LA GÉOPOLITIQUE DE L'INTELLIGENCE ARTIFICIELLE : RÉGULATION ET PUISSANCE

Karim BENYEKHLEF[1] & Jie ZHU[2]

1 Karim Benyekhlef est professeur titulaire, directeur du Laboratoire de cyberjustice et titulaire de la Chaire LexUM en information juridique du Centre de recherche en droit public, Faculté de droit, Université de Montréal.

2 Jie Zhu est avocate, agente de recherche et docteure en droit au Laboratoire de cyberjustice de la Faculté de droit, Université de Montréal.

TABLE DES MATIÈRES

INTRODUCTION

[1] De nos jours, le numérique est devenu un enjeu stratégique dans les rapports de puissance entre États. L'intelligence artificielle (IA), dont les formidables développements récents ont partie liée avec l'émergence et le déploiement du cyberespace et des données massives (*big data*), constitue la composante essentielle d'une lutte bel et bien engagée et dont l'objectif est d'assurer aux États un avantage stratégique décisif dans l'appropriation, le contrôle et, *in fine*, la domination de et par cette technologie aux usages si variés. L'IA représente ainsi un enjeu géostratégique aux dimensions militaires affirmées. On présume, en effet, que l'IA permettra notamment une meilleure coordination sur le champ de bataille et une résilience améliorée des systèmes, des réseaux de communication, des capteurs et des interfaces homme-machine en cas de conflit (SPECIAL COMPETITIVE STUDIES PROJECT, 2022). C'est sans évoquer le recours à des systèmes létaux autonomes (BARRIER, 2018; MCFARLAND, 2020; COMITÉ INTERNATIONAL DE LA CROIX ROUGE, 2021).

[2] La compétition autour de l'IA ne se limite pas à la seule question militaire, même si celle-ci revêt des dimensions préoccupantes; elle porte également sur des enjeux économiques de première importance. Il s'agit là aussi de s'assurer un avantage compétitif crucial dans le développement et le déploiement des outils d'IA et de commander ainsi une position prééminente dans le marché. L'IA devient alors une question *géoéconomique*. La géoéconomie « is […] about shaping and managing the strategic environment in which the states operate for the pursuit of their national interests by economic means » (VIHAM, 2018, p. 4). Le contexte international actuel est en effet propice à la réémergence de la géoéconomie « as a favoured form of geopolitical combat for some of the world's most powerful states and shaping the outcomes of some of the world's most important strategic challenges […] the grand strategies of the twenty-first century geopolitics will be pursued chiefly through economic means » (VIHAM, 2018, p. 1). La géoéconomie est au cœur de l'action récente des États-Unis, que ce soit par le recours aux sanctions économiques, des atteintes courantes aux principes du libre-échange au nom de la sécurité nationale, le refus de se soumettre aux décisions des panels de l'OMC[3], des mesures protectionnistes propres à permettre la réindustrialisation[4], etc. L'hégémon américain cherche aussi à maintenir sa prééminence dans le champ commercial du numérique et de l'IA et à défendre l'avantage acquis de ses champions nationaux (Google, Amazon, Facebook, Apple, etc.). Cette posture géoéconomique est confortée par la position prépondérante des États-Unis dans le système financier international et la dollarisation de celui-ci qui leur permet de contrôler les chaînes de valeur et une portion appréciable

3 Lire la déclaration de l'*Office of the United States Trade Representative* à la suite d'une série de décisions de panels de l'OMC rejetant l'exception de la sécurité nationale dans l'imposition de tarifs sur l'acier et l'aluminium imposés par l'administration Trump et prolongés par celle de Biden : « The United States strongly rejects the flawed interpretation and conclusions in the World Trade Organization (WTO) Panel reports released today regarding challenges to the United States' Section 232 measures on steel and aluminum brought by China and others. The United States has held the clear and unequivocal position, for over 70 years, that issues of national security cannot be reviewed in WTO dispute settlement and the WTO has no authority to second-guess the ability of a WTO Member to respond to a wide-range of threats to its security » (OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, *Statement from USTR Spokesperson Adam Hodge*, 9 décembre 2022, en ligne : <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/december/statement-ustr-spokesperson-adam-hodge>.

4 Voir le H.R. 4346 – *Chips and Science Act*, entré en vigueur le 9 août 2022 (Pub. L. 117-167), en ligne : <https://www.congress.gov/bill/117th-congress/house-bill/4346/text>. Sur cette question, lire William Alan REINSCH et Thibault DENAMIEL, « The CHIPS and Science Act Guardrails' Implications for the U.S. Trade Agenda », Center for Strategic & International Studies (CSIS), 13 avril 2023, en ligne : <https://www.csis.org/analysis/chips-and-science-act-guardrails-implications-us-trade-agenda>.

du commerce international dès lors que le dollar est utilisé dans une transaction ou qu'une composante *made in USA* se retrouve dans le produit ou l'outil transigé[5].

[3] Les enjeux d'ordre géopolitique apparaissent donc substantiels. Ils recouvrent des considérations de puissance qui animent les États et, au premier chef, les États-Unis et la Chine et, plus en arrière-plan, l'Union européenne. Cette con, dépourvue de capacité industrielle et d'entreprises numériques à vocation globale, entend peser par le recours à la régulation[6]. Les appels à la régulation de l'IA, en particulier, se multiplient depuis l'émergence des *Large Language Models* (Grands modèles de langage), type ChatGPT-4. Nous n'examinerons pas ces différents projets de régulation de l'IA qui se multiplient, mais dont on saisit parfois mal comment ils entendent réguler, au sens le plus juridique du terme, un phénomène aussi disparate et protéiforme. Une régulation fondée sur les risques (LATIL, 2023) semble emporter la faveur de certains. Elle suppose, à l'instar de la Législation sur l'IA de l'Union européenne, un modèle de conformité (*compliance*) fondé sur des règles techniques (standards) sujettes à des audits et des certifications. Il n'est pas clair qu'un tel modèle soit en mesure de refléter les exigences juridiques relatives aux droits fondamentaux, ni d'en permettre la pleine réalisation. En tout état de cause, il faut surtout se demander, dans le cadre de la présente contribution, si une régulation véritable et effective s'avère possible dans un contexte de compétition internationale exacerbée par des considérations liées à la sécurité nationale et à la volonté de puissance. Une régulation verrait sans doute le jour, dans l'Union européenne en particulier, mais quelle sera la portée de celle-ci ? Cette dernière aura-t-elle une incidence significative et réelle ? Ou se heurtera-t-elle très rapidement aux réticences soutenues, voire catégoriques, de l'hégémon américain si celle-ci limite, d'une quelconque manière, le champ d'action des opérateurs américains ? Il nous apparaît que si la régulation de l'IA par l'UE se limite à une approche fondée sur la conformité (*compliance*), il est possible que celle-ci ne suscite pas l'hostilité des États-Unis. En effet, la conformité impose des contraintes de nature administrative, voire bureaucratique, auxquelles les entreprises sont habituées et qui ne limite qu'à la marge la capacité d'action et de manœuvre de ces dernières. Cela dit, nous n'aborderons pas la question si difficile d'une régulation effective de l'IA.

---

5 Sur les stratégies américaines de guerre économique qui passent notamment par le droit, lire entre autres Ali LAÏDI, *Le droit, nouvelle arme de guerre économique*, Paris, Actes Sud, 2019. Sur le recours aux sanctions comme composante de la panoplie de la guerre moderne, lire Nicholas MULDER, *The Economic Weapon. The Rise of Sanctions as a Tool of Modern War*, New Haven, Yale University Press, 2022.

6 L'économiste Élie Cohen évoque cette question dans une entrevue : « L'Europe a abandonné aux États-Unis sa souveraineté industrielle sur le matériel, et aux GAFAM et à des entreprises essentiellement américaines celles sur les plates-formes, les logiciels et les services […]. L'usage intelligent de la norme doit être appuyé par un pouvoir industriel, par une commande publique et par un contrôle du marché. Alors, être une puissance normative permettra-t-il à l'Europe de construire une puissance industrielle et technologique ? La réponse est non ! » (Sophy CAULIER, « Depuis ses débuts, le vieux Continent est hostile à l'émergence de champions », *Le Monde*, 11 septembre 2022, en ligne : <https://www.lemonde.fr/economie/article/2022/09/11/numerique-depuis-ses-debuts-l-europe-est-ouvertement-hostile-a-l-emergence-de-champions_6141160_3234.html>.

Voir Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Journal officiel, L 119, 4 mai 2016; Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle (Législation sur l'intelligence artificielle) et modifiant certains actes législatifs de l'Union, qui entrera en vigueur vingt jours suivant sa publication au Journal officiel, prévue entre mai et juillet 2024; COMMISSION EUROPÉENNE, Proposition de Directive du Parlement européen et du Conseil relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle (Directive sur la responsabilité en matière de l'IA, COM(2022) 496 final, Bruxelles, 28 septembre 2022; Commission européenne, Proposition de Directive du Parlement européen et du Conseil relative à la responsabilité du fait des produits défectueux, COM(2022) 495 final, Bruxelles, 28 septembre 2022; Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques), Journal officiel L 265 du 12 octobre 2022; Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), Journal officiel L 277 du 27 octobre 2022.

[4] Dans les lignes qui suivent, nous nous contenterons de brosser le contexte géopolitique dans lequel s'inscrivent les développements des technologies liées au numérique et à l'IA. Nous verrons alors que celles-ci constituent, en effet, une composante capitale des luttes de puissance auxquelles se livrent les États-Unis et la Chine ainsi que d'autres acteurs plutôt périphériques, comme l'Union européenne. Ces luttes recèlent de multiples dimensions, à la fois juridiques (sanctions et mesures protectionnistes), militaires et commerciales. Les dimensions commerciales passent, en premier lieu, par l'action des opérateurs économiques qui, en quelque sorte, s'inscrit dans la continuité de celle menée par les États. L'entreprise devient alors un outil dans la panoplie stratégique de l'État. On pressent les difficultés des États tiers à brider, sur le plan normatif, les entreprises des hégémons. Cette course compétitive des entreprises entre elles autour de l'IA ne sera certainement pas propice à l'encadrement normatif strict d'une technologie qui suscite de plus en plus de craintes et dont on demande qu'elle soit l'objet d'un moratoire[7]. Abordons maintenant les thèmes de la géopolitique dans le contexte du cyberespace et du numérique.

[5] La géopolitique se caractérise par une pluralité d'écoles et d'approches (ROSIÈRE, 2021; BEUCHER & CIATTONI 2021; Ó TUATHAIL, DALBY & ROUTLEDGE, 2006). Elle porte sur ces processus dynamiques de restructuration des espaces (géographiques) par les rapports de puissance, rivalités de pouvoir, alliances et solidarités qu'entretiennent différents acteurs et communautés sur la scène internationale (CATTARUZZA, 2019)[8]. La discipline met traditionnellement l'accent sur la lutte des pouvoirs entre États – en tant qu'acteurs prédominants de la politique internationale – et s'exerçant sur des territoires géographiquement délimités (LACOSTE, 2014), même si la géopolitique critique entend porter son regard sur l'analyse des discours. En effet, « les États justifient leurs politiques de puissance par des discours » et la capacité de ceux-ci « à forger des représentations et plus particulièrement à désigner l'ennemi » (ROSIÈRE, 2021, p. 19). L'avènement de l'Internet et du cyberespace opère une confusion des frontières post-westphaliennes tant en ce qui a trait aux espaces sur lesquels les rivalités de pouvoir peuvent s'exercer, qu'à l'identité des acteurs appelés à y jouer un rôle de plus en plus important. Aux territoires dont il était redondant d'adjoindre le qualificatif de « géographiques » se superpose dorénavant un cyberespace non moins investi de potentiel, de moyens comme de puissance; aux États-nations relativement monolithiques se greffent désormais des regroupements transnationaux, associations régionales, organisations supranationales, communautés déterritorialisées, plateformes et acteurs numériques qui revendiquent une autonomie croissante vis-à-vis du contrôle (juridique) des États-nations. Et on pressent bien sûr l'importance du discours autour de la maîtrise et du contrôle du cyberespace.

