digital Trade Principles, the G7 2022 Action Plan Promoting Data Free Flow with Trust ;
- G20 : 2019 G20 Osaka Leader's Declaration ;
- Accords exécutifs sur l'accès transfrontalier aux preuves électroniques, par exemple les accords États-Unis/Royaume-Uni et États-Unis/Australie ; lois sur la protection des données militaires et un grand nombre d'autres lois nationales, etc ;
- Cadre ibéro-américain de protection des données : par exemple, le guide sur les transferts internationaux de données ;
- OMC : voir le programme de travail sur le commerce électronique ;
- Assemblée générale des Nations Unies : voir les résolutions sur le droit à la vie privée à l'ère numérique.

1.2. Aperçu des règles existantes

Le droit international existant en matière de données numériques en est encore à ses balbutiements. À l'exception du droit de l'Union européenne, il existe peu de règles contraignantes de droit international spécifiquement consacrées aux données numériques. En effet, la plupart des instruments universels, régionaux ou bilatéraux qui traitent des données numériques le font soit par interprétation, soit en intégrant les données numériques dans un champ d'application matériel plus large, par exemple dans le cadre du droit à la vie privée consacré par les instruments relatifs aux droits de l'homme. Bien que des cadres internationaux de protection des données existent depuis les années 70 grâce aux travaux de l'OCDE et du Conseil de l'Europe, la plupart des règles spécifiquement consacrées aux données numériques ont été adoptées dans des contextes limités, principalement dans les domaines de la protection des données, de la cybercriminalité et du droit commercial (par exemple, par le biais de l'Accord général sur le commerce des services ou de l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce).

Contrairement au domaine de la sécurité numérique, on observe un passage progressif des premiers instruments non contraignants (par exemple, les lignes directrices de l'OCDE sur la

protection de la vie privée) vers des instruments contraignants (par exemple, le Règlement général sur la protection des données de l'Union européenne (RGPD)), même si la plupart des règles se trouvent encore dans le droit national. Au niveau international, il existe très peu d'instruments spécifiquement consacrés aux données numériques. La plupart des règles internationales existantes sur les données numériques se trouvent dans le droit régional de l'UE, de l'Union africaine (par exemple, la Convention de Malabo, même si elle n'est pas encore entrée en vigueur), du Conseil de l'Europe (Convention 108 sur la protection des données ; Convention sur la cybercriminalité), de l'OCDE, de la CEDEAO et d'autres organisations internationales régionales ou sous-régionales en Afrique et en Asie. Les accords et traités exécutifs bilatéraux constituent également une source importante de règles existantes.

1.3. Aperçu de règles consensuelles et règles litigieuses

En principe, il existe un large consensus sur l'applicabilité du droit international général et des différentes branches pertinentes du droit international (droit international des droits de l'homme, droit international humanitaire, droit de la responsabilité internationale, etc.) au domaine numérique, y compris aux questions relatives aux données numériques. Il existe également un consensus relatif concernant les principales caractéristiques de la protection des données (droit de rectification, organes de contrôle, etc.).

On observe cependant de nombreuses différences culturelles et juridiques dans la conceptualisation des données personnelles, la notion de vie privée et l'application du droit existant en matière de droits de l'homme. Les approches nationales et régionales de la protection des données varient considérablement d'une juridiction à l'autre, ce qui contribue à accroître la fragmentation juridique. Il existe également de nombreux désaccords sur l'accès transfrontalier aux données dans le domaine de la cybercriminalité et au regard de la compétence, notamment en ce qui concerne les normes appropriées de protection des données (par exemple, les affaires *Schrems*) et les critères d'attribution de compétence (par exemple, le *Cloud Act*, les preuves électroniques, les droits européen, chinois et russe). Enfin, l'idéal d'une libre circulation des données est confronté à un nombre croissant d'obstacles qui soulèvent des défis importants du point de vue du droit commercial.

2. La sécurité numérique

2.1. Principaux principes et règles du droit international

Par principe, l'ensemble du droit international général ainsi que toutes les branches pertinentes du droit international s'appliquent à la sécurité numérique.

Divers processus techniques et politiques spécifiquement consacrés à la sécurité numérique ont également été menés à bien ou sont en cours dans de nombreuses organisations internationales, parmi lesquelles les Nations unies (Programme mondial des Nations unies sur la cybercriminalité sous l'égide de l'UNODC ; processus de l'OEWG et du GGE des Nations unies[2] ; comité intergouvernemental spécial d'experts à composition non limitée chargé d'élaborer une convention internationale générale sur la lutte contre l'utilisation des TIC à des fins criminelles), l'UIT (Centre régional de cybersécurité de l'UIT ; groupe d'étude de l'UIT-T dans le secteur de la normalisation des télécommunications, indice mondial de cybersécurité, etc.), l'OCDE (groupe de travail sur la sécurité et la vie privée dans l'économie numérique), l'OSCE, les organisations régionales et sous-régionales (OEA, UA, ASEAN). Des initiatives multipartites sont également en cours dans le domaine du terrorisme, de la cybersécurité ou des discours de haine (Tech Against Terrorism, Global Internet Forum to Counter Terrorism, l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, l'Appel de Christchurch).

Note 2 Selon la pratique générale, seront conservés ici les acronymes anglais: Open-ended Working Group et Group of Governmental Experts.

Exemples d'instruments adoptés par des organisations ou des processus internationaux

- ASEAN : Declaration to fight cybercrime; ASEAN Leaders' Statement on Cybersecurity Cooperation ;
- Ligue arabe : Arab Convention on Combating Information Technology Offenses ;

- Conseil de l'Europe : Convention sur la cybercriminalité et ses protocoles additionnels ; Déclaration du Comité des ministres concernant la viabilité financière du journalisme de qualité à l'ère numérique Decl(13/02/2019)2 ; Recommandation CM/Rec(2018)2 du Comité des ministres aux États membres sur les rôles et les responsabilités des intermédiaires d'internet ; Déclaration du Comité des ministres sur les capacités de manipulation des processus algorithmiques Decl(13/02/2019)1 ;
- G7 : Engagement de Charlevoix pour la défense de la démocratie contre les menaces étrangères, Actions du G7 pour renforcer la cybersécurité des entreprises ;
- UIT : résolutions, par exemple Résolution sur le renforcement du rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technologies de l'information et de la communication REV. DUBAI, 2018 ; et des recommandations, par exemple la Recommandation UIT-T X.1500 - Amendement 12 (2011 Techniques révisées d'échange d'informations sur la cybersécurité structurées ;
- OSCE : mesures de confiance, documents PC.DEC/1106 et PC.DEC/1202 ;
- Appel de Paris pour la confiance et la sécurité dans le cyberespace ;
- Résolutions de l'Assemblée générale des Nations unies : sur la création d'une culture mondiale de la cybersécurité (par exemple, A/RES/57/239) ; sur la lutte contre la désinformation (par exemple, A/RES/76/227) ; sur la promotion et la protection des droits de l'homme et des libertés fondamentales (par exemple, A/RES/75/176) ; sur les progrès de l'informatique et des télécommunications dans le contexte de la sécurité internationale et sur la promotion du comportement responsable des États (par exemple, A/RES/76/19) ;
- Résolutions du conseil de sécurité de l'ONU : sur le terrorisme, notamment sur la propagande terroriste et les discours de haine en ligne (par exemple, la résolution S/RES/2354 (2017) sur la mise en œuvre du Cadre international global de lutte contre les discours terroristes), sur la sécurité des infrastructures critiques (S/RES/2341(2017)) ;
- Rapports du Groupe d'experts gouvernementaux et du Groupe de travail des Nations unies sur la cybersécurité : A/65/201, A/68/98, A/70/174, A/75/816, A/76/135 ;

- UNHCR : résolutions sur la promotion, la protection et l'exercice des droits de l'homme sur Internet, par exemple, A/HRC/RES/38/7 et A/HRC/RES/47/16 ;
- OMS : déclaration commune de l'OMS et al. sur la gestion de l'infodémie sur la COVID-19 : Promouvoir des comportements sains et atténuer les effets néfastes de la diffusion d'informations fausses et trompeuses ;
- Organisation de coopération de Shanghai : Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization ;
- OEA : voir le travail du CICTE, le Comité interaméricain contre le terrorisme ; les résolutions de l'Assemblée générale, par exemple, AG/RES. 1939 (XXXIII-O/03) et AG/RES. 2004 (XXXIV-O/04)) ; les travaux du Comité judiciaire interaméricain sur le droit international et les cyber-opérations des États ;
- Arrangement de Wassenaar : dispositions relatives aux logiciels d'intrusion sur la liste des biens et technologies à double usage.

2.2. Aperçu des règles existantes

Il existe peu de règles internationales contraignantes spécifiquement dédiées à la sécurité numérique, sauf dans le domaine de la cybercriminalité et dans le droit européen. Cependant, de nombreux instruments contraignants non spécifiquement dédiés à la sécurité numérique sont également applicables. On trouve des règles non spécifiques à la sécurité numérique tant au niveau universel (par exemple, l'interdiction du recours à la force, le droit international humanitaire, le droit international des droits de l'homme, le droit international de l'espace, le droit international des télécommunications) qu'au niveau régional.

La cybercriminalité et la sécurité internationale sont les deux principaux domaines dans lesquels nous trouvons des dispositions consacrées à la sécurité numérique. Des dispositions pertinentes peuvent également être identifiées dans les instruments traitant des activités terroristes. Le droit commercial pourrait également s'intéresser de plus en plus à la sécurité numérique, d'autant plus que l'imposition d'exigences de sécurité dans le domaine des TIC peut constituer des obstacles au commerce et violer les règles commerciales existantes. Contrairement au domaine de la cybersécurité, les opérations d'information n'ont pas encore été abordées par la plupart des initiatives normatives, sauf dans la perspective de la lutte contre la

propagande terroriste, et peut-être aussi dans celle des droits de l'homme (notamment les droits à des élections libres et équitables et à la liberté d'information/d'accès à l'information) et de la souveraineté (déstabilisation des régimes politiques).

2.3. Aperçu des règles consensuelles ou litigieuses

En principe, il existe un large consensus sur l'applicabilité du droit international général et des différentes branches du droit international (droit international des droits de l'homme, droit international humanitaire, droit de la responsabilité internationale, etc.) dans le domaine de la sécurité numérique. Pourtant, malgré ce consensus, de nombreuses questions sur l'interprétation et l'application du droit international au cyberespace restent litigieuses. Il existe des désaccords non résolus sur des questions concernant la substance du droit international (par exemple, sur l'existence de certaines règles ou principes de droit international dans le cyberespace, tels que la vigilance (*due diligence*) et la souveraineté), l'interprétation de ses règles et normes (seuils, élément de coercition et non-intervention, données en tant qu'objet protégé en vertu du droit des conflits armés (DCA), effets non physiques et recours à la force/attaque armée) et sur leur mise en œuvre (attribution, etc.) dans le cyberespace. L'extension du droit de la responsabilité de l'Etat aux activités numériques a en particulier fait l'objet de nombreux désaccords, notamment sur les questions d'attribution, de contre-mesures et de défense. Dans l'ensemble, le traitement de l'application du droit international à la sécurité numérique a été inégal : on s'est beaucoup attaché à résoudre les désaccords sur certaines règles juridiques internationales (par exemple, sur l'interdiction du recours à la force), tandis que d'autres ont été traitées de manière beaucoup plus superficielle (par exemple, les droits de l'homme)[3].

Note 3 Par exemple, sur les 184 règles du *Manuel de Tallinn 2.0 sur le droit international applicable aux cyberopérations* (CUP 2017), seules cinq étaient consacrées aux questions de droits de l'homme.

3. L'intelligence artificielle

3.1. Principaux principes et règles du droit international

Les discussions internationales et les instruments normatifs sur l'IA se concentrent dans une large mesure sur les questions éthiques, qui sont souvent confondues avec les questions juridiques. La recommandation de l'UNESCO sur l'éthique de l'IA est un excellent exemple d'instrument abordant l'IA sous un angle éthique, tout en contenant des dispositions juridiques détaillées sur la substance. Les sections suivantes donnent un aperçu des instruments juridiques internationaux existants sur l'IA, sans s'attarder sur ses implications éthiques.

Au niveau international, il existe peu de règles contraignantes, voire aucune, spécifiquement consacrées à l'IA. Il existe cependant des normes internationales relatives aux droits de l'homme qui peuvent être directement appliquées à l'IA. Les droits concernés peuvent inclure la liberté de pensée, le respect de la vie privée et la non-discrimination (par exemple, les droits consacrés par le Pacte international relatif aux droits civils et politiques, le Pacte international relatif aux droits économiques et sociaux, la Convention européenne des droits de l'homme, la Convention interaméricaine des droits de l'homme, la Charte africaine des droits de l'homme et des peuples, la Convention d'Istanbul contre la violence à l'égard des femmes, etc.), ainsi que d'autres règles internationales générales couvrant l'utilisation des technologies par les États. Lorsque les technologies de l'information sont déjà déployées dans le cadre d'hostilités, les questions relatives à l'interdiction du recours à la force et au droit des conflits armés, ainsi que d'autres règles connexes du droit international, sont également pertinentes.