[7] Il ne fait plus de doute que la formidable évolution des technologies au cours des dernières décennies, culminant par les progrès importants réalisés grâce à l'IA, met au défi la puissance normative des institutions étatiques et fait de la technologie un enjeu

7 Lire à égard la lettre réclamant une pause dans la recherche et les travaux autour de l'IA générative : FUTURE OF LIFE INSTITUTE, « Pause Giant AI Experiments : An Open Letter », 22 mars 2023, en ligne : <https://futureoflife.org/open-letter/pause-giant-ai-experiments/>.

8 Aussi Amaël CATTARUZZA et Kévin LIMONIER, « Le territoire entre jeux de pouvoir et représentations » dans *Introduction à la géopolitique*, Paris, Armand Colin, 2019, p. 56, par. 29 : « L'étymologie du mot "territoire" renverrait d'ailleurs à cet imaginaire qui entoure l'espace du pouvoir : s'il est communément admis que le terme provient du latin *terra*, certains auteurs avancent qu'il proviendrait également de *terrere*, qui a donné "terreur" en français, et dont découle *territor* (celui qui répand la terreur). Autrement dit, le *territorium* renvoyait dans la Rome antique à un espace, généralement celui délimité par les murs de la cité, inspirant la terreur ».

géopolitique, voire géostratégique (DOUZET & DESFORGES, 2018). Par ailleurs, les États n'ont pas tardé, dans la poursuite de leurs intérêts nationaux, à se servir de la technologie ainsi qu'à s'allier à des acteurs numériques stratégiques. Alors que plusieurs annoncent imprudemment la fin des États à l'orée de la « quatrième révolution industrielle », la présente contribution raconte l'histoire d'une (re)conquête du cyberespace par les États, et celle de la continuation de la géopolitique sous une nouvelle forme. Ainsi, après avoir (re)tracé les frontières géopolitiques du cyberespace (I), nous ferons une étude de cas de l'IA en tant qu'une nouvelle ressource stratégique dans l'équilibre des puissances géopolitiques (II).

I. LA GÉOPOLITIQUE DU CYBERESPACE: UN OXYMORE ?

[8] La vision traditionnelle de la géopolitique se cantonne aux espaces géographiques relativement bien délimités où se déploie le jeu des puissances politiques, un jeu marqué par les rivalités internationales et luttes de pouvoir entre États westphaliens. Le cyberespace s'ancre ainsi dans « un monde cyber-westphalien » (DEMCHAK & SPIDALIERI, 2022, p. 15 « "Cyber Westphalian" world ») où se regroupent, par-delà les territoires géopolitiques traditionnels, de nouvelles communautés déterritorialisées, et où se tissent de nouveaux foyers de tension et de nouvelles dynamiques de puissance.

A. TERRITOIRE ET SOUVERAINETÉ : RETOUR AUX SOURCES

[9] En matière de géopolitique, l'intérêt premier a été, jusqu'à très récemment, porté sur les États en tant qu'acteurs principaux rythmant la dynamique des relations internationales. Et les rivalités de pouvoir s'exercent en premier lieu sur des territoires en tant qu'espaces pluridimensionnels (culturels, politiques, sociaux, économiques) appropriés, contrôlés ou marqués par différents États (CATTARUZZA & LIMONIER, 2019). Après un rappel sur le lien normatif entre territoire et souveraineté (1), nous mettrons en évidence la fluidité de la notion de frontières à l'ère contemporaine (2) avant d'aborder, dans la prochaine section (B), le tracé des frontières dans le cyberespace.

1. RAPPEL SUR LE LIEN NORMATIF ENTRE TERRITOIRE ET SOUVERAINETÉ

[10] Les juristes ont coutume d'associer la notion de territoire à la souveraineté. Quoique, d'un point de vue géopolitique, la souveraineté étatique soit une forme de contrôle ou d'appropriation de territoires parmi d'autres, elle en est sans doute la plus saillante et reconnue. Deux perspectives – interne et externe – permettent d'appréhender le concept de la souveraineté (BENEKHLEF, 2015).

[11] D'une part, la souveraineté interne désigne un pouvoir de commandement vertical rattaché à la puissance d'État. Ce rattachement implique la nécessité d'une habilitation étatique pour que les institutions appelées à produire, à appliquer ou à interpréter la norme soient autorisées à le faire au nom de l'État. En l'absence d'une habilitation étatique (qu'elle soit expresse ou implicite), les individus, les personnes morales ainsi que les autres groupements civils sont exclus de l'exercice de la souveraineté et, par ce fait même, de tout pouvoir normatif reconnu. D'autre part, la souveraineté externe d'un État se caractérise, dans l'ordre international, par une relation horizontale d'égalité, de coopération, de courtoisie et de non-intervention dans les rapports avec les autres.

[12] Cette double perspective, héritée de la théorie politique réaliste (JEANGÈNE VILMER, 2020; MEARSHEIMER, 2014), reconnaît une importance première aux traités de Westphalie (1648) comme ayant aménagé la configuration constitutive des relations internationales modernes[9][1]. Avant l'ère westphalienne prévalait le principe dynastique et le rattachement des autorités royales à une source divine. Avec les traités de Westphalie, le principe de la souveraineté territoriale exclusive se substitue aux prétentions à l'universalité des empires et aux liens de dépendance féodaux vassaliques. La souveraineté de l'État sur un territoire donné circonscrit le domaine de validité de la norme du souverain (de l'État) et lui confère le droit exclusif de gérer les affaires à l'intérieur de ses frontières territoriales sans l'ingérence d'autres États[10]. Quant aux affaires extérieures, le principe de la diplomatie confère à un État un droit d'intervention limitée dans la mesure où la souveraineté des autres États est respectée.

2. ÉVOLUTION DE LA NOTION DE FRONTIÈRES

[13] Les frontières internationales au sens westphalien constituent un sous-groupe de frontières politiques (p. ex. régionales, sociales, urbaines, culturelles) qui font office d'interfaces de séparation ou de démarcation entre deux communautés, phénomènes ou ensembles distincts[11]. Dans les mots du professeur Amaël Cattaruzza :

> Pour rendre compte de cette vision large des frontières, distincte de la simple notion de frontière internationale, Michel Foucher propose de les définir comme des « discontinuités territoriales, à fonction de marquage politique ». Les formes de ces discontinuités peuvent ainsi être appréhendées de manière plus souple, allant de la ligne au point (port, aéroport, etc.) en passant par la zone (frontières maritimes, zones grises, etc.). La ligne-frontière n'est d'ailleurs qu'une forme particulière de la frontière, qui s'inscrit souvent dans une vision européo-centrée du monde. Les modèles asiatique (« L'Empire du Milieu ») ou africain, entre autres, laissent entrevoir d'autres formes géographiques de frontières (zone-tampon, gradient, etc.), qui perdurent encore aujourd'hui dans certaines régions du monde. (CATTARUZZA, 2019a, par. 15)[12].

[14] La notion de frontières est inhérente à la règle de droit et nécessaire au partage des pouvoirs souverains[13]. Dans la tradition westphalienne, la délimitation des

9 Quoique cette interprétation des traités de Westphalie ait été remise en question par certains, dont : Benno TESCHKE, « La théorisation du système étatique westphalien : les relations internationales de l'absolutisme au capitalisme », (2012) 52 *Cahiers de recherche sociologique* 13, en ligne : <https://doi.org/10.7202/1017276ar>.

10 Et aussi, dans le contexte de l'Europe médiévale, de l'Église.

11 Pour un rendu poétique de l'omniprésence des frontières, lire : Régis DEBRAY, *Éloge des frontières*, Gallimard, 2013.

12 Lire aussi Paul KLÖTGEN, « La frontière et le droit, esquisse d'une problématique », (2012) 1962 *Revue* générale *du droit* 45, note en bas de page 4 : « […] Rome ne connaissait guère le concept de frontière ligne, mais plutôt une frontière en perpétuel devenir, non pas une limite brutale mais une zone de transition, de commerce, de communication entre le monde romain et le monde barbare ».

13 Nécessité qu'illustrent ces *Pensées* de Pascal avec ironie : « On ne voit presque rien de juste ou d'injuste, qui ne change de qualité, en changeant de climat. Trois degrés d'élévation du Pôle renversent toute la Jurisprudence. Un Méridien décide de la vérité […] Plaisante justice qu'une rivière ou une montagne borne ! Vérité au-deçà des Pyrénées, erreur au-delà. » Certains vont jusqu'à affirmer que « le droit est une science des frontières » (Paul KLÖTGEN, « La frontière et le droit, esquisse d'une problématique », (2012) 1962 *Revue générale du droit* 45).

frontières(-lignes)[14] internationales permet de consacrer, en premier lieu, le monopole du droit étatique sur un territoire donné. Elle marque la limite d'application du droit étatique[15]. Le monopole du droit étatique se comprend à la fois du droit explicitement reconnu à l'appareil étatique de dicter ses règles à ses sujets, et du droit d'un État à la non-ingérence de la part des autres États dans ses affaires intérieures. À l'extérieur des frontières nationales, des enjeux de puissance se dessinent – d'ordre militaire, économique, idéologique et technologique (BADIE, 2019) – et fondent l'action des États.

[15] Il ne fait pas de doute que l'interdépendance croissante des industries, des économies et des technologies est la toile de fond qui dilue, dans les faits, l'idéal juridique d'une absolue souveraineté des États sur leurs territoires respectifs. Cette interdépendance relativise de fait cette division qui se veut étanche entre « l'idée d'une spécificité de l'international, où aucun pouvoir absolu ne vient réguler les relations entre les acteurs, [et le] national, régulé par le pouvoir structurant de l'État » (CATTARUZZA, 2019b, par. 10). Ainsi, de la même manière que les frontières sont moins souvent transgressées que renégociées, la souveraineté, avec son caractère d'absoluité, relève davantage de la fiction juridique.

[16] Alors qu'elles conviennent au gouvernement de communautés relativement sédentaires et homogènes, les frontières westphaliennes ne rendent plus compte de la richesse et de la diversité des relations, intérêts, expériences, identités et catégories des gouvernés. La séculaire « coïncidence » des frontières territoriales, sociales et culturelles s'estompe au profit d'une interpénétration et confusion des catégories :

> Elles [les cartes géographiques] ne reflètent pas […] une parfaite concordance entre le territoire et la communauté; dans le monde contemporain, les niveaux d'appartenance – la région, la province, la nation, l'Europe pour certains, le monde – supposent un individu aux identités multiples. Au surplus, l'observateur remarque l'importance croissante des flux de populations qu'il s'agisse d'immigrants, de réfugiés, d'exilés, d'expatriés ou encore de personnes qui traversent régulièrement les frontières pour leur travail, des nomades du travail et du commerce attestant de sociétés de plus en plus multi-ethniques. On doit aussi signaler les diasporas qui exhibent des caractéristiques transnationales puisqu'elles se retrouvent dans plusieurs pays différents, maintiennent des liens importants entre elles et cultivent et protègent leurs identités d'origine. […]. Ces phénomènes bien réels s'opposent à une association

14 L'*Affaire du temple de Préah Vihéar (Cambodge c. Thaïlande)* du 15 juin 1962, décidée par la Cour internationale de justice, est généralement citée comme entérinant la vision des frontières-lignes en droit international public. Lire en particulier les pages 14 et 17 du Recueil officiel de la C.I.J. : « On voit en premier lieu que ces articles [de la Convention de frontières de 1904 entre le Cambodge et la Thaïlande] ne mentionnent pas Préah Vihéar. C'est pourquoi la Cour ne peut rendre une décision sur la souveraineté dans la zone du temple qu'après avoir examiné quelle est la ligne frontière. En second lieu, alors que, dans la chaîne des Dangrek, la frontière établie par l'article Ier devait suivre d'une manière générale la ligne de partage des eaux, le tracé exact de cette frontière devait, en vertu de l'article 3, être fixé par une Commission mixte franco-siamoise. […] En conséquence, la ligne frontière devait être, à toutes fins, celle qui résulterait des travaux de délimitation, à moins que l'on ne pût démontrer l'invalidité de la délimitation ». La notion de frontière zone, quant à elle, n'est pas parvenue à s'imposer : lire Paul KLÖTGEN, « La frontière et le droit, esquisse d'une problématique », (2012) 1962 *Revue générale du droit* 45, 52 et suiv.