En plus de ces instruments généraux, un nombre croissant d'organisations internationales adoptent des règles spécifiquement dédiées à l'intelligence artificielle, parmi lesquelles le Conseil de l'Europe, l'OCDE (recommandation du Conseil sur l'intelligence artificielle), l'UNESCO (recommandation de la Conférence générale sur l'éthique de l'IA), l'UIT (notamment à travers ses sommets *AI for Good*). Aux Nations unies, les discussions sur les implications de l'intelligence artificielle en matière de sécurité internationale se sont concentrées sur le développement de systèmes d'armes létaux autonomes (SALA). La question a été inscrite à l'ordre du jour des réunions des Hautes Parties contractantes à la Convention sur l'interdiction ou la limitation de l'emploi de certaines armes classiques (CCAC) en

2013. Après quelques réunions informelles, les discussions ont pris une forme similaire à celles relatives à la cybersécurité internationale : un Groupe d'experts gouvernementaux (GEG) a été créé en 2016, et a adopté 11 principes directeurs sur les SALA en décembre 2019. Par ces principes, le GEG a affirmé l'applicabilité du droit international et du droit international humanitaire en particulier, ainsi qu'un ensemble de principes éthiques et non contraignants. Dans le contexte de ce Livre blanc, il convient de souligner que les principes SALA ne font aucune mention des capacités cybernétiques autonomes[4].

Exemples d'instruments adoptés par une organisation/un processus international

- Déclaration de Benguérir : Déclaration finale du Forum sur l'Intelligence Artificielle en Afrique ;
- Conseil de l'Europe, Assemblée parlementaire : Recommandation 2344 (2020) sur les interfaces cerveau-machine : nouveaux droits ou nouveaux dangers pour les libertés fondamentales ? ; Recommandation 2185 (2020) intelligence artificielle et santé : défis médicaux, juridiques et éthiques à venir ; Recommandation 2182 (2020) sur la justice par algorithme - Le rôle de l'intelligence artificielle dans les systèmes de police et de justice pénale ; Résolution 2346 (2020) sur les aspects juridiques concernant les « véhicules autonomes » ; Résolution 2345 (2020) sur l'intelligence artificielle et les marchés du travail : amis ou ennemis ? ; Résolution 2343 (2020) sur la prévention des discriminations résultant de l'utilisation de l'intelligence artificielle ; Résolution 2341 (2020) sur la nécessité d'une gouvernance démocratique de l'intelligence artificielle ;
- Conseil de l'Europe, Comité des Ministres : Déclaration sur les risques de la prise de décision assistée par ordinateur ou reposant sur l'intelligence artificielle dans le domaine du filet de sécurité sociale Décl(17/03/2021)2 ; Déclaration sur les capacités de manipulation des processus algorithmiques

Note 4 La cybersécurité n'est que brièvement mentionnée dans le sixième principe, le principe (f), comme l'une des « garanties non physiques appropriées » qui devraient être envisagées « lors de la mise au point ou de l'acquisition de nouveaux systèmes d'armes basés sur des technologies émergentes dans le domaine des systèmes d'armes létaux autonomes ».

Décl(13/02/2019)1 ; Recommandation CM/Rec(2019)1 sur la prévention et la lutte contre le sexisme ;

- Conseil de l'Europe, Conférence des ministres responsables des médias et de la société de l'information : Résolution sur l'intelligence artificielle
- Une politique intelligente. Défis et opportunités pour les médias et la démocratie ;
- Réseau ibéro-américain de protection des données : Recommandations générales pour le traitement des données personnelles en intelligence artificielle ;
- UNESCO : Recommandation sur l'éthique de l'intelligence artificielle ; Consensus de Beijing sur l'intelligence artificielle et l'éducation ;
- Nations Unies : 11 Principes sur les systèmes d'armes létaux autonomes adoptés en 2019 par le G EG sur les SALA, CCW/MSP/2019/9, annexe III, p. 10.

3.2. Aperçu des règles existantes

L'IA est peut-être l'un des rares domaines numériques où la plupart des États sont disposés à adopter de nouveaux instruments, comme en témoigne la recommandation sur l'éthique de l'IA adoptée par l'UNESCO en novembre 2021. Les tentatives de réglementation de l'IA sont très fragmentées et varient en fonction de la technologie ou de l'utilisation qui est prise en compte. Le droit international existant en matière d'IA n'en est qu'à ses débuts, même si de multiples initiatives et processus sont actuellement en cours, avec parfois un certain chevauchement quant à leur contenu.

Le nombre limité de règles internationales spécifiques à l'IA ne signifie pas pour autant que l'IA n'est pas régie par le droit international. En effet, les règles et principes existants du droit international sont pertinents pour réglementer les technologies de l'IA et leurs différentes utilisations. Cependant, il existe encore un certain degré d'incertitude quant à la manière dont ces règles pourraient être appliquées à l'IA. Il n'existe pas de règle contraignante du droit international spécifiquement dédiée à l'IA ; on note cependant l'existence d'un nombre croissant de normes non contraignantes adoptées sur l'IA en général ou sur certaines de ses applications spécifiques (par exemple, sur l'IA dans le domaine de la santé, les marchés du travail et l'éducation,

concernant les véhicules autonomes, ou encore l'utilisation de l'IA dans le secteur de la justice pénale).

3.3. Aperçu des règles consensuelles et règles litigieuses

En principe, il existe un accord sur l'applicabilité du droit international général et des différentes branches du droit international (droit international des droits de l'homme, droit international humanitaire, droit de la responsabilité internationale, etc.) à l'IA. Cependant, il n'existe toujours pas de position définie ou conceptuellement claire sur l'IA en droit international, et les interrogations sur le caractère suffisant et efficace des règles actuelles et sur la nécessité d'établir de nouvelles règles, par exemple dans le contexte des droits de l'homme, persistent. Dans cette optique, un important sujet d'incertitude et de discussion concerne la question de savoir si et comment les humains seront en mesure de garder le contrôle de l'IA et donc s'il est nécessaire d'établir de nouvelles règles dans cette perspective.

3.4. L'impact de l'IA sur le droit international

Les paragraphes précédents ont décrit comment le droit international réglemente les différentes dimensions de l'IA. Cependant, il est important de noter que le développement de certaines applications de l'IA peut avoir un impact sur la substance du droit international, les processus décisionnels liés au droit international, les processus d'élaboration du droit ainsi que sur la mise en œuvre et l'application de ses règles et principes. L'apprentissage automatique et l'analyse computationnelle des textes peuvent être utilisés, par exemple, pour les mécanismes de règlement des différends, les négociations de traités et les décisions internationales. La capacité de collecter et de traiter d'importants ensembles de données peut être utilisée pour identifier les violations des règles ou des principes du droit international.

4. Conclusion

Cet « état des lieux » conduit à une double conclusion. Tout d'abord, il existe un consensus sur l'applicabilité du droit international aux trois sujets étudiés et sur l'existence d'une grande diversité d'instruments normatifs pertinents pour les questions

en jeu. Les instruments contraignants ont une portée plutôt générale, sans aborder spécifiquement aucun des trois sujets. D'autre part, au niveau régional et universel, il existe également pléthore d'instruments non contraignants spécifiquement dédiés aux données numériques, à la sécurité numérique ou à l'IA.

La deuxième observation concerne l'existence de défis communs aux trois thèmes. Il a été possible d'observer des désaccords non résolus sur des questions de droit international général, ainsi que sur la pertinence, l'interprétation et la mise en œuvre des règles et normes juridiques internationales dans le cyberespace. Ces désaccords pourraient en partie être attribués aux différentes approches culturelles des États et groupes régionaux numériquement puissants qui pèsent dans les négociations actuelles. Il découle de ce constat trois défis majeurs, qui seront présentés dans la section suivante.

2.

les défis

L'émergence de nouvelles technologies dans les domaines des données numériques, de la sécurité numérique et de l'intelligence artificielle a de profondes implications politiques, sociales et économiques, tant positives que négatives. Si certains des défis et opportunités découlant de l'utilisation des technologies numériques sont spécifiques à un secteur, trois défis communs qui traversent les trois sujets considérés ont été identifiés : la relation entre les acteurs publics et privés, l'instrumentalisation politique du droit international sur les questions numériques et les inégalités numériques endémiques. En effet, malgré la fragmentation technique, juridique et géographique de la sphère numérique (telle qu'observée à partir des règles et processus recueillis dans l'exposé des faits), ces défis sont omniprésents et soulèvent des questions difficiles pour les décideurs politiques, les juristes internationaux et les chercheurs travaillant sur les trois sujets.

Bien que les défis identifiés ici ne soient pas exhaustifs, ils sont susceptibles de façonner les débats sur les technologies numériques dans les années à venir. Ils peuvent également être pertinents au-delà du domaine numérique, par exemple dans le contexte de certains des autres sujets envisagés par l'ILA/ADI pour son 150ème anniversaire, alors que le droit international est aux prises avec une polarisation politique croissante, des inégalités persistantes et un paysage d'acteurs non étatiques de plus en plus complexe. Il est essentiel de noter que ces défis sont souvent interdépendants : la relation entre les acteurs publics et privés, par exemple, implique la distribution souvent inégale des capacités numériques, et ces deux défis sont subsumés dans la politisation plus large des débats juridiques internationaux sur les questions numériques. Toute évaluation des solutions proposées doit donc tenir compte de leurs externalités, positives ou négatives, sur les autres défis et opportunités. Dans cette partie, chacun de ces trois défis sera discuté et illustré par des exemples tirés des domaines des données numériques, de la sécurité numérique et de l'IA. L'objectif est de comprendre les difficultés et les opportunités qu'ils soulèvent.

1. Les frontières entre le public et le privé

Les débats sur la répartition appropriée des rôles et des responsabilités entre les acteurs publics et privés sont une caractéristique récurrente de la mondialisation. Dans le domaine numérique, le développement et l'utilisation de nouvelles technologies par des acteurs privés ont suscité à la fois de l'enthousiasme et des inquiétudes quant à la capacité des États à ré-

glementer efficacement l'accès à l'information et la liberté d'expression en ligne, et à assurer la sécurité de l'environnement numérique sans entraver l'innovation. Les multinationales, en particulier les grands fournisseurs de services en ligne, contrôlent et exploitent de vastes quantités de données numériques qui font partie intégrante de la gouvernance publique, de l'activité économique et des droits individuels, et elles sont à la pointe du développement des technologies d'intelligence artificielle. Leurs capacités de protection des données sont également un élément clé des efforts de cybersécurité, et elles jouissent d'un rôle de premier plan dans la prévention, la détection et la réponse aux cyberopérations malveillantes. Ces technologies et ces données sont une source de revenus pour ces entreprises, mais aussi un outil précieux pour servir l'intérêt public. À l'inverse, d'autres acteurs non étatiques, qu'il s'agisse de groupes ou d'individus, sont également responsables de la conduite d'opérations malveillantes, parfois en étroite collaboration avec des États. Les caractéristiques des relations entre les États et une grande variété d'acteurs privés, entre les sphères privée et publique, font donc partie intégrante des débats sur les données numériques, l'intelligence artificielle et la sécurité numérique, et les sections suivantes donnent un aperçu de certains des principaux défis à venir.

1.1. Les données numériques

- Collecte, stockage et analyse des données par les acteurs privés et publics

Les entreprises privées analysent d'énormes ensembles de données, contenant souvent des données personnelles, et les utilisent pour développer de nouvelles applications et technologies, mais aussi pour diverses activités commerciales comme la publicité ou le développement de produits ou de services ciblant des individus et des groupes particuliers. Les gouvernements s'intéressent également aux données numériques, que ce soit à des fins de surveillance ou pour améliorer le fonctionnement de l'administration publique. Les organisations internationales ont également identifié les données comme un atout stratégique[5]. La production, le contrôle et l'utilisation des données numériques sont donc devenus d'un intérêt capital pour un large éventail d'acteurs, y compris les États et les organisations internationales. La plupart des données numériques

Note 5 Voir, par exemple, le Secrétaire général des Nations unies, *Data strategy of the Secretary-General for action by everyone, everywhere with insight, impact and integrity* (2020) ; I.T.U., "New UN targets chart path to universal meaningful connectivity" (19 avril 2022) <https://www.itu.int/hub/2022/04/new-un-targets-chart-path-to-universal-meaningful-connectivity/>.

sont toutefois entre les mains d'acteurs privés, sur lesquels les citoyens s'appuient presque entièrement pour protéger leurs données et les droits associés. De nombreux acteurs privés disposent de plus de données sur les citoyens que les gouvernements, ce qui génère des dépendances vis-à-vis du secteur privé pour l'exécution des fonctions gouvernementales. Pendant la crise du Covid-19, par exemple, les entreprises de l'industrie de la surveillance et de la technologie ont étendu leurs services vers le secteur de la santé pour proposer des analyses de *big data* comme outil afin de faire face aux défis de la pandémie. Dans le contexte de la guerre en Ukraine, les données numériques détenues par Clearview, une entreprise américaine connue pour avoir collecté des milliards de photos d'individus en ligne, ont été utilisées par le gouvernement ukrainien pour identifier les morts et combattre la désinformation[6]. De même, la création, l'utilisation et la détection des technologies de *deep fake* impliquent des acteurs privés et publics.

Un autre aspect de l'effacement des lignes de démarcation entre les acteurs et les responsabilités publics et privés concerne la coopération requise dans l'exercice de la compétence étatique. Dans le cadre d'enquêtes criminelles, par exemple, les États doivent souvent coopérer avec le secteur privé pour recueillir des preuves numériques. Pour contrer la désinformation et les discours de haine, ils sont aussi souvent contraints de collaborer avec les plateformes numériques. En France, par exemple, vers 2015, le gouvernement français a dû négocier avec Twitter afin qu'il retire du contenu après le refus initial de l'entreprise de se conformer à la loi française. À l'inverse, il arrive aussi que les plateformes numériques facilitent les violations du droit international commises par l'État lui-même, comme cela a peut-être été le cas lorsque Meta (anciennement Facebook) a été accusé de ne pas avoir fait assez pour empêcher l'incitation au génocide menée par les autorités publiques du Myanmar sur sa plateforme.

Les organisations et les tribunaux internationaux sont confrontés à des défis similaires, une observation qui a été soulignée par le Secrétaire général des Nations unies dans la *Stratégie des Nations Unies en matière de données*. L'issue de l'affaire de la CIJ sur l'*application de la Convention pour la prévention et la répression du crime de génocide (Gambie c. Myanmar),* par exemple, pourrait dépendre de la capacité à contraindre Meta à remettre

Note 6 Paresh Dave, Jeffrey Dastin, "Exclusive : Ukraine has started using Clearview AI's facial recognition during war" (*Reuters*, 14 mars 2022) <https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/>.

les données pertinentes[7]. Si la possibilité de collecter des données numériques peut offrir de nouvelles opportunités pour les missions d'enquête et la réalisation de la justice internationale, elle soulève également de nouveaux défis concernant la chaîne de preuves et la valeur probante de ces données, notamment lorsqu'elles sont collectées par des acteurs non étatiques et en dehors d'un processus d'enquête formel[8].

Enfin, les acteurs privés concurrencent directement les États en prenant part à des activités qui étaient auparavant la seule prérogative des autorités publiques. Un bon exemple est le développement des crypto-monnaies qui, à ce jour, échappent largement à la plupart des lois nationales et au droit souverain des États sur les monnaies. Ces évolutions remettent en cause les rôles et responsabilités des entités privées vis-à-vis des citoyens mais aussi leur relation avec les États dans la mise en œuvre des fonctions gouvernementales.

Note 7 Michael A. Becker, « The Gambia v Facebook : Obtaining Evidence for Use at the International Court of Justice (Part I)' (*EJIL : Talk !*, 5 octobre 2021) <https://www.ejiltalk.org/the-gambia-v-facebook-obtaining-evidence-for-use-at-the-international-court-of-justice-part-i/>.

Note 8 Les enquêtes de source ouverte menées par Bellingcat, tout récemment dans le contexte du conflit en Ukraine, en sont un bon exemple : https://www.bellingcat.com/tag/ukraine/?fwp_categories=news&fwp_tags=ukraine.

- Données et économie numérique

Les données sont au cœur des systèmes économiques développés par le secteur privé autour des nouvelles technologies : monnaies électroniques, plateformes et nouveaux services de paiement, actifs numériques, etc. Quatre types de problèmes peuvent découler du contrôle des acteurs privés sur ces données : 1) la confrontation entre une logique commerciale et une logique de sécurité, y compris de sécurité juridique, dans la manière dont les données sont traitées. Concernant la sécurité juridique, différentes questions sont soulevées : des questions individuelles dans le contexte de l'application de la loi aux questions collectives dans celui de la sécurité nationale ; 2) une approche géopolitique opposée à une approche commerciale dans la manière dont l'usage des données doit être régulé ; 3) un risque de divergence et un manque de communication et de dialogue entre les acteurs économiques et les régulateurs, les premiers ne comprenant pas nécessairement l'intérêt des nouvelles règles produites par les seconds, ce qui peut avoir un impact sur le contenu et l'application de la loi ; 4) la question de savoir ce qui doit être réglementé, en tenant compte du fait qu'il n'est peut-être pas essentiel de tout intégrer dans le droit.

La forte dimension privée du secteur économique pourrait laisser penser que les efforts normatifs devraient surtout porter sur les questions de conflits de lois. Mais il est également nécessaire de travailler sur les dispositions de fond des nouveaux instruments, comme le fait UNIDROIT par exemple dans le cadre de son projet « Actifs numériques et droit privé ». Certains secteurs ont déjà commencé à évoluer. Les secteurs de la banque et de la finance, particulièrement réglementés, ont déjà accepté que le risque puisse exister sans remettre en cause l'intégrité de leurs pratiques. Pour s'adapter aux nouveaux défis, les États et les organisations internationales ont par exemple développé des approches communes pour prévenir l'utilisation abusive des crypto-monnaies à des fins criminelles[9]. Dans le domaine du signalement des incidents de cybersécurité, le RGPD constitue par exemple un point de départ pour l'obligation qui en découle à l'égard des acteurs privés.

Les données de l'économie numérique n'appellent pas seulement des changements dans ce que dit le droit mais aussi dans la manière dont il est fait. Toutes ces données peuvent être utilisées pour mieux comprendre les pratiques et ainsi faire évoluer le droit en fonction des besoins, voire les anticiper. Le rôle des acteurs privés dans la collecte et l'analyse de ces données nous amène à nous interroger sur le rôle qui pourrait leur être attribué dans l'élaboration des normes. Le caractère public-privé de ce secteur incite à poursuivre la réflexion sur le « droit international collaboratif[10] », c'est-à-dire sur l'amélioration des mécanismes d'élaboration, d'application et d'interprétation du droit afin de le rendre plus efficace et efficient.

En résumé, deux grands défis se posent ici : d'une part, la nécessité pour la réglementation de tenir compte de la neutralité technologique et, d'autre part, la nécessité d'élaborer un ensemble commun de normes minimales qui protègent les intérêts individuels et collectifs mais favorisent également le développement technologique. Afin de préserver la stabilité économique, le droit ne doit pas changer radicalement, mais il doit évoluer en fonction des besoins du monde réel.

Note 9 Voir GAFI/FATF, *Updated Guidance for a Risk-Based Approach for Virtual Assets and Virtual Assets Service Providers* (2021), https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021.html.

Note 10 Voir Catherine Kessedjian, *Le droit international collaboratif,* Paris, Pedone, 2016, 190 p.

- Données et pluralité normative

Une autre dimension des défis associés à la question des frontières entre le public et le privé est la pluralité normative qui découle du rôle et de l'importance croissante des acteurs privés. Les normes établies par les conditions générales d'utilisation des grandes plateformes en ligne (concernant, par exemple, la réglementation de l'expression) servent de base aux plateformes pour prendre des mesures et réglementer le contenu, devenant ainsi les normes *de facto* applicables sur le « territoire virtuel » des plateformes et entrant en concurrence avec les lois en vigueur dans un pays. Il est intéressant de noter que les conditions générales d'utilisation intègrent des éléments qui relèvent normalement du droit public. Par exemple, le conseil de surveillance de Meta fait référence au droit international dans plusieurs des décisions qu'il a rendues depuis sa création[11]. Cela conduit à une situation à la fois de concurrence et de complémentarité entre les normes privées et les normes publiques.

Note 11 Pour une liste de ces décisions, voir https://www.oversightboard.com/decision/.

1.2. La sécurité numérique

Dans le domaine de la sécurité numérique, le brouillard qui entoure la distinction entre le public et le privé ressort du paysage des menaces lui-même. Tout d'abord, les États, y compris ceux qui disposent de capacités avancées, peuvent autoriser, voire faciliter les activités des acteurs non étatiques d'une manière spécifiquement conçue pour ne pas exercer le niveau de contrôle qui engagerait leur propre responsabilité. La frontière peut également être floue entre les activités menées dans l'intérêt ou à la demande plus ou moins explicite d'un État et les activités menées dans le propre intérêt de l'acteur de la menace. En termes de capacités, le code peut faire l'objet de fuites et les outils peuvent être réutilisés par de nombreux acteurs, comme en témoignent les fuites des Shadow Brokers et leur réutilisation par des États et des acteurs non étatiques. À l'inverse, des outils peuvent être développés et mis en œuvre pour masquer l'identité de leurs auteurs et compliquer leur identification. Deuxièmement, l'impact des menaces numériques rend encore plus floue la frontière entre les sphères publique et privée. Les effets des activités malveillantes peuvent se propager bien au-delà des cibles initiales, comme l'ont montré de nombreuses cyberactivités malveillantes dans le passé. Les opérations d'information, par leur nature même, transcendent

également toutes les frontières (public/privé, civil/militaire). Enfin, les acteurs non étatiques peuvent exercer des prérogatives habituellement réservées aux États afin de se défendre ou de défendre les autres dans l'espace numérique. Le brouillage de toutes ces lignes présente toutefois un avantage : tout effort visant à accroître le niveau de sécurité d'un acteur est susceptible de profiter aux autres, et donc de rendre plus difficile pour quiconque l'exploitation des vulnérabilités existantes et la conduite d'activités malveillantes.

La relation entre l'État et les acteurs non étatiques est également pertinente dans le contexte de la garantie de la sécurité d'un État et, plus globalement, de la sécurité internationale. L'importance d'assurer la sécurité du domaine numérique a considérablement accru le pouvoir des entreprises privées de cybersécurité et des équipes d'intervention en cas d'urgence informatique (CERT). Leur collaboration et leurs relations avec les États sont déjà devenues un sujet de discussion important, notamment dans le cadre de l'attribution des cyberopérations, de la sécurité des infrastructures critiques et de la lutte contre la cybercriminalité. Les États comptent de plus en plus sur les entreprises privées pour stocker et protéger les données sensibles et les infrastructures critiques, et ils sont aussi souvent contraints de collaborer avec les entreprises de cybersécurité pour prévenir, identifier et répondre aux menaces de cybersécurité. Il en va de même pour les organisations internationales telles qu'Interpol. Les entreprises privées, en particulier les plateformes numériques, jouent également un rôle particulièrement important dans les efforts visant à limiter les opérations d'information nuisibles, les États s'appuyant largement sur elles. Le Code de bonnes pratiques de l'UE contre la désinformation et le règlement sur les services numériques (Digital Services Act, DSA) sont des initiatives clés à cet égard. Il en va de même des divers processus nationaux (par exemple, les négociations actuelles sur le projet de loi britannique sur la sécurité en ligne, les débats aux États-Unis sur la réforme de l'article 230 de la loi sur la décence des communications, diverses lois nationales visant à endiguer la désinformation, etc.). Au final, la relation entre l'État et les entreprises privées en matière de modération du contenu et d'opérations d'information définira qui a le contrôle de l'expression sur Internet.

Les rôles respectifs des entreprises privées, des ONG et des particuliers dans les négociations internationales sur la sécurité numérique sont devenus un sujet de débat important. Par exemple, les règles relatives à la participation de la société civile aux processus du GGE et de l'OEWG de l'ONU et au comité *ad hoc* sur la cybercriminalité ont été la source de nombreux

désaccords entre les États participants[12]. Les entreprises privées (notamment Microsoft) sont également très intéressées par les négociations à l'ONU et plus généralement par les négociations internationales, bien que leur participation soit très variable. Les discussions sur les rôles et responsabilités respectifs des États et de la société civile, dont les entreprises privées, soulèvent des questions importantes sur la légitimité de l'élaboration de normes internationales et sur l'équilibre des pouvoirs entre les parties prenantes, qui peuvent varier selon les différentes étapes du processus de création de normes. L'un des défis sera de concevoir des structures institutionnelles capables d'accueillir la participation de tous les acteurs concernés, tout en préservant les prérogatives essentielles de l'État en matière de création de normes et de prise de décision. Si les processus multilatéraux et centrés sur l'État ne réussissent pas, il est également possible que d'autres acteurs et processus viennent combler le vide. Des processus tels que le processus d'Oxford sur les protections du droit international dans le cyberespace[13] ou le *Manuel de Tallinn* (fréquemment cité et débattu par les États, parfois même dans leurs doctrines nationales sur l'application du droit international dans le cyberespace) ont déjà montré qu'ils pouvaient être efficaces s'ils parvenaient à obtenir l'adhésion d'un nombre suffisant d'États. Des entreprises privées ont également initié divers processus dans le domaine de la sécurité numérique, comme la Charte de confiance (Siemens), le Cybersecurity Tech Accord (Microsoft), et dans le cadre de la lutte contre le terrorisme (voir notamment le Global Internet Forum to Counter Terrorism).