15 Lire aussi Karim BENYEKHLEF, *Une possible histoire de la norme. Les normativités émergentes de la mondialisation* (2e éd.), Montréal, Thémis, 2015, p. 59 : « Sur son territoire, un territoire bien délimité, le souverain commande l'ensemble des sujets, nationaux comme étrangers, qui s'y trouvent […] ».

trop étroite entre le territoire, la communauté, l'identité et la culture. (BENYEKHLEF, 2015, p. 598–99)[16].

[17] Même sur un plan normatif, les frontières internationales semblent dépassées ou plutôt résorbées par la densité croissante des rapports « transfrontières » à géométrie variable que sont ces alliances régionales auxquelles participent différents gouvernements (p. ex. Nations Unies, Union européenne, espace Schengen, OTAN, accords de libre-échange)[17] ainsi que le foisonnement d'accords intergouvernementaux et d'initiatives conjointes ou multilatérales pour faire face aux défis globaux que sont la protection de l'environnement, les crises humanitaires, l'afflux des réfugiés, les planifications fiscales agressives, la criminalité transnationale, le blanchiment d'argent, le financement du terrorisme. Une tendance plus récente consiste en la conclusion d'accords de coopération entre différents États, pour ce qui concerne l'échange de renseignements, la coopération policière, douanière ou encore entre différentes administrations[18]. Il y a également lieu de noter la multiplication des juridictions internationales « gravitant autour » des États souverains, tels que la Cour pénale internationale (CPI) ou l'Organe de règlement des différends (ORD) de l'Organisation mondiale du commerce (OMC).

[18] On doit cependant garder à l'esprit que, outre l'absence d'un mécanisme de sanction contraignant dans l'ordre public international, l'efficacité des traités internationaux ou régionaux est bridée par la non-adhésion des plus grands joueurs internationaux. Ainsi, la Chine, la Russie et les États-Unis ne sont pas parties au Statut de Rome instituant la Cour pénale internationale (CPI) (1998). La *Convention américaine relative aux droits de l'homme* (1969), instituant la Cour interaméricaine des droits de l'homme, ne lie notablement pas les États-Unis ni le Canada. Les moyens de pression informels, mais stratégiques, que peuvent exercer certains grands États sur les activités des organisations internationales ne doivent pas non plus être sous-estimés. C'est ainsi que les États-Unis ont voulu bloquer le passage du budget de l'OMC (BASCHUK, 2019; SCHNEIDER-PETSINGER, 2020) et ont effectivement bloqué, depuis octobre 2018, la nomination des membres de son Organe d'appel dans le but d'infléchir les décisions de l'organisation dans le sens des intérêts américains[19].

16 Lire aussi Karoline POSTEL-VINAY, « Géographie et pouvoir », (2001) 10-1 *Critique internationale* 51, en ligne : <https://doi.org/10.3917/crii.010.0051>; Denis RETAILLÉ, « L'État, le territoire et les relations internationales, nouvelles approches géographiques », (1993) 68-69 *Revue des mondes musulmans et de la Méditerranée* 41, 42, en ligne : <https://doi.org/10.3406/remmm.1993.2553> : « Il y a plus de "nature" dans l'affirmation de l'ethnie (même si cela est tout à fait contestable à l'analyse), plus d'histoire dans la nation, plus d'idéologie dans une Église, etc. Les organisations spatiales en diffèrent d'autant. Les ramener à la *surface exclusive délimitée par une frontière*, c'est-à-dire au territoire pris dans son sens le plus courant, c'est raccourcir considérablement les chaînes explicatives de la relation sociale et politique par l'espace, et surtout s'interdire d'imaginer d'autres configurations que le découpage terrestre comme solution à la recherche de l'identité »; Michel FOUCHER, *Fronts et frontières. Un tour du monde géopolitique* (2e éd.), Paris, Fayard, 1991.

17 *Cf.* Jason FARR, « Point : The Westphalia Legacy and the Modern Nation-State », (2005) 80-3/4 *International Social Science Review* 156 : « The increasing power of organizations like the United Nations (UN), the World Trade Organization (WTO), and the European Union (EU) suggest that nation-state sovereignty is declining and perhaps served merely as an interlude in a world dominated by imperialistic institutions ».

18 Ces accords et échanges relèvent du transgouvernementalisme, sur ce sujet, lire Karim BENYEKHLEF, *Une possible histoire de la norme. Les normativités émergentes de la mondialisation* (2e éd.), Montréal, Éditions Thémis, 2015, p.706 et s.

19 Depuis fin mars 2020, en réponse au blocage complet de l'Organe de d'appel de l'OMC, l'Union européenne, le Canada, la Chine ainsi que seize autres membres ont mis en place un mécanisme d'appel provisoire multipartite, prenant la forme d'un arbitrage rapide prévu à l'article 25 du *Mémorandum d'accord sur les règles et procédures régissant le règlement des différends* : le *Multi-Party Interim Appeal Arbitration Arrangement* (MPIA). En date de la rédaction des présentes, 53 sur 164 membres de l'OMC ont adhéré à cette procédure provisoire, dont les décisions peuvent être consultées à l'adresse : <https://wtoplurilaterals.info/plural_ initiative/the-mpia/>.

[19] Au-delà des relations entre États, les compétences internes des États s'entrecroisent à l'envi dans la délimitation et l'aménagement de nouvelles frontières normatives comme conditions d'exercice du droit et des souverainetés nationales. En effet, le tracé des frontières s'avère un imparable exercice dans l'aménagement des modes de coexistence entre différents droits et intérêts qui peuvent entrer en conflit. Ainsi, tout l'art de gouverner consiste à départager, dans l'infinie diversité des circonstances, les droits et libertés relatifs des individus, gouvernants-gouvernés, groupes et communautés (CAMPAGNA, 2000). Ainsi, avec l'intensification des flux migratoires et la globalisation des échanges, il en va de la multiplication des conditions alternatives de rattachement au for (KLÖTGEN, 2012), voire de cette extraterritorialité (délibérée) de législations nationales ou régionales (LOONAM & REARDON, 2020; CREMONA & SCOTT, 2019), pour justifier l'application du droit national dans des situations présentant des éléments d'extranéité et la compétence des tribunaux étatiques à l'égard de personnes de nationalité étrangère (notamment selon les règles de droit international privé). Alors que la reconnaissance de la double, voire de la pluri-citoyenneté, assujettit les sujets de droit à des obligations concurrentes qui leur sont imposées par plus d'un État, les notions de lois de police et d'ordre public demandent l'application exclusive d'un droit national malgré la présence d'éléments de rattachement à plus d'un État. Les sujets de droit nationaux peuvent encore se prévaloir de juridictions internationales comme l'arbitrage international, institution prévue dans de nombreux traités bilatéraux ou multilatéraux sur l'investissement et les accords commerciaux internationaux. Les traités sur l'investissement et les contrats d'État reconnaissent couramment aux investisseurs privés qui sont des ressortissants et, partant, sujets de droit d'un autre État (contractant), un recours contractuel direct contre un État pour des mesures contrevenant aux règles prohibant la discrimination ou le traitement inéquitable (LAVIEC, 1985; DANIC, 2012; BENYEKHLEF, 2015), tandis que les contrats commerciaux internationaux permettent aux contractants privés de se prévaloir d'une juridiction arbitrale de règlement des conflits dont les décisions pourront être applicables directement par les tribunaux nationaux des États qui ont adhéré aux traités. Au niveau des obligations, les sujets de droit, comme les entreprises privées, se voient de plus en plus imposés une responsabilité (pénale) internationale pour violation du droit international coutumier relatif au travail forcé, à l'esclavage, aux crimes contre l'humanité ainsi qu'aux traitements cruels, inhumains ou dégradants[20]. Pour plusieurs, la reconnaissance des droits de la personne aurait joué un rôle prédominant à cette évolution :

> […] [traduction] « [l]'émergence rapide des droits de la personne a entraîné un changement révolutionnaire en droit international, soit le passage d'une conception de l'ordre mondial axée sur l'État à une axée sur la personne » (Payam Akhavan, « Canada and International Human Rights Law: Is the Romance Over ?, (2016), 22 Canadian Foreign Policy Journal 331, p. 332). Cette évolution a fait en sorte que le droit international vise maintenant [traduction] « non seulement à maintenir la paix entre les États, mais aussi à protéger la vie des personnes ainsi

20 Propositions publiées en France et en Belgique, lire notamment Jean-Baptiste RACINE, « Droit économique et droits de l'homme : introduction générale », dans Laurence BOY, Jean-Baptiste RACINE et Fabrice SIIRIAINEN (dir.), *Droits économiques et droits de l'homme*, Larcier 2009, p. 7, et les autres contributions à cet ouvrage; Nicolas MATHEY, « Les droits de l'homme et libertés fondamentales des personnes morales de droit privé », *RTDciv.* 2008.205; Véronique CHAMPEIL-DESPLATS et Danièle LOCHAK (dir.), *Libertés économiques et droits de l'homme*, Presses universitaires de Paris Ouest, 2011.

que leur liberté, leur santé [et] leur instruction » (Emmanuelle Jouannet, « What is the Use of International Law ? International Law as a 21st Century Guardian of Welfare », (2007), 28 Mich. J. Int'L. 815, p. 821). Le professeur Christopher Joyner a ajouté : [traduction] « Les droits des personnes se trouvant dans un État transcendent maintenant les frontières nationales et sont essentiellement devenus une source de préoccupation commune en droit international » (Christopher C. Joyner, « 'The Responsibility to Protect' : Humanitarian Concern and the Lawfulness of Armed Intervention », (2007), 47 Va J. Int'l L. 693, p. 717)[21].

[20] Dans le contexte de la globalisation, prennent une importance croissante les droits économiques, sociaux et culturels – droits de l'homme de deuxième génération – ainsi que les droits collectifs de troisième génération dont les droits à un environnement sain, à l'assistance humanitaire et au partage dans l'exploitation du patrimoine commun de l'humanité. À la différence des droits – individuels – de première génération, la pénétration de ces droits dits de solidarité a la particularité d'emprunter le chemin inverse, en s'imposant de l'ordre international aux ordres juridiques internes des États[22]. En effet, il est possible de structurer le développement des droits de la personne en quatre temps depuis l'apparition au XVIe siècle de l'État moderne :

> S'ils ont tout d'abord émergé au sein des nouveaux États-nations (Droits de la personne nationalisés), ce cadre national n'a rapidement pas été suffisant. Il a fallu développer des instruments juridiques régionaux et internationaux capables d'assurer le maintien de la paix et de la sécurité internationale et de faire respecter les droits de la personne (Droits de la personne internationalisés et régionalisés). En outre, la « nouvelle » mondialisation à laquelle nous assistons depuis la fin de la Seconde Guerre mondiale est elle-même « créatrice » de droits, ce qui a notamment permis de rendre les droits de la personne plus souples et plus « sanctionnables » et, par-là, le droit international des droits de la personne est venu pénétrer le droit interne et la structure judiciaire nationale (Droits de la personne mondialisés). Enfin, le développement de modèles globaux, comme l'État de droit ou la bonne gouvernance, ont permis récemment une nouvelle pénétration des droits de la personne dans la structure même des États (Droits de la personne globalisés). (BENYEKHLEF, 2015, p. 122)

[21] Une certaine lucidité demeure de mise. Une rhétorique appuyée des droits de la personne s'est faite jour depuis un certain temps déjà, constituant une composante essentielle du discours occidental et, en particulier, des États-Unis et conduisant bien entendu à une pure instrumentalisation de ceux-ci. Les droits de la personne deviennent alors un justificatif masquant, avec plus ou moins de réussite, les visées

21 *Nevsun Resources Ltd.* c. *Araya*, 2020 CSC 5, par. 108

22 Dominique ROUSSEAU, « Les droits de l'homme de la troisième génération », (1987) 19-2 *Revue interdisciplinaire d'études juridiques* 19, DOI : <https://doi.org/10.3917/riej.019.0019>. « Alors que les droits "anciens" se sont inscrits d'abord dans des textes internes avant d'être repris dans des documents internationaux, les droits "nouveaux", apparus depuis une dizaine d'années, ont suivi un cheminement inverse; ou plus exactement, ils sont, pour l'instant, inscrits seulement dans les écrits ressortissant au droit international, sauf lorsque l'ordre constitutionnel de certains pays les reçoit à la suite d'une rédaction nouvelle ou d'une modification récente de leur constitution ».

impériales notamment des États-Unis. Les droits de la personne sont alors déconsidérés, se transformant en simple variable d'ajustement des luttes de puissance.

[22] Cet activisme dans le (re)modelage continu de nouvelles frontières géopolitiques n'émane pas que des États. Certains sujets de droit eux-mêmes peuvent réclamer à l'avenant un espace d'autodétermination, voire de souveraineté, qui s'affirme avec audace par-delà les frontières westphaliennes des souverainetés nationales. Figurent parmi ces revendications autonomistes

- l'émergence de groupes armés transnationaux (p. ex., Al-Qaïda et l'État islamique, le Hezbollah)[23];
- l'anticolonialisme et les enjeux des souverainetés autochtones, lesquels remettent en question l'exclusivité territoriale (BAUDER & MUELLER, 2021; MORIN, 1997) ainsi que la légitimité (ANGHIE, 2004; SIMPSON, 2004) de la souveraineté à la Westphalienne;
- la décentralisation par la technologie (p. ex. des registres distribués) (Bodó, Brekke & Hoepman, 2021).

[23] Certains associent cette tendance à une émancipation progressive d'une conception exclusivement occidentale de la souveraineté :

> […] if Western statehood is inherently linked to the notion of a clearly delineated contiguous territory … non-Western statehood more often opens the possibility of fluid transnational space as a base of political authority, not merely social movement. The action of emancipated actors – whether armed or not and whether organised as groups or not – has historically pointed out the acuity of this parameter, as such actors sought to establish political dominion across such spaces. (OULD MOHAMEDOU, 2020, p. 1343)

[24] Dans la foulée de Michel Foucault, on peut ainsi affirmer que « l'axe traditionnel de la souveraineté, et donc du pouvoir politique, à savoir le territoire (à conquérir ou à défendre) s'est [re]déplacé pour porter son attention sur la population, sa régulation et son contrôle » (FOUCAULT, 2004, p. 66–67; aussi BENYEKHLEF, 2015). Par conséquent, l'exercice de la souveraineté doit s'inscrire dans un pluralisme juridique conçu comme « différents espaces juridiques superposés, combinés et mélangés » (BENYEKHLEF, 2015, p. 45 citant DE SOUSA SANTOS, 1988, p. 382). Ce climat pluraliste est propice à un réexamen de nos catégories et vecteurs normatifs

23 Zakaria DABONÉ, « Les groupes armés dans un système de droit international centré sur l'État », (2011) 93-2 *Revue internationale de la Croix-Rouge* 85, 87 : « Les groupes armés sont constitués d'individus sur lesquels l'État où ils se trouvent souhaite garder un contrôle particulier grâce à son droit interne. À ce titre, les groupes armés ne bénéficient pas du même statut que les forces gouvernementales. En droit interne ou dans le langage des autorités publiques, leurs membres ne sont que des individus insoumis à la loi, des 'bandits' de droit commun, des terroristes, des 'apatrides', punissables du seul fait d'avoir pris les armes. En droit international, aucun instrument ne place les insurgés sur le même pied que les membres des forces armées gouvernementales. Les groupes armés héritent alors en droit international, lorsque celui-ci s'applique, d'un statut peu privilégié. ». Sur cette question, voir aussi : Alix LE MOIGN, « Les groupes armés non étatiques et l'internationalisation de leurs soutiens », (2018) 30-1 *Les Champs de Mars* 201, DOI : <https://doi.org/10.3917/lcdm.030.0201>; Mohammad-Mahmoud OULD MOHAMEDOU, « D'Al Qaïda à l'État islamique : acteurs non-étatiques mondialisés et évolution de la violence politique post-moderne », (2017) 172-4 *Relations internationales* 3, DOI : <https://doi.org/10.3917/ri.172.0003>.

traditionnels et prend toute son actualité avec l'avènement du cyberespace et du métavers.

B. TRACÉ DES (NOUVELLES) FRONTIÈRES DANS LE CYBERESPACE

[25] Si cette fluidité croissante des frontières westphaliennes est un phénomène qui transcende le cyberespace, ce dernier y participe par sa vocation transfrontière et soulève, à première vue, des enjeux communs à d'autres espaces collectifs, comme l'espace maritime[24], aérien[25] ou extra-atmosphérique[26]. À la différence toutefois de ces autres espaces géographiques partagés qui préexistent aux États, le cyberespace est une création humaine. Le cyberespace est, par ailleurs, rapidement devenu un enjeu de compétition industrielle, normative et géopolitique pour les États.

[26] À cet égard, Frédérick Douzet présente le cyberespace comme une architecture structurée en couches superposées. Par ordre décroissant de géolocalisation physique, quatre couches en particulier attirent notre attention : la première est l'infrastructure physique de l'Internet et renvoie à l'ensemble d'équipements matériels qui, de câbles sous-marins et terrestres aux objets connectés en passant par les serveurs, postes de travail et centres de données, constituent l' « épine dorsale de l'Internet » (DOUZET, 2014, par. 9). La deuxième couche, dite logique, est celle qui assure la liaison entre deux éléments de l'infrastructure physique de l'Internet. Elle « comprend tous les services [p.ex. le routage et l'adressage] qui permettent d'assurer la transmission des données entre deux points du réseau et, donc, de faire voyager l'information, découpée en petits paquets de données, de son expéditeur à son destinataire » (DOUZET, 2014, par. 10). À la troisième couche, logicielle, appartiennent les programmes informatiques et logiciels facilitant l'expérience Web des usagers, depuis les courriers électroniques aux réseaux sociaux, moteurs de recherche et jeux de rôle en ligne massivement multijoueur (MMORPG). La dernière couche, enfin, est constituée de flux de données, d'informations et d'empreintes digitales que génèrent ou laissent les utilisateurs du Web.

---

24 La *Convention des Nations Unies sur le droit de la mer* (1982), dite de Montego Bay, précise les limites de la souveraineté des États côtiers et archipels (art. 2) sur la mer territoriale (art. 3 et 4), leur droit de contrôle dans la zone contiguë à leur mer territoriale (art. 33), le régime juridique particulier applicable à la zone économique exclusive (art. 55 et suiv.) et au plateau continental (art. 76 et suiv.). La haute mer (art. 86 et suiv.) est ouverte à tous les États en ce qu' « [a]ucun État ne peut légitimement prétendre soumettre une partie quelconque de la haute mer à sa souveraineté » (art. 89). Aussi les fonds marins situés au-delà du plateau continental que constituent la « Zone » et ses ressources sont reconnus comme « le patrimoine commun de l'humanité » (art. 136). Pour une critique du droit international de la mer et de ses limites face aux ambitions expansionnistes de certains États côtiers, Lire Alexandra BELLAYER-ROILLE, « Entre souveraineté et transnationalité, les défis du droit de la mer », (2014) 95-3 *Revue internationale et stratégique* 111, DOI : <https://doi.org/10.3917/ris.095.0111>.

25 La *Convention relative à l'aviation civile internationale* signée à Chicago, le 7 décembre 1944, reconnaît nommément à chacun de ses États contractants « la souveraineté complète et exclusive sur l'espace aérien au-dessus de son territoire » (art. 1) ainsi que les eaux territoriales y adjacentes (art. 2). Le respect de cette souveraineté aérienne emporte notamment l'interdiction pour des aéronefs d'État de survoler le territoire d'un autre État ou d'y atterrir sans autorisation (art. 3) ainsi que celle d'exploiter des services aériens internationaux réguliers au-dessus ou à l'intérieur du territoire d'un État contractant sans permission (art. 6). Les aéronefs d'État comprennent ceux utilisés « dans des services militaires, de douane ou de police » (art. 3(b)) à l'exclusion des aéronefs civils. À l'égard de ces derniers, le protocole additionnel du 10 mai 1984 interdit aux États contractants de recourir à l'emploi des armes et leur enjoint d'assurer la vie des personnes se trouvant à bord en cas d'interception (art. 3bis).

26 Le *Traité sur les principes régissant les activités des États en matière d'exploration et d'utilisation de l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes* (Traité de l'espace), conclu le 27 janvier 1967 consacre un espace extra-atmosphérique (comprenant la Lune ainsi que les autres corps célestes) qui se doit d'être sans frontière ni souveraineté. En tant que « l'apanage de l'humanité tout entière », son exploration et utilisation « doivent se faire pour le bien et dans l'intérêt de tous les pays, quel que soit le stade de leur développement économique ou scientifique » (art. 1). Il ne peut pas non plus « faire l'objet d'appropriation nationale par proclamation de souveraineté, ni par voie d'utilisation ou d'occupation, ni par aucun autre moyen » (art. 2). Les États parties au Traité s'engagent cependant à ne pas militariser l'espace extra-atmosphérique dont l'utilisation doit demeurer « exclusivement à des fins pacifiques » (art. 4). Le Traité reconnaît par ailleurs une responsabilité internationale des États parties à l'égard de leurs activités nationales dans l'espace extra-atmosphérique (art. 6), y compris les dommages causés par les satellites (art. 7).

[27] Imperceptiblement mais irrésistiblement, des frontières géopolitiques dans le cyberespace se tissent au travers notamment :

- d'un accès sélectif à l'information à travers le filtrage automatisé des champs informationnels par les algorithmes;
- du profilage et de la catégorisation des utilisateurs en fonction des données personnelles générées en ligne et hors ligne;
- de l'amplification des effets bulles et chambres d'écho polarisant les opinions, avec le risque de renforcer certains enfermements sectaires; et
- de la fragmentation – à la fois technologique et normative – du cyberespace (POHLE & VOELSEN, 2022).

[28] À la différence d'autres espaces géopolitiques, le cyberespace se singularise à la fois par son caractère multicouche – de l'architecture matérielle et logicielle à l'émergence des cultures numériques –, le foisonnement de ses points de rencontre ou de confluence obligés avec les espaces géopolitiques traditionnels (centres de données, serveurs, Internet des objets, technologies prêt-à-porter) ainsi que la participation active des utilisateurs qui appartiennent à différents groupes culturels, nationaux, régionaux ou encore socio-économiques. Ce système imbriqué complique la question du contrôle et de la régulation du cyberespace.

[29] Il n'est pas jusqu'aux *frontières* des droits subjectifs qui se trouveraient érodées avec l'avènement du cyberespace. Le noyau de notre vie privée est plus que jamais éclaté avec la dissémination des « traces » et « faisceaux d'indices » à caractère personnel sur et à travers le Web, alors que bien des traces technologiques sont collectées à notre insu.

[30] Ainsi, la question du tracé des frontières dans le cyberespace se pose au regard des trois attributs de la norme du point de vue sociologique, tels que définis par Guy Rocher[27] :

- l'identification des règles applicables;
- les personnes à qui sont reconnus le pouvoir et l'autorité nécessaires pour édicter ces normes, les appliquer et les interpréter et ;
- les personnes assujetties qui reconnaissent, explicitement ou implicitement, à ces normes et règles un caractère de légitimité et de contrainte.

[31] En effet, au pouvoir normatif explicitement reconnu de l'appareil étatique s'adjoint désormais un pouvoir normatif implicite des technologies à réguler / policer les comportements des sujets de droit ainsi qu'à conforter ou à remettre en question la légitimité, voire la suffisance, des règles étatiques applicables à ces mêmes

27 Guy ROCHER, *Traité de sociologie du droit et des ordres juridiques*, Montréal, Thémis, 2022, p. 18. Lire aussi Santi ROMANO, *L'ordre juridique*, Dalloz, 2002.

technologies. Avec la construction du cyberespace, ce sont les trois attributs de la norme qui se trouvent en quelque sorte déterritorialisés, à savoir tant au niveau des règles applicables que les personnes qui se voient (implicitement) reconnaître le pouvoir et l'autorité nécessaires pour les édicter, les appliquer et les interpréter ainsi que les personnes qui y sont assujetties.