Enfin, la relation entre l'État et les acteurs non étatiques se manifeste dans le domaine de la pluralité normative. Tant pour la couche physique que pour la couche logique, la sécurité est largement définie par des acteurs non étatiques. Les normes mondiales comme l'ISO façonnent l'avenir des technologies et

Note 12 Voir la résolution sur la participation multipartite à l'OEWG récemment proposée par le Royaume-Uni : AGNU, « Royaume-Uni de Grande-Bretagne et d'Irlande du Nord : projet de résolution. Modalités de participation des organisations non gouvernementales, des organisations de la société civile, des établissements universitaires et du secteur privé au Groupe de travail à composition non limitée sur la sécurité de son utilisation 2021-2025 » [7 avril 2022] A/76/L.49 ou les débats sur la participation de plusieurs parties prenantes au Comité spécial sur la cybercriminalité : « General Assembly Adopts Resolution Outlining Terms for Negotiating Cybercrime Treaty amid Concerns over "Rushed" Vote at Expense of Further Consultations » [26 mai 2021] GA/12328.

Note 13 Oxford Process on International Law Protections in Cyberspace, <https://www.elac.ox.ac.uk/research/the-oxford-process-on-international-law-protections-in-cyberspace/#:~:text=The%20Oxford%20Process%20on%20International%20Law%20Protections%20in%20Cyberspace%20is,2020%20in%20partnership%20with%20Microsoft>.

l'architecture de l'Internet est gérée par des acteurs non étatiques. Étant donné que la sécurité n'est pas toujours une priorité pour les exigences techniques ou qu'elle est revue à la baisse pour des questions de sécurité nationale[14], les exigences techniques et les procédures de sécurité, comme dans le cas de la divulgation de vulnérabilités, peuvent avoir un impact, direct ou non, sur le niveau de sécurité. Même si les États peuvent influencer ces normes, ils sont privés d'un grand pouvoir dans ce domaine, devant faire face à une réglementation technique privée. Dans le domaine de la désinformation, différents efforts de corégulation ou d'autorégulation existent cependant.

1.3. L'intelligence artificielle

Les acteurs non étatiques, en particulier les entreprises privées et les instituts de recherche, sont aujourd'hui les principaux acteurs du développement des technologies et des applications de l'IA. Même lorsque les États développent leurs propres applications d'IA, dans la plupart des cas, elles sont basées, au moins en partie, sur des solutions technologiques développées par des acteurs non étatiques. Une application d'IA peut être le résultat de différentes solutions développées par différents acteurs, qu'il s'agisse d'acteurs liés aux États ou d'acteurs non étatiques. Elle contribue ainsi à brouiller les frontières entre ces différents acteurs. Dans ce contexte, les questions liées à la relation et à la répartition des responsabilités entre les acteurs publics et privés sont particulièrement pertinentes en ce qui concerne l'IA. En outre, le développement de l'IA nécessite l'accès à des données qui sont souvent détenues par des acteurs privés, ce qui soulève des préoccupations similaires à celles déjà abordées dans le contexte de la collecte, du stockage et de l'analyse des données par des acteurs privés et publics qui ne seront donc pas reprises dans cette section.

Le rôle des acteurs non étatiques dans les utilisations de l'IA pour le compte d'États ainsi que les relations de ces acteurs avec les États prennent des formes très différentes. Afin d'accomplir certaines tâches, y compris des fonctions qui font partie intégrante de l'exercice de la puissance publique, les organismes publics et d'autres entités agissant au nom des États utilisent des applications d'IA développées par des acteurs privés. On constate, par exemple, une utilisation croissante des solutions d'IA dans le cadre des contrôles aux frontières et de

Note 14 Voir les révélations d'E. Snowden sur la cryptographie et les États-Unis.

l'immigration[15], des enquêtes criminelles et financières, ou dans le contexte d'un conflit[16]. Le développement du secteur dit de la « santé en ligne » ou « e-santé » peut également illustrer la difficile relation entre les acteurs publics et privés, car les données collectées par des applications développées par des entreprises privées peuvent être utilisées par des institutions de santé publique. La réalisation d'une activité spécifique à l'aide d'une technologie d'IA peut être le résultat de différentes activités menées par des États et des acteurs non étatiques, pour développer certaines technologies, les transformer et ensuite les utiliser. Une telle diversité de rôles joués par les acteurs non étatiques remet également en question la manière dont ces relations peuvent être appréhendées par le droit international.

Note 15 Voir, par exemple, Parlement européen, *Intelligence artificielle aux frontières de l'Union européenne. Aperçu des applications et des questions clés* (2021).

Note 16 L'entreprise américaine Clearview AI offre un exemple pertinent, puisque son application de reconnaissance faciale a été utilisée par les autorités chargées de l'application de la loi aux États-Unis et a plus récemment été fournie au gouvernement ukrainien dans le but d'identifier les soldats russes tués en Ukraine.

2 La politique juridique dans le cyberespace

Compte tenu de leurs importantes implications sociales et économiques, les débats internationaux sur la gouvernance des technologies numériques sont souvent litigieux et politiquement tendus. L'élaboration de règles juridiques et de normes non contraignantes est devenue un objet de débat politique et de stratégie, un moyen pour les États et les autres parties prenantes intéressées de promouvoir leur vision de la gouvernance de l'Internet, et peut-être même de la gouvernance au sens large.

2.1. Les données numériques

Il existe actuellement plusieurs modèles différents de protection des données. A titre d'exemple, et au risque de les simplifier à l'extrême, on peut citer un modèle européen considérant les données comme un attribut de la personne et consécutivement appelant à la plus forte protection, un modèle américain considérant les données comme un actif et favorisant leur libre collecte et utilisation, notamment à titre commercial, et un modèle chinois, émergent, axé sur la préservation de la souveraineté et de la sécurité. Ces trois modèles présentent des

caractéristiques communes mais aussi des logiques sous-jacentes très différentes, qui conduisent leurs promoteurs à diverger dans leur interprétation des normes internationalement établies et à envisager des méthodes de protection et de contrôle des données différentes, voire opposées.

La confrontation entre ces différents modèles se matérialise à travers les questions entourant l'extraterritorialité des instruments normatifs, mais aussi la compétence opérationnelle des Etats et des organisations internationales. Plus généralement, on assiste à une opposition entre deux logiques concurrentes, l'une privilégiant la libre circulation des données, l'autre leur protection. Il est légitime que les États et les groupes régionaux défendent des instruments normatifs fondés sur leurs propres valeurs, mais leurs effets extraterritoriaux peuvent entraîner une augmentation des conflits de normes et de juridictions. La solution réside non seulement dans l'élaboration de règles sur les conflits de normes et de juridiction, mais aussi dans les règles de fond du droit international public et privé.

Elle dépend aussi et surtout du développement des mécanismes appropriés de dialogue, de coopération, voire de complémentarité entre les différents systèmes normatifs, que ce soit au stade de la formation du droit ou à celui de sa mise en œuvre. L'inscription de la *Protection des données personnelles dans la circulation transfrontière de l'information* au programme de travail à long terme de la Commission du droit international des Nations unies (CDI)[17] pourrait être une perspective intéressante en ce sens, si elle se réalise. Une réflexion sur la politique juridique nous amène à réfléchir aux mécanismes juridiques qui permettront de développer un véritable droit *international* et à la manière de répondre à la fracture numérique, comme nous le verrons plus loin dans ce rapport.

2.2. La sécurité numérique

Il existe un large consensus sur le fait que les menaces numériques (cyber et informationnelle) vont continuer à augmenter en nombre et en sophistication. Selon plusieurs entretiens avec des experts, la nature des activités malveillantes (cybercriminalité, cyberterrorisme, attaques contre les infrastructures critiques, cyberespionnage, surveillance de masse, opérations informationnelles, etc.), qui vont des cyberactivités sophistiquées commanditées par des États aux menaces de bas niveau, restera probablement la même alors que leur sophistication, leur

Note 17 Commission du droit international, *Rapport sur les travaux de la cinquante-huitième* session [2006] A/61/10, Annexe D.

ampleur et leur rythme d'exécution augmenteront. L'instabilité et l'insécurité croissantes dans la sphère numérique ont fait et continueront donc de faire l'objet de nombreux débats juridiques et politiques. En effet, si de nombreux acteurs dépensent d'énormes ressources pour contrer ces menaces, les États et les acteurs non étatiques tirent également profit de la conduite d'activités malveillantes et il est peu probable qu'ils restreignent considérablement leurs options. Cela aura un impact à la fois sur le contenu de la loi pertinente et sur le processus législatif.

Aujourd'hui, les principaux enjeux des négociations internationales sur la cybersécurité ne sont pas juridiques mais géopolitiques. Par le biais des négociations internationales sur la sécurité numérique, les États rivalisent pour imposer différentes conceptions de la gouvernance de l'Internet/des TIC : certains voient la sphère numérique principalement comme une opportunité de faire progresser l'économie, d'autres se concentrent sur son potentiel pour assurer la prospérité humaine, et d'autres encore donnent la priorité à la sécurité des États. Ces différentes visions coexistent et parfois entrent en conflit au sein d'un même État. Chacune de ces visions a un impact sur la manière dont les États pensent et parlent du droit international, sur les choix effectués quant à son interprétation et sur le type de règles juridiques internationales envisagées par les États. Par exemple, les États qui privilégient le développement économique recherchent des règles juridiques internationales qui préservent l'innovation, tandis que ceux qui se concentrent sur les droits de l'homme mettront l'accent sur le respect de la vie privée/le chiffrement. Quant à ceux qui se préoccupent principalement de la sécurité nationale, ils chercheront à passer outre les protections en matière de cybersécurité afin de dépersonnaliser les utilisateurs et/ou d'imposer des contrôles du contenu numérique. Les États peuvent également exploiter volontairement les défis liés à l'interprétation du droit international, en générant de nouvelles ambiguïtés, ajoutant ainsi confusion et instabilité à la situation actuelle. Au cours des entretiens menés par le comité de pilotage chargé de préparer le Livre blanc, il a été suggéré que cet état de fait n'implique pas nécessairement que le droit international soit la racine des problèmes ou la solution et que le manque de clarté juridique n'est pas nécessairement le principal obstacle au respect des règles. Il s'inscrit plutôt dans une crise plus large du multilatéralisme où le droit international est devenu un outil de compétition politique. Alors que certains États sont intéressés par le maintien du *statu quo,* d'autres y voient une opportunité de proposer de nouvelles règles et de faire avancer leurs propres intérêts.

Cette dimension politique des débats juridiques sur la sécurité numérique se manifeste également dans le domaine de la désinformation. Si les États ont réussi à trouver un consensus sur la propagande terroriste, le développement des opérations informationnelles par des États et des acteurs non étatiques pour parvenir à des fins différentes, y compris pour s'ingérer dans les affaires intérieures d'autres États, remet en cause les fondements mêmes des démocraties occidentales. Pendant des décennies, les démocraties occidentales ont prudemment évité d'inclure les opérations informationnelles dans les discussions internationales, alors que des Etats comme la Chine ou la Russie, qui défendaient le concept de sécurité de l'information, ont tenté de le faire. Aujourd'hui, les États occidentaux s'efforcent de trouver le juste équilibre entre le contrôle du contenu et la protection des droits de l'homme. Le phénomène des opérations informationnelles est alimenté par les États eux-mêmes. En effet, de plus en plus d'États développent des doctrines militaires pour légitimer et mener ces opérations, créant ainsi des vulnérabilités pour leurs propres sociétés et augmentant le dilemme auquel ils sont confrontés.

Les défis géopolitiques autour de la diplomatie numérique touchent également le modèle du cyberespace lui-même. Les débats sur le rôle de l'Union internationale des télécommunications au cours des années 2000 ont resurgi à mesure que la fragmentation du cyberespace et la politique et le contrôle de son infrastructure ont augmenté. Cela renforce les débats autour du modèle multipartite de la gouvernance de l'Internet et accentue un peu plus la division entre les différentes visions de la régulation, tant formelle que matérielle, du cyberespace.