[32] Cette « déterritorialisation » ne renvoie pas nécessairement à une décentralisation, mais annonce plutôt une autre « centralisation » autour des acteurs et des ressources qui ne font pas expressément partie de l'appareil étatique. Cette autre centralisation s'opère par (SCHNEIDER, 2019; GOLDSMITH & WU, 2006) :

- le contrôle du système de noms de domaines (DNS) par l'ICANN (Internet Corporation for Assigned Names and Numbers);
- le rôle névralgique de quelques grandes plateformes comme « contrôleurs d'accès » de facto au cyberespace;
- la gestion du trafic Internet par quelques grandes entreprises de télécommunication;
- la centralisation des fermes de minage de cryptomonnaie.

[33] Sur ce plan, la souveraineté des États s'affirme dans ces différents points de contrôle névralgiques que sont d'abord les infrastructures physiques qui constituent cette première couche fondamentale du cyberespace. Ce contrôle s'exerce en outre sur les acteurs principaux que sont – du côté de l'offre –, les fournisseurs d'accès et de télécommunications, les plateformes numériques, les registraires, mais aussi – du côté de la demande – les usagers-consommateurs dont les intérêts ainsi que le poids économique ne pèsent pas moins dans la dynamique du marché. Cette souveraineté se renforce en particulier chez les États puissants qui le sont notamment en raison de l'abondance ou de la concentration de ces ressources sur les territoires qui peuvent relever, à différents niveaux, de leur juridiction.

[34] De façon moins explicite, les États contribueraient aussi volontiers à cette concentration par leur inaction ou des choix – normatifs – de non-intervention (laisser-faire, laissez-passer) favorables à l'innovation technologique ou propices à la formation de monopoles / oligopoles numériques.

[35] La « déterritorialisation » n'est pas non plus synonyme de « délocalisation » ou de « dématérialisation ». L'expression invite plutôt à relativiser la pertinence du territoire national comme fondement du pouvoir normatif. Les États westphaliens ne sont pas inconscients de cette érosion de leur pouvoir souverain, ni ne sont totalement impuissants à y remédier.

[36] Que ce soit l'idéal d'un village planétaire (MCLUHAN & FIORE, 1968) interconnecté, une culture d'innovation donnant lieu à l'essor du Web participatif[28][1], la décentralisation institutionnelle annoncée par les registres distribués ou la fascination récente que suscite le métavers, l'idéal d'émancipation qu'inspire le Web[29][2] d'hier comme d'aujourd'hui est suivi immanquablement d'une reprise en main par les États. À l'ère de la quatrième révolution industrielle, cette reconquête du cyberespace passe en partie par la maîtrise de l'IA, en tant que ressource stratégique dans l'équilibre des puissances.

II- L'INTELLIGENCE ARTIFICIELLE (IA) : UNE (NOUVELLE) RESSOURCE STRATÉGIQUE DANS L'ÉQUILIBRE DES PUISSANCES

[35] Lentement mais sûrement, l'Internet a permis le développement de l'IA par la consolidation d'une infrastructure matérielle et logicielle permettant la cueillette, le croisement et le traitement exponentiels d'une formidable quantité de données (*big data*). Les technologies associées à l'IA emportent des retombées d'ordre transversal, assimilables sans doute aux grandes découvertes historiques qui ont déterminé le cours de nos civilisations (GUTHLEBEN, 2021). Paraphrasant le savant juriste Rudolf von Jhering (1818-1892), si la force des armes et la force intellectuelle (l'Église et le Droit) ont jusqu'alors servi de trait d'union entre les peuples et dicté le cours des mondes[30], la maîtrise technologique est devenue de nos jours un avantage compétitif *transversal* qui semble déterminer plus que jamais les rapports de puissance entre les États (MIAILHE, 2018).

[37] Si l'analyse géopolitique traite des conflits de représentations, notamment idéologiques, l'importance stratégique de l'IA semble devenir un type d'idéologie partagé par les États, quels que soient leurs parcours et leurs différences culturels ou politiques.

A. LA COURSE À L'HÉGÉMONIE DE L'IA

[38] En géopolitique, une situation d'hégémonie désigne une configuration asymétrique de l'ordre international où un État surpasse les autres en termes de puissance et réussit à imposer ou à faire accepter ses choix au niveau international (VANEL, 2003). Cette puissance doit emporter à la fois l'autorité (pouvoir de contrainte) et la légitimité (acceptation ou reconnaissance de l'autorité par les États qui y sont soumis) (BOUQUET, 2014). Dans cette perspective, l'hégémonie de l'IA passe par une alliance stratégique que les États cherchent à tisser avec les réseaux numériques et les

---

28 *Cf.* Christophe AGUITON et Dominique CARDON, « Web participatif et innovation collective », (2008) 50-1 *Hermès* 75, DOI : <https://doi.org/10.4267/2042/24155> : « En effet, les transformations les plus spectaculaires et les ruptures les plus significatives dans les comportements de communication, le logiciel libre, le Wifi, le P2P, les blogs et beaucoup de services Internet regroupés derrière l'étiquette 'Web 2' n'ont pas été initiés 'par le haut', grâce à un plan de développement industriel accompagnant la mise à disposition d'une technologie nouvelle issue des laboratoires de recherche, mais ont pris forme au sein d'un milieu hétérogène associant très étroitement usagers, technologues, innovateurs et militants. »

29 Et pas que le Web. Du *globish* à l'Internationale, de l'hypothèse Gaïa à la gouvernance mondiale, l'utopie d'un monde sans frontières participerait de cette « idée bête [qui] enchante l'Occident : l'humanité, qui va mal, ira mieux sans frontières. » (Régis DEBRAY, *Éloge des frontières*, Gallimard, 2013).

30 *Cf.* Rudolf VON JHERING, *L'esprit du droit romain dans les diverses phases de son développement* (traduit par O. DE MEULENAERE), t. 1, 2e éd., Marescq, Paris, 1880, p. 1 et 2 : « Trois fois Rome a dicté des lois au monde, trois fois elle a servi de trait d'union entre les peuples : par l'unité de l'*État*, d'abord, lorsque le peuple romain était encore dans la plénitude de sa puissance; par l'unité de l'*Église*, ensuite, après la chute de l'empire romain, et la troisième fois enfin, par l'unité du *Droit*, à la suite de la réception du droit romain au moyen-âge. La contrainte extérieure et la force des armes amenèrent une première fois ce résultat; ce fut la force intellectuelle qui prévalut aux deux autres époques ». Sur le droit comme force politique dans la construction de l'Église et de l'État moderne, lire Karim BENYEKHLEF, *Une possible histoire de la norme. Les normativités émergentes de la mondialisation* (2e éd.), Montréal, Éditions Thémis, 2015, p. 416 et suiv.

grandes plateformes qui sont devenus, en quelque sorte, les « mercenaires » du Web et d'un monde multipolaire.

1. DES ORIGINES MILITAIRES DE L'INTERNET ET DU CYBERESPACE

[39] Aujourd'hui, l'inclination marchande de la Silicon Valley peut occulter, aux yeux des non-initiés, ses origines industrielles et militaires. Si la guerre a toujours été un puissant moteur des innovations et des progrès technologiques des sociétés humaines, l'histoire de l'Internet ne fait pas exception, ni n'est étrangère aux impératifs, ou du moins, aux incitatifs militaires[31]. « Les deux guerres mondiales du XXe siècle ont scellé l'union ancienne entre la science et la guerre » (LAPERCHE, 2005, par. 3; aussi LESLIE, 2000; RASMUSSEN, 2015). Le Rideau de fer s'est construit le long d'une ligne frontière militarisée entre les deux Blocs dans l'immédiat après-guerre. Le lancement du premier satellite artificiel (Spoutnik) en 1957 par l'URSS illustre le recours à la science comme instrument de puissance. En effet, ce lancement fut pour les États-Unis un « *technological Pearl Harbor* » (BUCKLEY, 1971)[32]. Le gouvernement américain n'a pas hésité alors à se ménager la collaboration active de l'industrie technologique et de la recherche universitaire dans des projets d'innovation d'envergure requérant « des investissements considérables et un temps d'amortissement relativement long » (ÜLGEN, 2007, par. 67).

[40] Quatre mois plus tard, la création de la *Defense Advanced Research Projects Agency* (DARPA) au sein du Département de la Défense américaine inaugure une nouvelle ère dans la recherche et le développement des nouvelles technologies destinées à un usage militaire. L'une des initiatives les plus fructueuses de la prochaine décennie aura été l'ARPANET (*Advanced Research Projects Agency Network*), le premier réseau à transfert de paquets de données permettant de raccorder à distance différents terminaux (ordinateurs ou calculateurs). S'inspirant notamment des travaux de Paul Baran (1926-2011) sur les communications distribuées et ceux de Donald Davies (1924-2000) sur la commutation des paquets (BARAN, 1962)[33], ce réseau aurait été conçu pour offrir une meilleure résistance aux attaques ennemies[34][2] ainsi qu'aux défaillances systémiques en fragmentant les communications en « paquets » ou « blocs de données » qui seront réassemblées à l'adresse de destination et en les transmettant de façon distribuée par les différents nœuds du réseau, de sorte que la destruction ou la défaillance de l'un n'a pas d'impact sur le fonctionnement des autres composantes du système.

[41] Parallèlement à l'ARPANET, l'Internet, tel que nous le connaissons aujourd'hui, a été « médié » par l'émergence des réseaux universitaires (p. ex. BITNET, Usenet), soutenus dès 1983, par la *National Science Foundation* (NSF). Ces réseaux, mis à la

31 Sur cette question, lire parmi une abondante littérature : Charles THIBOUT, « Les GAFAM et l'État : réflexion sur la place des grandes entreprises technologiques dans le champ du pouvoir », (2022) 125 *Revue internationale et stratégique* 75.

32 Lire aussi sur le choc du lancement du Spoutnik : Deborah D. STINE, « U.S. Civilian Space Policy Priorities : Reflections 50 Years After Sputnik », dans William N. CALLMERS (dir.), *Space Policy and Exploration*, New York, Nova Science Publishers, 2008, p. 1.

33 Sur les origines et contributeurs de l'ARPANET, lire Cade METZ, « Paul Baran, the Link Between Nuclear War and the Internet », *WIRED* (4 septembre 2012), en ligne : <https://www.wired.co.uk/article/h-bomb-and-the-internet>.

34 Ou plutôt pour « *empêcher* l'éclatement d'une guerre nucléaire, en permettant de maintenir les canaux de communication ouverts en cas de crise diplomatique » (entretien personnel de Paul BARAN avec Paul E. CERUZZI le 24 avril 2001, rapporté dans Paul E. CERUZZI, « Aux origines américaines de l'Internet : projets militaires, intérêts commerciaux, désirs de communauté », (2012) 18-1 *Le Temps des médias* 15, par. 3, DOI : <https://doi.org/10.3917/tdm.018.0015)>.

disposition des chercheurs et étudiants, ont précédé le déploiement commercial et populaire de l'Internet connecté à partir de réseaux locaux d'ordinateurs personnels et de stations de travail.

[42] Ainsi, la légende de la Silicon Valley est née de cette heureuse alliance entre le gouvernement américain, le monde de la recherche et de l'industrie, « plus que d'initiatives isolées d'entrepreneurs géniaux » (LAURIER, 2018; aussi BENOÎT, 2019). L'État américain s'est, dès le début, impliqué activement dans le maintien d'un environnement réglementaire favorable, voire incitatif, à l'innovation. Les chercheurs distinguent ainsi une intervention selon trois niveaux :

> Tout d'abord, [le gouvernement américain] élabore et applique un ensemble de lois et de règlements bureaucratiques concernant la politique fiscale, le capital boursier et le passif des entreprises, les rapports salariaux, les brevets et les divers droits de propriété (matérielle, commerciale, intellectuelle, etc.) ainsi que la politique de concurrence. À la demande d'acteurs particulièrement influents dans une industrie, l'État interviendra éventuellement afin de favoriser ou de sauver certaines entreprises. Ensuite, l'État peut acheter en vastes quantités (et, partant, favoriser) certains produits ou financer la recherche et le développement de certains procédés et marchandises, et, par conséquent, de certaines entreprises – aux États-Unis, le ministère de la Défense a toujours joué un rôle crucial à cet égard puisqu'une grande partie des innovations technologiques récentes, à commencer par l'Internet, sont d'origine militaire. Troisièmement, tous les niveaux du gouvernement étatsunien financent la recherche universitaire et encouragent la mise sur le marché de produits jugés socialement utiles. (FLIGSTEIN, 2001)

[43] Aussi, le phénomène des GAFAM s'inscrit « dans cette histoire du développement technologique sous *ordination* étatique » (THIBOUT, 2022, p. 77, italique dans l'original). En usant somme toute de stratégies classiques du contrôle de la concurrence, telles que le rachat des *startups* et le verrouillage technologique des produits, quelques entreprises dominantes se consolident peu à peu en une position oligopolistique dans le secteur de l'informatique (FLIGSTEIN, 2001).

[44] Quoiqu'au cours de la dernière décennie du XX^{e} siècle, l'Internet ait été présenté « comme un moyen de réaliser une utopie démocratique mondiale et le moyen de faire advenir la société de la connaissance » (ISAAC, 2022, p. 5)[35], il ne faut pas perdre de vue qu'Internet est, à toutes fins pratiques comme de droit, un réseau principalement contrôlé par les États-Unis (POHLE & VOELSEN, 2022). Cette maîtrise découle d'une nécessité pratique de faire contrôler par une seule entité l'assignation et l'enregistrement des adresses Internet afin d'éviter les dédoublements et la possible confusion des marques et des sites Web (CERUZZI, 2012). Depuis 1998, ce rôle a été assigné à l'ICANN (*Internet Corporation for Assigned Names and Numbers*) qui, avant 2016, était une organisation sans but lucratif de droit privé « sous protectorat américain » (SOUPIZET, 2021, par. 43). Or, l'Internet, en facilitant la circulation et le

35 Lire également la *Déclaration d'indépendance du cyberespace* (1996) de John Perry Barlow, qui s'indigne, dans un lyrisme aujourd'hui suranné, de l'exercice de tout droit de souveraineté sur le cyberespace, conçu comme la « nouvelle demeure de l'esprit ».

croisement des données massives, est la matrice de l'IA et de ses formidables réalisations induites notamment par les techniques de l'apprentissage profond (*deep learning*).

2. LA VALEUR AJOUTÉE DE L'IA ET LE TECHNO-NATIONALISME

[45] Pour les États, la valeur ajoutée de l'IA réside non seulement dans le renforcement des capacités de défense nationale (U.S. GOVERNMENT ACCOUNTABILITY OFFICE, 2022) ou des projets de cybersécurité (nationale), mais couvre un terrain transversal beaucoup plus vaste de services essentiels allant de l'industrie pharmaceutique et de la santé aux chaînes d'approvisionnement.

[46] D'où l'engouement des États pour le « techno-nationalisme », l'expression renvoyant « à une stratégie de développement technologique basée sur d'étroits partenariats public-privé, par laquelle l'État n'est pas seulement un investisseur majeur dans les domaines de la recherche et du développement (R&D), mais joue également un rôle actif en tant qu'entité de planification » (GONZÁLEZ, 2021). L'expression est de Robert B. Reich, qui l'employait dans un article de 1987 pour l'opposer au techno-mondialisme (REICH, 1987), à une époque où, brandissant le spectre d'une menace économique par le Japon, les États-Unis surveillaient du coin de l'œil les progrès de l'économie japonaise dans les microcircuits, les semi-conducteurs et l'électronique grand public. Les tenants du techno-nationalisme considèrent que le développement technologique est un projet national qui se doit d'être autosuffisant et s'émanciper de toute dépendance – qu'elle soit technologique, financière, matérielle ou expertale – envers d'autres États. Par ailleurs, le techno-mondialisme perçoit l'innovation technologique comme un patrimoine commun de l'humanité qui doit être exploitée au bénéfice de tous.

[47] Dans le monde multipolaire contemporain, le techno-nationalisme, en traçant un trait d'union entre « innovation nationale et succès politique [national] » (DE CATHEU, 2021), serait un autre impérialisme (SAUL, 2022) en ce qu'il offre une nouvelle matrice idéologique qui renforce les frontières géopolitiques entre certains États. Ainsi, pour faire contrepoids à l'emprise historique des États-Unis sur les géants du numérique, l'Union européenne cherche à se démarquer par ses ambitions normatives[36] alors que la souveraineté technologique de la Chine s'affirme notamment par l'émergence des géants asiatiques (BATX : Baidu, Alibaba, Tencent et Xiaomi) et le programme « Made in China 2025 »[37]. Les tigres (Thaïlande, Malaisie, Indonésie, Vietnam et Philippines) et dragons (Corée du Sud, Taïwan, Hong Kong et Singapour) asiatiques ne sont pas en reste : les capitales comme Singapour, Séoul et Bangkok « sont devenues les nouveaux *hubs* mondiaux du business à partir desquels une jeune génération d'entrepreneurs asiatiques avides de changer la donne émerge » (JOHNSON, 2018). Il en va pareillement des homologues russes (YVOT : Yandex, YKontakte, Ozon et Telegram), des géants américains (GAFAM) et chinois (BATX).

36 *Supra* note 6.

37 Commenté par « Une course à l'hégémonie technologique entre la Chine et les États-Unis », *Courrier international* (28 septembre 2018, en ligne : <https://www.courrierinternational.com/article/une-course-lhegemonie-technologique-entre-la-chine-et-les-etats-unis>.

3. GAFAM, BATX ET YVOT : LES MERCENAIRES DU CYBERESPACE ET DU MONDE MULTIPOLAIRE

[48] Le monde post-westphalien se caractérise non seulement par une fluidité croissante des frontières géopolitiques, d'une part, mais aussi, d'autre part, par une diversification des acteurs non institutionnels – multinationales, géants ou contrôleurs numériques, organisations non gouvernementales, société civile[38] – qui sont appelés à jouer un rôle marqué sur la scène internationale.

[49] Qu'il s'agisse de la maîtrise des technologies, de la numérisation de l'économie ou de la capacité de réguler *in facto* tous les pans de la vie sociale, les géants du numérique – pourtant *a priori* des acteurs privés – en viennent à jouer un rôle névralgique ainsi qu'à accaparer une place monopolistique d'ordre planétaire. Certains n'hésitent pas à qualifier cette cession de puissance à des agents économiques privés de « révolution copernicienne de la géopolitique », où « se substituerait à l'orthodoxie statocentrique un système "gafamo-centré", dans lequel les États seraient relégués au rang de constellations orbitales, simple décor d'une scène dont les grandes entreprises des technologies de l'information américaines seraient les acteurs principaux » (THIBOUT, 2022, p. 76; aussi BOULLIER, 2022).

[50] Alors que certains auteurs s'insurgent contre l'invasion des « barbares numériques » (SAULNIER, 2022), il serait plus juste (ou judicieux) de considérer les quelques géants du numérique comme des mercenaires (qui peuvent être) à la solde de gouvernements. Moins pirates que corsaires, leur expertise technologique peut être mobilisée tant pour policer le cyberespace que pour construire un métavers à l'image de nos civilisations.

[51] Au cours des deux premières décennies du XXIe siècle, l'industrie des services de l'information s'est ramifiée en plusieurs branches, allant de la collecte et du traitement des données de masse à la production en masse de dispositifs connectés, en passant par des capacités accrues d'identification, de traçage, de géolocalisation et de renseignement. Un nouvel écosystème biface voit le jour, que raffine le jeu des algorithmes et de l'IA :

> En première instance, le service d'information, en apparence gratuit pour l'utilisateur, a pour contrepartie les données de sa recherche que la plate-forme recueille et peut commercialiser, par exemple pour de la publicité ciblée. En seconde instance, la transaction est rémunérée par un prélèvement sur la vente. En outre, la plate-forme mémorise les données des clients comme celles des producteurs, car elles aident à fidéliser les premiers et à régner sans partage sur les seconds. Dans cette logique économique où les données sont devenues un facteur de production, on ne raisonne plus en termes de produits, ni même de marchés, mais d'écosystèmes autour de la centralité détenue par les plates-formes. (SOUPIZET, 2021, par. 10)

38 Sur le rôle des acteurs non étatiques dans les relations nationales, lire notamment Karim BENYEKHLEF, *Une possible histoire de la norme. Les normativités émergentes de la mondialisation* (2e éd.), Montréal, Thémis, 2015, p.571 et suiv.

[52] Depuis la fin de la guerre froide, alors que l'émergence de risques plus diffus tels que des attentats terroristes et des attaques informatiques met à mal « les dispositifs sécuritaires traditionnels » (THIBOUT, 2022, p. 79), les technologies intelligentes peuvent être mobilisées de manière novatrice au profit de la défense et du renseignement. Ainsi, à l'exception d'Amazon, les géants numériques se sont associés au programme PRISM de la National Security Agence (NSA) entre 2007 et 2012 en permettant un accès direct par l'agence de renseignement à leurs serveurs[39]. Des observateurs relèvent aussi une implication active des géants numériques dans le processus politique, depuis les dépenses de lobbying au financement des campagnes électorales, sans oublier la pénétration des employés des GAFAM dans divers ministères, institutions et départements étatiques (THIBOUT, 2022; BENOÎT, 2019). Ce va-et-vient régulier des effectifs du secteur public à l'industrie, voilà le phénomène bien connu – et depuis longtemps – de porte tournante ou « *revolving door* » (YATES & CARDIN-TRUDEAU, 2021; I VIDAL, DRACA & FONS-ROSEN, 2012; MORAN & LITWAK, 2021; ALFONSI, 2020)[40].

[53] On note également que depuis les années 2010, le passage « de l'Internet de l'information à l'Internet de la valeur » (GODBOUT, 2023; TAPSCOTT & TAPSCOTT, 2017), marqué par le Web transactionnel et l'émergence des cryptoactifs sur des registres distribués, remet en cause ce rôle « fiduciaire » jusqu'alors occupé par des institutions financières centrales comme intermédiaires de confiance (WERBACH, 2023). Les géants numériques, tout comme les États, n'ont pas tardé à émettre leurs propres cryptomonnaies (p. ex. le Diem de Facebook).

[54] Si, comme les géants pétroliers ou les magnats des chemins de fer de jadis, la capitalisation cumulée des GAFAM dépasse désormais le produit intérieur brut (PIB) de plusieurs pays, dont le Japon, les géants du numérique se distinguent par une diversification transversale sans précédent de leurs activités :

> En effet, qu'elle soit définie par ses infrastructures, par les services qu'elle fournit, par les modèles d'affaires qu'elle supporte ou par les écosystèmes qu'elle structure, la plateforme numérique se mue inévitablement, et assez rapidement vers une situation de domination. (EL YAHYAOUI, 2021, par. 5)

[55] Cette couche technologique transversale que les géants du numérique surimposent à la vie en société n'est pas sans plus-value pour des fonctions traditionnellement régaliennes telles que la défense et la sécurité, le service de renseignement, l'exploration spatiale jusqu'à la souveraineté monétaire avec l'émission possible de monnaies numériques de banque centrale (MNBC). Alors que s'estompent les frontières entre les domaines jusqu'alors réservés à l'initiative privée et ce qui relève de la puissance publique, les géants du numérique rivalisent avec les institutions étatiques sur plusieurs fronts et sont instigateurs de transformations radicales que

39 Selon les révélations d'Edward Snowden en 2013 : Edward SNOWDEN, *Permanent Record,* Macmillan, 2020. Voir aussi Samuel CHAPMAN, « Edward Snowden & the NSA PRISM Program : What you Need to Know in 2023 », *PrivacyJournal.net* (17 mai 2023), en ligne : <https://www.privacyjournal.net/edward-snowden-nsa-prism/>.