Dans le domaine de la cybercriminalité, la politique juridique a les mêmes conséquences, que ce soit en termes de méfiance pour obtenir un consensus au sein du comité *ad hoc* chargé d'élaborer un nouveau traité sur la cybercriminalité dans le cadre de l'ONU, de fragmentation de la réglementation internationale en matière de cybercriminalité et d'impact sur les droits de l'homme. En effet, nous assistons à une situation où la lutte contre la cybercriminalité est de plus en plus encadrée par le prisme de la sécurité nationale et non de la justice pénale, menaçant les droits de l'homme et les libertés fondamentales et limitant toute volonté de coopération.

Les conséquences sont triples. Premièrement, cette situation a un impact direct sur la capacité des États à parvenir à un accord significatif pour mieux assurer la sécurité et la stabilité du cyberespace dans le cadre de la sécurité internationale. Ensuite, elle exacerbe les désaccords entre les États, renforçant la logique des coalitions d'États partageant les mêmes idées et

s'agrégeant autour de valeurs communes, contribuant ainsi à la fragmentation de la réglementation. Enfin, elle conduit à une situation dans laquelle nous voyons certaines questions de sécurité être formulées sous un angle économique dans le but de surmonter les blocages actuels. Par exemple, l'OCDE, une organisation internationale dont le mandat est centré sur le développement économique, a commencé à travailler sur des questions de sécurité telles que la divulgation des vulnérabilités, la sécurité de la chaîne d'approvisionnement des TIC ou le piratage informatique par des acteurs privés.

Si le contenu des négociations internationales sur la sécurité numérique fait l'objet de nombreuses discussions controversées, les différents processus dans le cadre desquels ces négociations sont menées soulèvent également des implications politiques importantes. Cela est particulièrement vrai dans le contexte des négociations au sein de l'ONU, dont les plus médiatisées ont été menées dans le cadre du Groupe d'experts gouvernementaux de l'ONU (le dernier étant uniquement parrainé par les États-Unis et leurs alliés) et de l'OEWG parrainé par la Russie. Ces processus ont acquis une importance politique significative et leurs rapports sont vigoureusement négociés et discutés par les États et toutes les autres parties prenantes intéressées. De manière cruciale, les questions de droit international et plus particulièrement de son application dans le cyberespace étaient au cœur des deux processus.

Les États se sont montrés réticents à partager des points de vue précis sur l'application du droit international dans le contexte de la sécurité numérique (empêchant ainsi la clarification du droit, qu'il soit conventionnel ou coutumier), bien que le rapport final du Groupe d'experts gouvernementaux de 2021 (A/76/135) ait notamment été accompagné de la publication par certains États de déclarations nationales sur l'application du droit international dans le cyberespace (A/76/136). La valeur et la signification politique de ces déclarations feront l'objet de nombreux débats : si elles peuvent être considérées comme un outil permettant de clarifier le droit et d'obtenir l'adhésion des États, elles peuvent aussi être perçues comme une forme d'unilatéralisme érodant davantage des processus multilatéraux déjà fragiles.

Au final, l'un des principaux défis des années à venir consistera à identifier les forums appropriés pour discuter des questions sensibles de sécurité numérique et de leur interaction avec le droit international : les processus de l'ONU resteront très probablement pertinents, notamment à travers le mandat le plus récent de l'OEWG et du Comité *ad hoc* chargé d'élaborer un traité sur la cybercriminalité. Dans les années à venir, les négociations sur la cybercriminalité au sein de l'ONU feront l'objet

d'une grande attention, car elles pourraient réexaminer les normes discutées au sein du GGE/OEWG et/ou élargir la compréhension de ce qui constitue un « cybercrime » pour englober les opérations informationnelles, et pourraient même aborder des sujets tels que l'attribution aux États. D'autres organisations internationales dotées de mandats plus spécifiques pourraient également jouer un rôle important, notamment l'UIT, l'OCDE (qui travaille déjà sur la cybersécurité dans une optique économique, voir la section 1 ci-dessus), les organisations régionales de protection des droits de l'homme et d'intégration économique (Conseil de l'Europe, OEA, UA, ASEAN, etc.), et même l'OMC (les préoccupations en matière de sécurité et les obstacles techniques sont de plus en plus souvent invoqués et soulevés pour limiter le commerce des produits et services numériques). Le choix et la coordination (ou l'absence de coordination) de ces processus peuvent dépendre des intérêts politiques et de l'antagonisme des États les plus puissants, et sont susceptibles d'influencer le contenu des règles négociées. En ce qui concerne les questions d'interprétation du droit international, aucun organe traditionnel tel que la Sixième commission de l'Assemblée générale des Nations unies, la Commission du droit international ou la Cour internationale de Justice n'est pour l'instant en mesure d'être chargé de le clarifier. Cela laisse un rôle important à jouer aux institutions non multilatérales telles que l'Institut de droit international[18] ou l'ILA/ADI. Dans l'intervalle, d'autres initiatives telles que le *Manuel de Tallinn* ou le Processus d'Oxford sont intervenues.

Les forums et processus universels dans lesquels seront menées les négociations internationales sur la sécurité numérique ont également de profondes implications pour la participation active des pays en développement. Le risque existe qu'un manque de participation des pays en développement conduise à l'adoption de règles et de principes reflétant les intérêts des États puissants, ce qui pourrait éroder davantage la légitimité perçue du droit international en matière de sécurité numérique dans les décennies à venir. Au lieu de faire participer au dialogue davantage de pays en développement et de réduire les inégalités numériques (voir la section sur l'inégalité numérique endémique), les règles adoptées peuvent être soit non pertinentes, soit préjudiciables aux pays en développement si leurs perspectives ne sont pas intégrées. Il convient toutefois de noter qu'il existe une différence importante entre le niveau et l'impact de la participation aux processus universels et la forte produc-

Note 18 En 2021, l'IDI a créé une commission sur l'applicabilité du droit international aux cyberactivités.

tion normative au niveau sous-régional. Dans le domaine de l'interprétation du droit international dans le cyberespace, des efforts sont également déployés au niveau régional, comme l'illustrent les travaux du projet du Comité juridique interaméricain de l'Organisation des États américains sur l'amélioration de la transparence des points de vue des États sur le droit international dans le cyberespace[19].

2.3. L'intelligence artificielle

L'IA est confrontée à deux défis fondamentaux en matière de politique juridique dans le cyberespace, qui ont déjà été abordés dans les sections précédentes. Premièrement, il existe un degré important de confusion entre les questions juridiques et éthiques, ce qui n'est pas un problème en soi mais soulève tout de même quelques questions. À première vue, les discussions et les initiatives semblent se concentrer principalement sur les questions éthiques. Un examen plus approfondi de ces discussions montre toutefois que les questions et normes juridiques sont au centre de ces discussions et des instruments adoptés.

Note 19 Comité juridique interaméricain de l'Organisation des États américains, *International Law and State Cyber Operations* [2020].

L'éthique semble donc être davantage un point d'entrée pour faire avancer les questions liées à l'application du droit international à l'IA. Les frontières entre les questions éthiques et les questions juridiques ne sont donc pas toujours claires. Il convient de noter que cela peut être un sujet de préoccupation car cela pourrait affecter la valeur ou la substance des règles juridiques. Deuxièmement, dans le domaine de la sécurité internationale, la plupart de l'attention s'est concentrée sur les SALA et, par conséquent, d'autres formes de comportements inamicaux ou hostiles utilisant des applications d'IA tendent à être absentes des discussions existantes, ce qui peut accroître leur polarisation. Dans les forums multilatéraux, par exemple, il n'y a pratiquement pas eu de discussion sur les cyberopérations autonomes et la manière de les réglementer, alors qu'elles sont déjà une réalité.

Un troisième défi important concerne l'identification du bon équilibre entre une approche de l'IA dans son ensemble et des approches plus ciblées sur des technologies et des utilisations spécifiques de l'IA. Ces différentes technologies et applications soulèvent des questions juridiques différentes. Ce défi crée une double difficulté. D'une part, il n'y a que très peu, voire pas du tout, de questions juridiques générales sur l'IA, mais plutôt de nombreuses questions différentes sur les utilisations spécifiques

et les conséquences des produits basés sur l'IA. D'une certaine manière, ce défi est lié à la difficulté de définir clairement ce qu'il convient d'entendre par IA et comment les organisations et processus internationaux doivent l'aborder. D'un autre côté, cela a aussi une conséquence pratique, car différents débats et processus sont en cours en même temps, chacun se concentrant sur un ensemble assez limité de questions et de domaines d'application et avec des objectifs très différents. Enfin, dans certains cas, les discussions sur l'IA sont accessoires. Dans ces situations, l'IA n'est pas abordée en tant que telle, mais des décisions sont prises sur des questions qui peuvent avoir un impact sur l'IA en elle-même. C'est, par exemple, le cas dans le domaine de l'extrémisme violent et du terrorisme où des mesures de prévention peuvent être recommandées et impliquer l'utilisation de l'IA. Cependant, ces discussions très générales sur l'IA liées à d'autres sujets peuvent offrir des contributions très intéressantes qui contribueraient à des discussions similaires sur d'autres sujets. Ainsi, certaines de ces différentes discussions devraient être davantage connectées afin de faciliter la fertilisation croisée, mais aussi d'éviter les chevauchements et les contradictions. En adoptant une approche plus granulaire des différentes technologies liées à l'IA, il serait plus facile d'identifier les discussions similaires qui ont lieu dans différents forums.

Une dernière remarque sur la politique du droit international et de l'IA concerne l'approche adoptée. En général, l'IA est abordée dans une perspective réactive, visant à prévenir les utilisations (négatives) possibles de ces technologies. Les discussions sur les SALA en sont un bon exemple, de même que le débat sur le respect des droits fondamentaux par les nouvelles applications de l'IA. Pourtant, comme nous l'avons vu dans différentes parties de ce rapport, l'IA offre également des solutions positives pour le développement et l'application du droit international, la mise en œuvre des droits de l'homme ou la réduction de la fracture numérique. Cette question a été un peu abordée dans le cadre des missions d'enquête et des droits de l'homme, mais reste encore peu explorée.

3. La fracture numérique

3.1. Les données numériques

Les TIC sont un excellent moyen pour les habitants des pays en développement d'accéder à l'information et de participer au développement d'une plus grande diversité culturelle à l'ère du numérique. Toutefois, dans son rapport 2021 intitulé *Mesurer*

le développement numérique. Faits et chiffres, l'UIT a déclaré que 63% de la population mondiale avait accès à l'internet, mais que « 96 % des 2,9 milliards de personnes encore hors ligne [vivaient] dans les pays en développement[20] ». Le développement numérique n'est pas seulement une question de connectivité. Il comprend également un accès réel à l'Internet, c'est-à-dire la possibilité de bénéficier des services des TIC, aussi bien dans les villes que dans les campagnes et sans barrières de genre. Selon l'UIT, il existe à la fois un fossé entre les générations et un fossé entre les sexes. Il en résulte un « grand canyon de la connectivité » ou « fracture numérique » qui a une incidence directe sur le développement des États et sur leur capacité à atteindre les Objectifs de développement durable des Nations unies[21]. Bien que des programmes de renforcement des capacités dans le domaine de la connectivité soient mis en œuvre par des organisations internationales et de nombreux États[22], cette « fracture numérique » est loin d'être comblée et va accroître les inégalités de développement. Ces inégalités en matière de connectivité sont également affectées par la concentration des réseaux entre les mains de quelques acteurs en situation de monopole. Ajouté à la défaillance ou à la manipulation de l'architecture de l'Internet à des fins géopolitiques, cette situation menace la nature décentralisée de l'Internet et donc sa résilience, portant atteinte à la connectivité dans son ensemble.

Ce « grand canyon de la connectivité » renforce la fracture numérique en matière de données, une préoccupation croissante qui concerne les pays en développement mais aussi ceux qui ne disposent pas d'entreprises puissantes collectant et traitant les données à des fins économiques (par exemple, les pays européens). La « chaîne de valeur des données » est devenue essentielle au développement de l'économie numérique et requiert des capacités de production, de stockage et de traitement des données en vue de leur monétisation. Elle constitue une condition préalable au développement et à la vente de produits de l'Internet des objets (IoT) et d'applications et systèmes d'IA et produira en retour des données qui seront utilisées pour de futurs produits et services, augmentant ainsi le coût d'entrée sur le marché numérique. Comme le souligne un récent rapport de la CNUCED, « [a]vec l'évolution de l'économie numé-

Note 20 I.T.U., *Measuring Digital Devlopment. Facts and Figures 2021* (2021), 1.