40 Certains auteurs ont cependant relevé l'influence déclinante de ces lobbyistes aux États-Unis : James M. STRICKLAND, « The Declining Value of Revolving-Door Lobbyists: Evidence from the American States », (2020) 64-1 *American Journal of Political Science* 67.

certains assimilent à « une manière de révolution copernicienne de la géopolitique » (THIBOUT, 2022, p. 76).

[56] Sur le plan économique, les récentes tentatives normatives des différentes juridictions pour contenir l'expansion des GAFAM tant par la réglementation des pratiques anticoncurrentielles[41] que par les réformes adoptées dans la fiscalité internationale[42] témoignent en fait de l'emprise sans précédent des GAFAM sur les marchés et le dynamisme du réseau de valeur entretenu par ces derniers. Ce réseau de valeur se fonde sur une infrastructure technologique de pointe ainsi que sur une présence économique mondialisée sans commune mesure avec la localisation physique des entreprises. L'économiste Cédric Durand n'hésite pas à évoquer ici l'« hypothèse techno-féodale » selon laquelle la domination numérique se consolide au gré des mécanismes de « rente d'innovation dynamique » associée aux actifs intangibles que sont les bases de données, la propriété intellectuelle, les brevets et les algorithmes. Pour Durand, ce mécanisme rentier s'apparente au féodalisme en ce qu'il repose sur des dispositifs non productifs de captation de valeur que caractérise une économie qualifiée de prédation[43].

[57] Au niveau politique, l'actualité des dernières années illustre la capacité des grandes plateformes de communication et des médias sociaux d'orienter certains événements à résonance durable comme le Printemps arabe (2011) (TUFEKCI, 2017), le Brexit (2020) ainsi que les interférences ou les manipulations électorales. Certains craignent que ces risques de désinformation ne puissent être exacerbés avec l'avènement des modèles génératifs de langage (p. ex. chat GPT-4) et d'images (p. ex. DALL-E) (GOLDSTEIN et al., 2023; SANDERS & SCHNEIER, 2023).

[58] Ce dernier constat mérite toutefois d'être nuancé. Une étude longitudinale des flux Twitter d'environ 1 500 répondants américains n'a relevé aucune relation significative entre l'exposition des utilisateurs aux « interférences » russes aux élections présidentielles de 2016 et le changement de comportements électoraux et attitudes politiques (EADY et al., 2023). Il reste à démontrer dans quelle mesure, à l'exclusion

41 Avec notamment l'adoption, au niveau de l'Union européenne, du Règlement sur les marchés numériques (2022), lequel impose un ensemble d'obligations *ex ante* aux grandes plateformes numériques structurantes pour protéger la contestabilité et l'équité du fonctionnement du marché intérieur numérique. Aux États-Unis, une commission d'enquête bipartisane sur l'état de la concurrence des marchés numériques relève également le contrôle d'accès et le rôle d'intermédiaires stratégiques joué par les GAFAM sur les marchés numériques et la nécessité d'une réglementation des pratiques anticoncurrentielles : États-Unis, COMMITTEE ON THE JUDICIARY OF THE HOUSE OF REPRESENTATIVES (Subcommittee on Antitrust, Commercial, and Administrative Law), *Investigation of Competition in Digital Markets*, partie 1, Washington, U.S. Government Publishing Office, July 2022, en ligne : <https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf>. Un projet de loi, intitulé *Ending Platform Monopolies Act*, a été introduit au Congrès le 11 juin 2021 : *H.R. 3825 – Ending Platform Monopolies Act*, 117e Congrès (2021-2022), en ligne : <https://www.congress.gov/bill/117th-congress/house-bill/3825>. Au Canada, le Bureau de la concurrence abonde dans le même sens : BUREAU DE LA CONCURRENCE, *Examen de la* Loi sur la concurrence *du Canada à l'ère numérique*, mémoire, 8 février 2022, en ligne : <https://ised-isde.canada.ca/site/bureau-concurrence-canada/fr/comment-nous-favorisons-concurrence/promotion-concurrence/conseils-interventions-bureau-concurrence-matiere-reglementation/examen-loi-concurrence-canada-lere-numerique>.

42 L'action 1 du projet de lutte contre l'érosion de la base d'imposition et le transfert de bénéfices (BEPS) mené par l'OCDE et le G20 vise à relever les défis fiscaux posés par l'économie numérique.

43 Cédric DURAND, *Technoféodalisme. Critique de l'économie numérique*, La Découverte, Paris, 2020. L'auteur écrit à la p.173 : « L'essor du numérique nourrit une gigantesque économie de rente, non pas parce que l'information serait la nouvelle source de valeur, mais parce que le contrôle de l'information et de la connaissance, c'est-à-dire la monopolisation intellectuelle, est devenu le plus puissant moyen de capter la valeur ». Il ajoute à la p.210 : « La dynamique du capitalisme est animée en son cœur par un impératif d'investissement lié à la concurrence et à la dépendance généralisée au marché. Or l'essor des intangibles bouscule cette logique classique. Les actifs numériques et leurs utilisateurs devenant indissociables, la mobilité des individus et des organisations est entravée. Cet attachement case la dynamique concurrentielle et offre à ceux qui contrôlent les intangibles une capacité sans pareille de s'approprier la valeur sans véritablement s'engager dans la production. Ce qui prend alors le pas, c'est une relation de capture. Dans cette configuration, l'investissement n'est plus orienté vers le développement des forces de production mais des forces de prédation ».

d'autres facteurs, ces interférences auraient par ailleurs provoqué des effets de second ordre comme la remise en question de la légitimité de la présidence Trump et la méfiance à l'égard du système électoral. D'autres remettent également en question le rôle vectoriel qu'auraient pu jouer les réseaux sociaux dans les mobilisations de masse (MOROZOV, 2012; GLADWELL, 2010), même si l'omniprésence des médias sociaux contribue à la participation des citoyens dans les mouvements populaires de notre temps, et ce, dans des proportions bien sûr variables (FARIS, 2012).

[59] Si l'Internet d'aujourd'hui est né d'un soutien indéfectible du Département de la défense américaine (*supra*), les grandes entreprises numériques vont aujourd'hui jusqu'à s'émanciper de la tutelle des États en privatisant certains moyens de faire la guerre. Le conflit russo-ukrainien en cours offre un exemple frappant. Malgré la destruction des infrastructures d'Internet et le brouillage des signaux GPS par l'armée russe, les troupes ukrainiennes ont pu avoir recours au service Internet par satellite (Starlink) qui leur est offert par la société américaine SpaceX pour maintenir une connectivité essentielle en temps de guerre (MCKENNA & BOUTROS, 2022). Plus discrètement, Google, de son côté, a désactivé de son service de cartographie et de géolocalisation (Google Maps) les fonctions de trafic en direct en Ukraine, lesquelles auraient permis aux troupes russes de suivre la progression des forces ukrainiennes[44]. Au-delà des technologies cryptographiques (VILLATOUX, 2018) développées par et sous la supervision des États belligérants pour intercepter et déchiffrer les communications ennemies ou des cyberattaques orchestrées par les gouvernements rivaux, voilà des entreprises privées qui, non seulement, prennent ouvertement position dans un conflit armé, mais ont, par ailleurs, la capacité effective d'y participer et d'infléchir le cours des événements. Selon Abishur Prakash, cette incursion inédite des géants du numérique dans un conflit armé est à surveiller avec attention :

> Technology firms are no longer staying quiet in geopolitics for the sake of revenue, (…). Nor are they blindly following government decisions. They are acting independently, and at times, unexpectedly, to achieve geopolitical objectives – ones that they themselves have set. Going forward, having the support of Google or Meta will mean as much for a country as having the support of the world's superpowers. And, alongside all this, nations relying on technology companies might have to contend with these businesses – and their leadership […]. (PRAKASH, 2022).

[60] Ainsi, contrairement au présupposé hobbesien (FOISNEAU, 2000), les États ne seraient plus investis d'une puissance effective supérieure à celle de n'importe quel individu ou groupe d'individus. Il est remarquable que ces entreprises aient pu littéralement se saisir des technologies numériques, développées avec le soutien de la puissance publique aux États-Unis et en Chine, et ainsi s'assurer d'un monopole *de facto* sur celles-ci. Cette appropriation d'une technologie par des opérateurs privés n'est sans doute pas nouvelle. Ce qui la distingue, en l'espèce, c'est la nature prégnante des technologies numériques, leur pénétration totale de l'activité humaine et les ruptures qu'elles engagent dans le tissu socio-économique, voire anthropologique, nationale. La

44 Brian HEATER, « Google Disables Maps Live Traffic Tools in Ukraine », *Tech Crunch* (28 février 2022), en ligne : <https://techcrunch.com/2022/02/28/google-disables-maps-live-traffic-tools-in-ukraine/> : « Alphabet's move appears to stem from concerns that the information could similarly be exploited by the Russian military to track Ukrainian troop movement. The corporation hasn't offered anything in the way of specifics on the matter, including when the switch was flipped or whether it's taken similar action amid other global conflicts. »

maîtrise du numérique octroie à ses opérateurs une position de surplomb et une expertise technologique dont les États ne commencent qu'à mesurer l'importance et l'influence.

[61] En temps de paix, soulignons de fait le lobbying intensif des géants du numérique pour défendre leurs intérêts auprès des législateurs nationaux (OBSERVATOIRE DES MULTINATIONALES, 2022). Ce lobbying se révèle tant en termes de dépenses budgétaires que par la pénétration des employés des GAFAM au cœur de l'administration publique[45]. Selon certains, l'IA pourrait, à l'avenir, renforcer cette influence ciblée auprès des législateurs avec à la fois sa capacité accrue à générer du texte polyvalent de manière convaincante et similaire à un humain et l'avènement d'une nouvelle forme de lobbying (par les humains) assisté par l'IA (SANDERS & SCHNEIER, 2023).

[62] Beaucoup plus insidieuses seraient sans doute ces micro-directives qui, à grands renforts de données recombinées par l'algorithme, laissent entrevoir un avenir où les prérogatives normatives des États se trouveront déléguées à l'IA. De la même manière que le rôle d'intermédiaire de confiance des institutions financières centrales est en voie d'être remplacé par des registres informatiques décentralisés régis par un protocole crypté, une responsabilité semblable des gouvernements envers leurs populations pourra-t-elle être déléguée (en partie) à l'algorithme ? Nous en avons déjà un avant-goût avec la reconnaissance des « contrôleurs d'accès », expression popularisée par le Règlement européen sur les marchés numériques (2022), mais qui désigne au sens large tous les acteurs reconnus capables de structurer les marchés et d'en dicter les conditions de fonctionnement. L'Internet décentralisé, porté par la maturité des technologies de registres distribués, invite à déplacer le vecteur de confiance et de légitimité de l'humain à la machine. Il s'agit, après tout, d'une tendance amorcée de longue date avec l'intégration des outils algorithmiques dans les administrations (VAZQUEZ ROJAS, 2021; LONGHAIS, 2021) et la transformation numérique des services publics. Alors que la discrétion des décideurs humains, quoique balisée, laisse toujours subsister une crainte d'arbitraire ou d'erreur de jugement, la perspective de l'automation propose de substituer à la faillibilité humaine l'infaillibilité du Code. Une véritable délégation du pouvoir réglementaire à la machine s'opère avec l'ère des micro-directives faisant miroiter un futur où les lois seront, à toutes fins pratiques, édictées, modifiées et rendues caduques par l'IA en temps réel selon les conditions socio-économiques détectées et analysées par l'algorithme (CASEY & NIBLETT, 2016, 2017; ELIOT, 2021; KADIOĞLU KUMTEPE, 2021).

[63] L'expertise technologique des géants du numérique est indispensable pour mettre en œuvre un cyberespace réglementé. Tant par sa transversalité que par son omniprésence dans l'ère numérique et sa mobilisation assidue par les géants du Web, l'importance de l'IA peut ainsi être assimilée à une pièce centrale sur l'échiquier du monde contemporain. D'où l'intérêt des États à apprivoiser cette pièce devenue essentielle dans leur course à l'hégémonie planétaire.

45 Telle que révélée notamment par Edward Snowden : Glenn GREENWALD, *No Place to Hide. Edward Snowden, the NSA and the Surveillance State*, Signal, 2014.