Note 21 Secrétaire général de l'ONU, *Feuille de route pour la coopération numérique (juin 2020) ; A.G.N.U., Résolution sur les technologies de l'information et des communications au service du développement durable* [17 décembre 2021] A/RES/76/189.

Note 22 Pour une liste de ces programmes, voir https://cybilportal.org/es/projects/.

rique axée sur les données, un clivage lié aux données est venu aggraver la fracture numérique classique. Dans ce nouveau contexte, les pays en développement risquent de se retrouver dans une position subalterne, les données et leur valorisation étant concentrées dans les mains de quelques sociétés numériques d'échelle mondiale et autres multinationales[23] ».

Outre les conséquences économiques, ces inégalités techniques ont des conséquences directes sur la capacité à faire respecter les mécanismes de protection des données, car les données sont stockées et traitées par des acteurs puissants relevant souvent de la compétence d'autres Etats. Elles constituent également un démultiplicateur de fragmentation et de limitations des flux de données dans la mesure où, afin d'assurer l'application de leurs lois et réglementations sur les données, les États peuvent être tentés de limiter les flux de données, ce qui a un impact sur le développement des produits et services numériques. Des conséquences sociales et culturelles découlent également de ces inégalités techniques. Les produits et services basés sur des données numériques ne refléteront pas les valeurs et croyances morales et culturelles d'une population donnée, ce qui aura un impact négatif sur les individus et la société dans laquelle ils vivent. À l'inverse, la limitation des flux de données est susceptible d'accroître les « bulles de données », qui pourraient à leur tour être utilisées pour mettre en œuvre un contrôle et une surveillance accrus.

Enfin, comme la technologie peut également favoriser la mise en œuvre du droit international, notamment les droits de l'homme et les libertés fondamentales, l'État de droit et l'administration des services publics, l'absence de données numériques limite la capacité des États à remplir ces objectifs et responsabilités essentiels, ce qui entrave le renforcement de la sécurité humaine et de la démocratie[24]. De même, l'accessibilité des données est utile pour faire face aux grands défis de demain, tels que le réchauffement climatique ou le problème de la connectivité et de la fourniture de services humanitaires. Promouvoir l'accès aux données et leur partage effectif sera l'un des principaux défis des années à venir, tant pour les États

Note 23 CNUCED, *Rapport sur l'économie numérique 2021. Flux transfrontières de données et développement : A qui profitent ces flux ?* (2021), xvii.

Note 24 Dans le domaine de la prévention, de la détection et de la lutte contre la corruption, cela a été souligné par l'Assemblée générale des Nations unies : A.G.N.U., *Notre engagement commun à nous attaquer efficacement aux problèmes posés par la corruption et à prendre des mesures pour la prévenir et la combattre et renforcer la coopération internationale*, 2 juin 2021, A/RES/S-32/1.

que pour les organisations internationales. Pourtant, plusieurs facteurs peuvent expliquer le manque relatif de partage des données jusqu'à présent, notamment les préoccupations en matière de sécurité nationale, de confidentialité et de respect de la vie privée[25]. L'accessibilité des données n'est pas seulement un problème économique, mais aussi un problème pour la réalisation des ODD.

3.2. La sécurité numérique

La numérisation des sociétés s'est accompagnée du développement d'activités malveillantes provenant d'États et d'acteurs non étatiques. Alors que de plus en plus de services dépendent de la connectivité, que les produits sont de plus en plus connectés (Internet des objets) et que de nouvelles technologies sont développées (ordinateurs quantiques, IA, etc.), le nombre de vulnérabilités à exploiter ainsi que les nouveaux moyens de les exploiter vont par conséquent augmenter. L'augmentation du nombre de cyberattaques est devenue une préoccupation majeure pour un large éventail d'acteurs. La lutte contre ces menaces nécessite des capacités humaines, techniques, organisationnelles et juridiques qui sont inégalement réparties sur la planète et dont même les pays les plus développés sont dépourvus. En ce sens, il existe aujourd'hui un fossé mondial entre le niveau de connectivité et le niveau de sécurité. Les inégalités en termes d'accès et de transfert des données numériques sont également aggravées par des inégalités importantes en matière de capacités dans le domaine de la sécurité numérique. Les enjeux sont importants car les pays en développement déjà fragiles sont susceptibles d'être les plus touchés par une insécurité numérique endémique, tandis que les vulnérabilités qui en résultent sont capables d'accroître l'instabilité à l'échelle mondiale. Mais les pays les plus développés ont tendance à être les plus connectés, ce qui les rend également très vulnérables aux menaces numériques. La sécurité numérique des États est donc fortement dépendante des actions de tous les autres dans ce domaine. Il y a donc un intérêt commun entre tous les États, mais plus globalement de tous les acteurs, à combler le fossé de la sécurité numérique.

Outre les intérêts de sécurité nationale, la sécurité numérique est également une exigence pour assurer la protection des droits de l'homme. Un manque de cybersécurité représente un grand danger pour les données des utilisateurs, leur droit

Note 25 OCDE, *Recommandation du Conseil sur l'amélioration de l'accès aux données et de leur partage*, 2022, OECD/LEGAL/0463.

à la vie privée, la liberté d'expression ou la liberté de réunion et d'association. Sans sécurité, les États sont limités dans leur capacité à protéger et à défendre les droits de l'homme. Cela s'étend à la sécurité des technologies conçues pour faire progresser les droits de l'homme et le droit international ou qui peuvent être utilisées à cette fin[26]. Les opérations informationnelles ont également été décrites comme une menace pour la démocratie. Contrer ces opérations sera bénéfique pour la démocratie et l'État de droit. La même logique s'applique aux entreprises, aux droits de l'homme et à la diligence due[27]. Garantir la sécurité est un moyen pour elles de prévenir et de traiter les risques qu'un manque de sécurité peut avoir sur les droits de l'homme. La sécurité numérique est donc un catalyseur du respect et de la mise en œuvre du droit international.

Depuis la fin des années 1990, alors que les efforts pour accroître l'accès aux données et accélérer la numérisation des économies émergentes se sont intensifiés, la communauté internationale a progressivement développé des initiatives de renforcement des capacités dans le domaine cyber visant à améliorer la sécurité de l'environnement numérique[28]. Ces initiatives impliquent un large éventail d'acteurs et de communautés (États, organisations internationales, ONG, entreprises de cybersécurité, etc.), se concentrant sur une variété de sujets (accès aux données, cybersécurité, etc.) et d'objectifs (sensibilisation, partage de connaissances sur les capacités techniques, politiques, élaboration de lois, etc.). Bien que leur aspiration commune soit de faciliter le partage des connaissances et des capacités en matière de sécurité numérique, leur contenu et leur forme varient considérablement.

Étant donné l'importance collective de la protection de la sécurité de l'environnement numérique, la coordination, l'efficacité et la légitimité de ces initiatives sont devenues un sujet de discussion important. Toutefois, derrière leur nature apparemment technique, les initiatives de renforcement des capacités soulèvent également d'importantes questions politiques, notamment en

Note 26 Voir *supra* sur le rôle des données et de l'IA pour faire progresser les droits de l'homme et le droit international.

Note 27 Voir, par exemple, le projet B-Tech mené par le Haut-Commissariat des Nations unies aux droits de l'homme : https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/BTechprojectoverview.pdf.

Note 28 Pour un aperçu, voir https://www.iss.europa.eu/sites/default/files/EUISSFiles/CCB%20Report%20Final.pdf et https://www-tandfonline-com.ezp.lib.cam.ac.uk/doi/full/10.1080/23738871.2017.1294610.

ce qui concerne la relation entre les pays développés et les pays en développement, mais aussi entre les pays en développement eux-mêmes. Si le partage des connaissances et des compétences a le potentiel de renforcer la coopération et d'améliorer les capacités techniques, politiques et juridiques en matière de sécurité numérique, il pourrait également reproduire, voire aggraver, les inégalités et les dépendances existantes, reproduisant ainsi les hiérarchies de pouvoir existantes sur la scène internationale. Il a également été souligné que la duplication des législations existantes, sans tenir compte du contexte local, pourrait conduire à un contrôle accru des citoyens, mettant ainsi les droits de la personne humaine en danger. Sans une coordination suffisante et l'adhésion à des principes généraux, ces initiatives de renforcement des capacités risquent de devenir des projets à court terme et auto-centrés.

Dans ce contexte, la pérennité des efforts de renforcement des capacités en matière de cybersécurité est apparue comme un sujet de préoccupation majeur et constituera probablement l'un des défis les plus importants à l'avenir. Les initiatives de renforcement des capacités en matière de cybersécurité devront encourager l'adoption de mesures visant à promouvoir la sécurité de l'environnement numérique, sans restreindre indûment l'accès aux données et aux outils de sécurité et les possibilités de les utiliser (par exemple, en imposant des exigences plus strictes en matière d'enregistrement et de consignation des données). En d'autres termes, il faudra veiller à ce que les mesures de cybersécurité n'entravent pas le développement numérique, social et économique des États les moins avancés, qui ne sont pas toujours en mesure de supporter les coûts élevés d'une sécurisation numérique aussi rapide que possible. Trouver le bon équilibre entre cybersécurité et développement sera un facteur clé dans les efforts futurs pour réduire la fracture numérique.

3.3. L'intelligence artificielle

La donnée est l'actif préalable nécessaire au développement et au fonctionnement de l'IA. Les inégalités en termes d'accès aux données numériques et de capacités de sécurité numérique se traduisent et s'amplifient également dans le domaine de l'IA. Ce constat a deux conséquences principales.

Tout d'abord, la plupart des données sont collectées et stockées par un nombre limité d'acteurs opérant depuis certaines régions du monde, ce qui rend plus difficile l'émergence d'autres acteurs et le développement de leurs propres applications d'IA. Ainsi, les inégalités déjà existantes en termes de collecte et de stoc-

kage des données ont des conséquences sur la capacité à développer des applications d'IA à la fois en termes d'acteurs impliqués mais aussi en termes de localisation géographique.

Deuxièmement, il existe des inégalités importantes concernant la quantité de données collectées et traitées par les différents groupes de population dans le monde. Cela a un impact direct sur le développement des applications d'IA, qui ont tendance à s'appuyer sur les données des pays occidentaux, créant ainsi des biais importants. Ces biais affectent la légitimité des applications d'IA, en particulier lorsqu'elles sont utilisées à des fins d'application du droit.

L'IA a également la capacité de transformer les processus d'élaboration du droit, la substance et l'application du droit international, comme cela a déjà été évoqué. Cela peut avoir des conséquences doubles et opposées sur la fracture numérique. D'une part, la fracture numérique, et en particulier l'inégalité dans l'accès aux données, affecte également la capacité des États et des autres acteurs à bénéficier des solutions de l'IA en matière de droit international. Il pourrait s'agir d'une question sur laquelle les États pourraient accroître leurs efforts de renforcement des capacités ainsi que le partage des données, afin de permettre à davantage d'États d'accéder à ces données et d'utiliser ces applications d'IA. Une telle approche serait bénéfique pour la mise en œuvre des règles et principes du droit international ainsi que pour l'ordre international fondé sur des règles en général. D'autre part, les solutions basées sur l'IA peuvent aider les États aux capacités plus limitées à traiter une plus grande quantité de données et améliorer leur capacité à participer aux processus d'élaboration et d'interprétation du droit. Cette dernière remarque dépendra de la volonté des États de coopérer et de partager les données et les solutions d'IA dans ce domaine.

L'IA peut également jouer un rôle dans la réduction de la fracture numérique et de ses conséquences juridiques internationales. Les applications d'IA peuvent être utilisées pour collecter et traiter de grands ensembles de données sur différentes questions et ainsi aider à identifier des solutions possibles, par exemple, sur la façon dont une obligation juridique internationale spécifique est appliquée au niveau national. Dans cette perspective, l'IA peut offrir des solutions pertinentes pour les mécanismes de vérification et d'application des traités.

4. Conclusion

Les défis posés au droit international par les données, la sécurité numérique et l'IA sont de trois ordres. Ils concernent la relation entre acteurs publics et privés, soulignant les difficultés d'adaptation des mécanismes interétatiques du droit international au profit d'une nouvelle façon d'envisager la normativité, mais aussi la manière dont le droit est produit et mis en œuvre. Le second défi concerne la politique juridique, qui voit s'opposer les modèles culturels, politiques et juridiques que le droit international doit s'efforcer de faire dialoguer. Enfin, ces enjeux numériques ont mis en évidence la fracture numérique d'un point de vue économique, mais aussi du point de vue du développement durable.

Mais à ces défis correspondent aussi des opportunités offertes par le numérique. Les données et l'IA offrent également des moyens de combler les inégalités entre les États et d'améliorer la condition humaine. Par ailleurs, si le droit international semble parfois être affecté par les évolutions technologiques, celles-ci peuvent aussi l'aider à progresser, voire à le modifier. La collecte de données permet de mieux comprendre la pratique des acteurs des relations internationales et l'IA peut faciliter la mise en œuvre du droit international.

Les défis et les opportunités que les technologies numériques représentent pour le droit international soulignent la pertinence du renforcement des capacités juridiques. Ce renforcement a deux objectifs principaux. D'une part, contribuer à une meilleure compréhension de la substance du droit et de la manière dont il s'applique dans un contexte spécifique, par exemple, en ce qui concerne les différentes technologies abordées dans ce Livre blanc. D'autre part, contribuer à l'élaboration de réglementations et de politiques nationales et régionales conformes aux obligations du droit international, ainsi qu'à la mise en œuvre de ces obligations. Dans cette perspective, le partage des bonnes pratiques est un élément important du renforcement des capacités juridiques.

Cette deuxième partie montre donc les interrelations entre les données, la sécurité numérique et l'IA ; entre les défis qu'elles soulèvent ; entre les opportunités qu'elles présentent, et enfin entre chacun de ces éléments, posant ainsi des questions substantielles, qui pourraient alimenter les futurs débats et recherches.

3.

les questions juridiques

En confrontant les instruments juridiques décrits dans la première partie avec les principaux défis mis en évidence dans la deuxième partie, cette dernière partie identifie certaines des questions les plus saillantes concernant le développement futur du droit international sur les données numériques, la sécurité numérique et l'IA. En effet, l'adéquation des règles juridiques existantes est constamment évaluée à la lumière des impacts conceptuels et réels des nouveaux développements technologiques. Les discussions académiques et politiques existantes débattent souvent de la question de savoir si les règles juridiques internationales actuelles sont suffisamment claires, précises et complètes pour suivre le rythme rapide de la numérisation, bien qu'il existe également un scepticisme quant au fait que les technologies numériques donnent lieu à des défis juridiques fondamentalement distincts et ont un impact plus important sur le droit international que d'autres développements technologiques ou sociaux. Les sections suivantes donneront un aperçu bref et non exhaustif de certaines des principales questions juridiques qui émergent dans les domaines des données numériques, de la sécurité numérique et de l'IA. Auparavant, il convient de souligner les questions transversales et communes que les activités numériques poseront au droit international futur.

1. Les questions juridiques transversales

En raison de la difficulté du dialogue entre les États pour répondre juridiquement aux besoins du secteur numérique, de nombreuses initiatives non étatiques ont vu le jour pour proposer des interprétations du droit international, voire de nouvelles normes (par exemple, le *Manuel de Tallinn*, la Global Commission on the Stability of Cyberspace, etc.). Des groupes d'experts juridiques se penchent également sur le secteur numérique (par exemple, la Commission de droit international sur la protection des données personnelles dans les flux transfrontières d'informations ; l'Institut de droit international sur l'applicabilité du droit international aux cyberactivités). Sans aucun doute, l'ILA/ADI a un rôle à jouer dans la réflexion à mener sur l'évolution du droit international du numérique.

C'est un truisme de dire que les acteurs non étatiques doivent être pris en compte dans les modes de formation et d'application du droit, et d'autant plus dans le contexte du droit numérique. Il pourrait toutefois être utile de réfléchir à une typologie des différentes manières dont la relation entre le privé et le public peut fonctionner ou fonctionne en relation avec le droit international. À un niveau plus théorique, on pourrait se de-

mander si les questions numériques changent la façon dont le droit international traite traditionnellement les acteurs non étatiques. À un niveau plus pratique, cette typologie pourrait formuler des propositions pour mieux mettre en œuvre le droit international. Par exemple, il serait possible de différencier les entreprises privées selon qu'elles agissent : 1) en tant qu'agents des États dans l'exercice de leur prérogative de puissance publique (par ex. en protégeant, respectant et appliquant les droits de l'homme au nom d'un État) ; 2) en tant que compléments à l'accomplissement par l'État de ses fonctions/responsabilités/obligations (le conseil de surveillance de Meta a intégré le droit international des droits de l'homme dans son processus décisionnel) ; 3) en tant que concurrents des États dans l'exercice de leurs droits souverains (par ex. en élaborant leurs propres normes de sécurité numérique, susceptibles d'aller à l'encontre des demandes de décryptage de l'État) ; 4) en tant que substituts, dans l'exercice de fonctions relevant traditionnellement de la compétence d'un État (que ce soit en termes de données ou de défense) ; ou 5) en tant qu'acteurs autonomes qui croisent les acteurs publics tout en défendant leurs propres intérêts (par exemple, en décidant de coopérer ou non avec les demandes de coopération des forces de l'ordre, en concevant leurs propres interprétations du droit international et, à l'occasion, en les appliquant).

Il semble également nécessaire d'examiner comment les TIC modifient le droit international. Il est classique de réfléchir aux adaptations du droit international pour répondre aux besoins découlant des évolutions technologiques. Ces réflexions doivent nous amener à penser ou repenser le droit international institutionnel et matériel, l'évolution des normes mais aussi des sources, les processus de formation du droit international et les produits de ces processus. Mais il est également nécessaire de comprendre ce que ces TIC peuvent apporter au droit international. Nous savons que les solutions techniques peuvent compléter les solutions juridiques (par exemple, la protection de la vie privée *by design* ou *by default*). Mais le droit peut aussi utiliser les nouvelles technologies dans le domaine de la preuve, de l'identification de la pratique étatique ou de l'*opinio juris,* par exemple ; il le fait également dans le domaine de l'e-justice ou de la *legal tech*. Comment envisager les interrelations entre le droit international et les TIC ?

2. Les données numériques

Clarification du droit existant. L'identification des règles applicables aux données numériques et la clarification de leur interprétation seront l'un des principaux défis juridiques des prochaines décennies. Il est nécessaire de préciser davantage la manière dont le droit international s'applique aux données numériques, tout en façonnant l'évolution du droit de manière à refléter un large éventail d'intérêts et d'objectifs légitimes, notamment les impératifs parfois contradictoires des droits de l'homme et de la vie privée, de l'application du droit et de la sécurité nationale. Selon plusieurs entretiens avec des experts, l'interprétation des dispositions relatives à la vie privée dans le droit international des droits de l'homme revêtira une importance particulière, car le droit à la vie privée est l'un des droits fondamentaux qui a le plus rapidement évolué et de façon très malléable. La Cour européenne des droits de l'homme (CEDH) et la Cour de Justice de l'Union européenne (CJUE) en particulier sont à l'avant-garde du contentieux international en matière de protection de la vie privée et des données, devant trancher des affaires de plus en plus complexes et litigieuses, par exemple sur la surveillance de masse et ciblée par des acteurs publics et privés, sur l'interception et le stockage de données personnelles pour lutter contre la cybercriminalité, sur l'extraterritorialité des régimes de protection des données et sur les principaux paramètres de la protection des données elle-même (la notion de données, le droit à l'oubli, le droit à la rectification, etc.)[29]. Outre la coordination ou le conflit entre les approches de la CEDH et de la CJUE, la mesure dans laquelle d'autres organisations et tribunaux régionaux sont en mesure de développer leurs propres conceptions de la protection des données sera également importante, notamment en raison de l'influence croissante du RGPD européen. La clarification et l'interprétation des règles existantes seront également un sujet de préoccupation dans d'autres domaines du droit international qui impliquent des questions relatives aux données numériques. Il existe, par exemple, en droit international humanitaire, une grande incertitude quant à la question de savoir si les données numériques doivent être classées ou non comme bien pendant un conflit armé, et en droit commercial international (les données sont-elles un bien comme un autre, pouvant être appréhendé par les règles existantes, peut-être avec de légères modifications ?

Note 29 CEDH, *Guide sur la jurisprudence de la Cour européenne des droits de l'homme - Protection des données* (mise à jour le 31 décembre 2021) ; CJUE, *Fiche thématique sur la protection des données à caractère personnel* (mise à jour le 11 novembre 2021).

Comment prendre en compte les données produites par le commerce international ?).

Fragmentation de la réglementation. La clarification du droit sera particulièrement difficile étant donné le manque relatif d'harmonisation des initiatives existantes. Les États et les organisations internationales défendent souvent des conceptions concurrentes de la protection des données, ce qui se reflète dans les instruments juridiques qu'ils adoptent. Les différences entre l'approche de l'Union européenne en matière de protection des données, qui est axée sur les droits fondamentaux et l'autonomie personnelle, et les approches des États-Unis et d'autres États puissants comme la Chine et la Russie, seront probablement à l'origine d'importantes confrontations politiques au cours des prochaines décennies (voir la section ci-dessus sur la politique juridique en matière de données numériques). Même si le RGPD jouit déjà d'une influence considérable sur de nombreuses politiques nationales et régionales en matière de protection des données, on observe une tendance croissante à la nationalisation des normes et des lois relatives à la protection et à la sécurité de l'environnement numérique, ce qui pourrait fragiliser et compromettre davantage l'interopérabilité juridique des régimes juridiques internationaux, régionaux et nationaux pertinents. Le secteur privé a déjà commencé à mettre en place l'infrastructure nécessaire pour faire face à la fragmentation (voir Microsoft qui lance le modèle de *cloud* souverain).

La compétence extraterritoriale. La fragmentation des normes existantes et la tendance à la nationalisation s'accompagnent de tentatives visant à garantir l'application extraterritoriale des instruments nationaux ou régionaux**.** Étant donné que les données jouent un rôle important pour la coopération numérique, les preuves et l'entraide judiciaire, les conflits réglementaires découlant des flux transfrontières de données et de l'extraterritorialité des régimes de protection des données (par exemple, l'affaire *Schrems* II) donneront probablement lieu à certains des principaux défis juridiques dans le domaine des données numériques. La tendance à l'affirmation de la compétence extraterritoriale peut être structurelle. Dans la mesure où les États moins dominants sur le plan technologique s'efforcent de rattraper leur retard, ils sont susceptibles de recourir à une réglementation unilatérale et extraterritoriale pour tenter de garder le contrôle de leurs données numériques, et cela vaut pour l'UE comme pour les pays en développement.

Implications en matière de droits de l'homme. La collecte, le partage et la vente de données numériques, en particulier de données personnelles, ont d'importantes répercussions sur les

droits de l'homme, tant positives que négatives. Des pratiques telles que la publicité ciblée, le contrôle de contenu, la surveillance privée et publique, l'espionnage, la collecte de données pour les enquêtes criminelles, le filtrage d'internet, l'utilisation de données biométriques, etc. peuvent mettre en danger la vie privée et la liberté d'expression. Mais les données numériques et l'IA peuvent également contribuer à améliorer la condition humaine. Du point de vue des individus, l'un des principaux défis des prochaines décennies sera de faire en sorte qu'ils puissent suivre et garder le contrôle de leurs données.

Questions-clés

- Quels sont les différents types d'instruments et de mécanismes juridiques qui pourraient être développés afin d'assurer une protection efficace des données numériques par les entreprises technologiques ? Comment concevoir les relations entre acteurs privés et publics pour favoriser à la fois la circulation et la protection des données numériques ?
- Comment la communauté internationale va-t-elle gérer les ramifications juridiques (fragmentation réglementaire, extraterritorialité, etc.) d'une confrontation politique omniprésente entre des États prônant des modèles concurrents de protection des données ?
- Comment la communauté internationale pourrait-elle prévenir et atténuer les effets néfastes de l'accès inégal aux données numériques, notamment au big data ? Comment construire un droit des données véritablement international ?
- Comment les données peuvent-elles combler le fossé numérique, faciliter la réalisation des ODD et améliorer la condition humaine ?

3. La sécurité numérique

Fragmentation de la réglementation. Très peu de lois et de règlements sont harmonisés dans le monde. C'est le résultat à la fois d'un manque d'instruments universels mais aussi de visions différentes du cyberespace. Dans le domaine de la cybercriminalité, et malgré les efforts déployés pour faciliter la coopération, celle-ci reste compliquée ; la fragmentation réglementaire et le manque de coopération ralentissent, voire entravent les enquêtes criminelles. Un autre aspect de la fragmentation réglementaire concerne les exigences de sécurité. Ces exigences et les législations visant à renforcer la sécurité sont élaborées dans le monde entier. Outre la fragmentation du droit qui en résulte, le risque est grand de voir se développer des obligations contradictoires (par exemple dans le domaine de la cryptographie, de la divulgation des vulnérabilités, etc.) ou des obligations qui pourraient créer des vulnérabilités pour tous et menacer la sécurité juridique. La fragmentation réglementaire remet également en cause la mise en œuvre des mesures visant à contrer les opérations de désinformation, les discours de haine et plus globalement la lutte contre les contenus préjudiciables.

Incidences sur les droits de l'homme. La lutte contre les menaces numériques a des répercussions à la fois positives et négatives sur les droits de l'homme. D'une part, alors que l'espace numérique est de plus en plus utilisé pour mener des opérations informationnelles et que la désinformation prolifère, les États et les acteurs non étatiques impliqués dans le retrait des contenus exercent une pression sur plusieurs droits, notamment la liberté d'expression, le droit à un recours effectif ou l'interdiction de la discrimination. Dans le même ordre d'idées, l'extension des programmes de surveillance, ciblés ou non, et le succès de l'industrie de la surveillance, remettent en cause de nombreux droits et libertés fondamentaux. La numérisation des sociétés a également généralisé l'utilisation de preuves électroniques dans les enquêtes criminelles. La nécessité d'accéder aux preuves électroniques dans un délai très court peut remettre en cause l'obligation pour les États de protéger les droits de l'homme, notamment dans le cas de demandes extraterritoriales adressées à un fournisseur de services concernant des données relatives à un citoyen étranger. Les difficultés rencontrées pour accéder aux preuves électroniques peuvent inciter les États à opter pour la surveillance de masse, érodant ainsi la confiance dans les institutions publiques, l'État de droit et les libertés fondamentales. Comme le nombre de données augmente plus rapidement que le rythme de la coopération juridique, les ten-

dances décrites ci-dessus risquent de se poursuivre. D'autre part, le respect et la protection des droits de l'homme passent nécessairement par une plus grande sécurité numérique. Cela remet en question le rôle de la sécurité numérique dans la définition et l'évaluation des obligations des États, des organisations internationales et des acteurs non étatiques.

Multilatéralisme et droit international. La sécurité numérique remet en question la capacité du multilatéralisme à traiter de nouvelles questions et constitue une condition pour assurer son avenir. La vérification des engagements a été mise en évidence comme l'un des principaux défis à relever pour assurer le respect de nouvelles règles contraignantes dans le domaine des TIC dans le contexte de la sécurité internationale, ce qui pourrait également expliquer la réticence des États à s'entendre publiquement sur la plupart des questions. Mais la question de la vérification a des implications plus larges que la vérification d'éventuelles nouvelles obligations. Le nombre croissant d'activités malveillantes en ligne, la multiplication des sources d'information et la manipulation de l'information elle-même remettent en question la capacité de vérifier les informations en ligne, ce qui accroît la méfiance et la conflictualité. Objet du multilatéralisme, la sécurité numérique ne cesse également de questionner la place et le rôle des acteurs non étatiques dans son élaboration. En tant qu'exigence, la sécurité numérique jouera un rôle clé dans les modalités de négociation (protection de l'information) mais aussi dans la capacité des organisations internationales à assurer le niveau de protection pertinent pour leurs informations.

La compétence extraterritoriale. Compte tenu de la nature même des activités numériques malveillantes et des caractéristiques de l'espace numérique par rapport à la territorialité de la loi, la compétence extraterritoriale a été et sera un défi juridique majeur pour les années à venir. Cela est d'autant plus vrai que les menaces vont augmenter en nombre et en sophistication, tandis que la coopération restera probablement tendue dans de nombreux domaines, compte tenu du niveau de méfiance entre les États et du manque de capacités pour contrer les menaces émergentes.

Questions-clés

- Le rôle des acteurs privés dans le déclenchement ou la réponse à des activités malveillantes remet-il en question la manière dont le droit international traite les acteurs privés ?
- La communauté internationale sera-t-elle en mesure de parvenir à un consensus sur l'application et la signification des règles et des concepts de droit international existants en matière de sécurité numérique, ou de nouveaux concepts seront-ils élaborés ?
- Y a-t-il, et si oui, quel sera le rôle de la sécurité numérique par rapport aux autres obligations internationales ?
- Comment optimiser le renforcement des capacités dans le domaine cyber et le partage des technologies pour que les pays en développement soient en mesure d'assurer leur sécurité numérique ?

4. L'intelligence artificielle

Un premier défi juridique, qui a été souligné précédemment, concerne la confusion entre les questions juridiques et éthiques, et le fait que la plupart des processus et initiatives actuels tendent à se concentrer principalement sur l'éthique plutôt que sur le droit. Comme indiqué dans les sections précédentes du rapport, ce n'est pas un problème en soi et le travail sur les questions éthiques a également profité aux discussions juridiques. Pourtant, dans certaines circonstances, une telle approche peut affecter le contenu des normes juridiques internationales.

L'absence d'une définition claire et consensuelle de l'IA et de la plupart de ses notions connexes (autonome, machine, robot, système, etc.) crée d'importants défis juridiques. Ce défi de définition amplifie un autre défi connexe : le fait qu'il existe plusieurs processus et initiatives parallèles en cours en même temps. Comme ces différentes initiatives et processus peuvent utiliser un vocabulaire différent pour décrire des questions similaires, il est plus difficile d'identifier les éventuels chevauchements ou divergences.

Il existe également une incertitude quant à savoir si et comment les États doivent appliquer les règles traditionnelles du droit international à l'IA. Ce défi est lié à celui de la définition, pour deux raisons. Premièrement, il devient difficile d'identifier l'objet de la discussion et les conséquences potentielles de la réglementation. Deuxièmement, certaines discussions sur l'IA ont tendance à être très générales, alors qu'à des fins juridiques, il peut être nécessaire d'adopter une approche plus granulaire sur les différentes formes d'applications de l'IA et leurs conséquences.

Il n'existe actuellement aucune compréhension générale de la manière dont le droit international devrait réglementer l'application de l'IA dans les comportements inamicaux ou hostiles des États. Cette observation a des conséquences importantes pour différents aspects du droit international, tels que l'attribution du comportement pertinent, la détermination de sa légalité et l'invocation de la responsabilité des différents acteurs impliqués. Ces difficultés touchent deux branches du droit international en particulier : le droit international des droits de l'homme et le droit des conflits armés. En ce qui concerne le droit des droits de l'homme, les principaux défis sont la détermination des implications en matière de droits de l'homme des logiciels de reconnaissance faciale, les biais discriminatoires dans les algorithmes, l'attribution et la responsabilité des violations des droits de l'homme occasionnées par l'emploi de l'IA. Du point de vue du droit des conflits armés, il existe des défis concernant la réglementation de certains moyens et méthodes de guerre ainsi que l'évaluation de l'évolution technique des armements et de leurs conséquences juridiques. Tous ces défis sont exacerbés par les relations qui peuvent exister entre les États et les acteurs non étatiques dans le développement et l'utilisation des technologies d'IA. Le recours à des solutions d'IA développées par différents acteurs pour la prise de décision ainsi que dans les systèmes autonomes peut soulever des questions liées à l'attribution et à la responsabilité individuelle, notamment en ce qui concerne la responsabilité du commandement et la responsabilité pénale individuelle. L'imbrication des activités menées par des acteurs non étatiques et des États peut également soulever des questions liées à l'obligation de rendre des comptes et à la manière de réparer les dommages causés par les technologies basées sur l'IA, même en l'absence de comportement fautif. Enfin, cette situation soulève également

la question de savoir comment les acteurs non étatiques, en développant certaines technologies d'IA, devraient et peuvent tenir compte d'éventuelles obligations juridiques internationales, notamment en matière de droits de l'homme.

L'IA soulève des défis importants pour le droit international, mais elle offre également de nouvelles solutions pour les processus d'élaboration et d'interprétation du droit, ainsi que pour l'application du droit international. Plus généralement, l'IA offre également de nouvelles solutions qui peuvent avoir un impact positif sur les défis auxquels la communauté internationale est déjà confrontée, par exemple en contribuant à réduire la fracture numérique.

Questions-clés

- Comment prendre en compte la diversité des technologies et applications liées à l'IA et la diversité des questions juridiques qu'elles soulèvent ?
- Comment prendre en compte la diversité des acteurs impliqués dans le développement et le déploiement des technologies d'IA, notamment en termes de responsabilité et d'obligation de rendre des comptes ? Les futurs instruments juridiques relatifs à l'IA devraient-ils se concentrer sur des applications sectorielles spécifiques ou tenter d'aborder la question de manière globale ?
- Comment les États appliqueront-ils les règles traditionnelles du droit international aux technologies et solutions liées à l'IA, notamment le droit des droits de l'homme et le droit des conflits armés ?
- Comment combler le fossé entre les États en matière d'accès aux données pour le développement des technologies d'IA et plus généralement d'accès à l'IA ?
- Comment les solutions d'IA contribuent et contribueront à l'avenir au développement, à l'interprétation et à l'application du droit international ?

Conclusion

Au-delà des trois thématiques abordées (données, sécurité numérique et IA) et des trois défis identifiés (frontières entre le public et le privé, politique juridique dans le cyberespace, fracture numérique), il a été possible de soulever un certain nombre de questions susceptibles de nourrir nos futurs débats et recherches autour de thématiques juridiques déjà connues :

- Les sources du droit, la formation du droit, son interprétation et son développement progressif, la nécessité de nouvelles règles ;
- Les compétences des États, l'extraterritorialité ;
- La preuve ;
- La responsabilité et l'*accountability* ;
- et plus théoriquement la nature et la formulation du droit international.

Les questions et technologies numériques constituent à la fois un défi et une opportunité pour le droit international. Les différents sous-thèmes ont mis en évidence certaines spécificités pour chacun d'entre eux. Cependant, les aspects techniques de chaque thème ne doivent pas être surestimés car de nombreux défis et questions juridiques sont partagés par les trois sous-thèmes.

annexe 01

les personnes auditionnées

(par ordre alphabétique)

- Ian Barber, Juriste principal, Global Partners Digital.
- Rogier Creemers, Professeur assistant en études chinoises modernes, Université de Leiden.
- Bertrand de la Chapelle, Cofondateur et directeur du Réseau des politiques Internet et juridictionnelles.
- Viola de Azevedo Cunha, Chargée de recherche principale, Bureau de la recherche de l'Unicef.
- Carlo di Nicola, Juriste principal, UNIDROIT - Institut international pour l'unification du droit privé.
- David Emm, Chercheur principal en sécurité, Kaspersky.
- Sherif Hashem, Professeur de sciences et technologies de l'information, Université George Mason.
- Kubo Mačák, Conseiller juridique, Comité international de la Croix-Rouge.
- Angela McKay, Directrice des menaces et de l'atténuation des risques, Google.
- Marko Milanovic, Professeur de droit international, Université de Nottingham.
- Folake Olagunju, Responsable du programme Internet et cybersécurité, CEDEAO.
- Patryk Pawlak, Responsable exécutif du Bureau de Bruxelles, Union européenne pour les études de sécurité et directeur de projet, EU Cyber Direct.
- Kavé Salamatian, Professeur d'informatique, Université de Savoie, et responsable de la chaire européenne ERA en cybersécurité, Université de technologie de Tallinn.
- Alexander Seger, Chef de la Division de la cybercriminalité, Conseil de l'Europe.
- Johanna Weaver, Directrice du Tech Policy Design Centre, Australian National University.
- Richard Wingfield, Chef du service juridique, Global Partners Digital.
- Moctar Yedaly, Ministre adjoint, Ministère des Transports et de l'infrastructure de la Mauritanie.

Les entretiens

Le contenu du livre blanc s'appuie sur une série d'entretiens, réalisés entre novembre 2021 et janvier 2022, sur les questions qui ont intéressé le Comité (données numériques, sécurité numérique, intelligence artificielle et défis numériques en général). Le Comité a sélectionné des experts juridiques et non juridiques issus d'horizons professionnels variés (milieu universitaire, gouvernement, société civile, secteur privé, *etc.*).

Chaque entretien a duré 50 minutes et comprenait une présentation de 10 minutes par la personne auditionnée, suivie de 40 minutes de discussion avec le comité. Aucune exigence particulière n'a été formulée quant au contenu de la présentation.

DANS LA MÊME COLLECTION

Alimentation / Agriculture

Anthropocène

Lutte contre la corruption

Crimes de masse et impunité

Démocratie et état de droit

Droits de la personne humaine

Énergie

Entreprises et droits de la personne humaine

Espace extra-atmosphérique

État civil

Finance internationale

Fiscalité

Gouvernance mondiale

Investissements internationaux

Migration

Défis du numérique pour le droit international

L'océan

Les ODD au-delà de 2030

Patrimoine culturel

Propriété intellectuelle

Règlement des différends

Santé

Travail

Villes en droit international

livre blanc n° 16 - Défis du numérique pour le droit international
réalisation : 23 juillet 2022
création graphique : clémence hivert - *bluclemence@gmail.com*

www.ilaparis2023.org

Consultation publique du 1er septembre au 31 décembre 2022

adi-ila2023-dinum@laposte.net