C. LA COURSE À L'HÉGÉMONIE PAR L'IA

[64] La « guerre de l'information » prend une nouvelle tournure au temps du numérique et de l'immatérialité des frontières. En effet, les États entendent s'assurer une domination technologique, composante de leur volonté de puissance ou de sécurité :

> Les capacités scientifiques d'un État (nombre de chercheurs et de brevets déposés, publications, budget des centres de recherche, transfert dans les entreprises industrielles et de services, etc.) sont à l'évidence un facteur de puissance et d'influence. Soit que l'antériorité ait permis une accumulation des savoirs comme c'est le cas dans les puissances établies, soit encore que l'investissement dans l'innovation donne un avantage comparatif (dans tous les domaines), soit enfin que l'accès aux savoirs scientifiques et l'effort de recherche nationale accompagnent le développement des puissances ascendantes. Les savoirs scientifiques et technologiques sont un enjeu central de la compétition entre les États et entre les firmes. (FOUCHER, 2014; aussi AUDIER, 2019)

[65] À cet égard, les États cherchent à se ménager une maîtrise de l'IA par le biais d'une « relocalisation » / « reterritorialisation » de cette ressource stratégique – notamment au moyen de différents instruments normatifs (1) – et d'un protectionnisme justifié par des préoccupations relatives à la sécurité nationale au regard d'une technologie à multiples usages (2).

1. L'AVÈNEMENT D'UN NOUVEAU PROTECTIONNISME TECHNO-NATIONALISTE

[66] Au risque de dupliquer autant de versions nationales du Grand Pare-feu de Chine, deux phénomènes, en particulier, retiennent notre attention : l'exportation contrôlée des technologies stratégiques et les exigences relatives à la protection et à la localisation des données à la base de l'IA.

A) LE CONTRÔLE DES EXPORTATIONS DES TECHNOLOGIES STRATÉGIQUES

[67] Plusieurs regroupements et régimes multilatéraux (Groupe d'Australie[46], Régime de contrôle de la technologie des missiles[47], Groupe des fournisseurs nucléaires[48], Arrangement de Wassenaar[49]), embargos et le Traité sur le commerce des armes (TCA)[50] ont été mis en place pour contrôler les exportations de biens et technologies qui peuvent être utilisés à des fins militaires.

---

46 Le Groupe d'Australie (GA) se présente comme « an informal forum of countries which, through the harmonisation of export controls, seeks to ensure that exports do not contribute to the development of chemical or biological weapons » : The Australia Groupe, en ligne : <https://www.dfat.gov.au/publications/ minisite/theaustraliagroupnet/site/en/index.html>.

47 Le Régime de contrôle de la technologie des missiles (RCTM), créé en 1987 à l'initiative des États-Unis, du Canada, de la France, de l'Allemagne, de l'Italie, du Royaume-Uni et du Japon, réunit aujourd'hui trente-quatre pays cherchant à « empêcher la prolifération des vecteurs non pilotés d'armes de destruction massive et qui s'efforcent de coordonner les efforts de prévention à cet égard par le biais des régimes nationaux de licences d'exportation » : le Régime de contrôle de la technologie des missiles (MTCR), en ligne : <https://mtcr.info/mtcr/?lang=fr>.

48 Le Groupe des fournisseurs nucléaires réunit des pays fournisseurs d'articles nucléaires et qui cherchent à prévenir la prolifération d'armes nucléaires au moyen de deux séries de directives relatives aux exportations d'articles nucléaires et d'articles connexes : Nuclear Suppliers Group (NSG), *À propos du NSG,* en ligne : <https://www.nuclearsuppliersgroup.org/fr/>.

49 Arrangement de Wassenaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage, Wassenaar, signé le 19 décembre 1995 (entré en vigueur le 12 juillet 1996).

50 Assemblée générale des Nations Unies, Nations Unies, *Traité sur le commerce des armes*, New York, adopté le 2 avril 2013 (entré en vigueur le 24 décembre 2014)

[68] L'avènement des technologies à double usage pose un défi supplémentaire à la réglementation du commerce des armes. Ce facteur fragilise le maintien de l'équilibre entre la sécurité nationale et l'incitatif à l'innovation. Le fait que les sociétés privées, développant ces technologies, n'appartiennent pas, comme telles, au secteur de la défense, ni ne sont contrôlées par les gouvernements, rend difficile la surveillance que souhaitent exercer les autorités nationales à l'égard des activités de celles-ci. Nous l'avons mentionné, la maîtrise du numérique par les opérateurs privés constitue un défi pour les États.

> […] the pace at which these advances are occurring and the extent to which many of them are primarily focused on the development of civilian products – such as self-driving cars, medicines and manufacturing tools – make it difficult to identify specific items that could be made subject to export control without affecting levels of competitiveness and innovation in the sectors involved. […] A state has a unique relationship with the defence sector – acting as customer, sponsor and regulator – which allows it to control, influence or oversee the systems that are being developed. The lines of control and influence are more tenuous in the commercial sector and it is here that many of the key developments are taking place. (BROMLEY & BROCKMANN, 2019, p. 538–39).

[69] L'Arrangement de Wassenaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage est un régime multilatéral mis en place en 1996 et qui compte, à ce jour, quarante-deux États participants, dont les États-Unis, le Canada, les pays de l'Union européenne, le Royaume-Uni, l'Argentine, l'Afrique du Sud, l'Inde, l'Australie, la Russie, l'Ukraine et la Turquie, à l'exclusion notable de la Chine et d'Israël. Depuis le 11 septembre 2001, l'Arrangement de Wassenaar vise aussi le commerce d'armes aux acteurs non étatiques. Il a été amendé en 2013 pour inclure les systèmes de surveillance basés sur l'Internet. L'Arrangement a été codifié dans plusieurs législations nationales, y compris un nouveau règlement européen instituant un régime de l'Union de contrôle des exportations[51][1]. Or, ce régime mis en place a-t-il atteint son objectif déclaré qui est de contribuer à la sécurité internationale en faisant la promotion de la transparence des échanges et transferts d'armes conventionnelles et de technologies à usage double ? Certains relèvent d'emblée le contrôle difficile des technologies d'inspection approfondie des paquets de données (IAP) permettant la surveillance électronique et qui sont développées sur la base de produits du marché grand public (BENYEKHLEF, 2012). D'autres constatent qu'avant et après Wassenaar, les échanges internationaux d'armes entre les pays signataires n'ont pas changé ni n'ont fait l'objet de restrictions significatives face aux incitations / intérêts économiques (LEWIS, 2015). Quoi qu'il en soit, depuis le milieu des années 1990, l'Arrangement de Wassenaar s'avère être le régime multilatéral le plus important, complétant, d'une certaine manière, d'autres embargos multilatéraux sur les biens et technologies à double usage (BROMLEY & WEZEMAN, 2019).

---

51 *Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte).* Au Canada, voir la Liste des marchandises et technologies d'exportation contrôlée, DORS/89-202; GOUVERNEMENT DU CANADA, Guide de la Liste des marchandises et technologies d'exportation contrôlée du Canada, version de décembre 2020, en ligne : <https://www.international.gc.ca/trade-commerce/guides/export_control_list-liste_exportation_controlee.aspx?lang=fra>.

[70] De son côté, le *Traité sur le commerce des armes* (TCA), adopté en 2013 par l'Assemblée générale des Nations Unies, se veut un véritable instrument multilatéral contraignant visant à réglementer le commerce international d'armes conventionnelles, comprenant les armes légères et de petit calibre, les chars et véhicules blindés de combat, les systèmes d'artillerie de gros calibre, les missiles et lanceurs de missiles, les avions et hélicoptères de combat ainsi que les navires de guerre (art. 2). Le Traité interdit notamment tout transfert d'armes classiques qui violerait les obligations internationales prises par ses États parties (art. 6) et enjoint à ces derniers, avant d'autoriser une exportation, d'en évaluer les risques, notamment eu égard à la paix et à la sécurité, à la facilitation d'actes de terrorisme ou de criminalité transnationale, ou encore à une violation grave du droit international humanitaire ou du droit international des droits de l'homme (art. 7). À la date de la rédaction des présentes, le TCA a été ratifié par 113 États. Il est malheureux de noter qu'au moment où le TCA est adopté après d'âpres négociations, le contrôle des technologies à double usage doit prendre de nouvelles formes au regard de la pénétration transversale de ces technologies stratégiques dans plusieurs secteurs de l'économie, certaines n'excluant pas le recours à l'IA. Ainsi, le contrôle de l'investissement étranger doit dorénavant faire partie des stratégies utilisées par les États pour contrôler le commerce des armes et des ressources à double usage en raison du caractère de la technologie[52].

B) LA PROTECTION ET LES EXIGENCES DE LOCALISATION DES DONNÉES COMME OBSTACLE NON TARIFAIRE

[71] Les exigences relatives à la localisation des données, avec pour corollaire le rapatriement des infrastructures technologiques sur les territoires nationaux, participent à cette tendance de la fragmentation du cyberespace. Les exigences de localisation peuvent prendre plusieurs formes; elles renvoient aux exigences nationales qui, soit requièrent que des données relatives à des individus soient physiquement stockées et traitées sur le territoire national, soit ne permettent leur transfert hors frontières qu'à certaines conditions[53]. Tant les types de données que les catégories d'individus visés par ces exigences peuvent varier. Une exigence de localisation peut concerner toute donnée à caractère personnel relative à une personne ayant un lien de rattachement quelconque avec l'État, ou encore des types de données jugées sensibles qui ne concernent pas nécessairement un individu, mais plutôt une catégorie restreinte de citoyens (p. ex. les personnes occupant des fonctions stratégiques). Une gradation de restrictions peut également être imposée en fonction de différentes catégories de données (YAYBOKE, RAMOS & SHEPPARD, 2021). Alors que le développement et le déploiement responsables de l'IA reposent sur la disponibilité et l'analyse des données massives, la localisation de ces données est essentielle pour assurer à l'État un contrôle sur l'IA.

52 Mark BROMLEY et Kolja BROCKMANN, « Controlling Technology Transfers and Foreign Direct Investment : The Limits of Export Controls », dans Stockholm International Peace Research Institute (SIPRI), *Yearbook 2019. Armaments, Disarmament and International Security. 10. Dual-Use and Arms Trade Controls*, Oxford University Press, 2019, p. 538, à la page 538, en ligne : <https://www.sipri.org/sites/default/files/SIPRIYB19c10sV.pdf> :« Unlike almost all other items that are subject to export control, technology can take an intangible form (e.g. knowledge that is carried in an individual's head) and be transferred using intangible means (e.g. emails or other means of transferring data electronically). »

53 Lindsey R. SHEPPARD, Erol YAYBOKE et Carolina G. RAMOS, « The Shift Toward Data Localization », CSIS – International Security Program, juillet 2021, en ligne : <https://csis-website-prod.s3.amazonaws.com/s3fs-public/Sheppard_TheShiftTowardDataLocalization_PullOutSection.pdf?aqf3UcmQdpPGu9cJYmrw1uaXBw3ShbrW>. Au niveau de l'Union européenne, voir le chapitre V (art. 44 et suiv.) du *Règlement général sur la protection des données* (RGPD) relatif au contrôle des flux transfrontières de données à caractère personnel, lesquelles ne peuvent être exportées vers des pays tiers qu'à certaines conditions.

[72] Une des législations les plus citées à cet égard est l'exigence prévue dans une loi russe de 2014, obligeant explicitement les plateformes à héberger sur le territoire russe les données relatives aux personnes physiques et morales russes. Mais il est des situations où une libre circulation de principe pourrait se heurter, plus subtilement, à une localisation *de fait* de certaines données sur le territoire national. Ainsi, même en l'absence d'une interdiction explicite, la circulation transatlantique des données à caractère personnel entre les États-Unis et l'Union européenne est demeurée incertaine jusqu'à tout récemment depuis que la Cour de justice européenne a invalidé en juillet 2020 l'accord relatif au transfert des données personnelles qui avait été négocié entre l'Union européenne et les États-Unis (affaire *Schrems II*)[54].

[73] En 2017, le Bureau du représentant américain au commerce (USTR ou *Office of the United States Trade Representative*) a qualifié la localisation de données de « barrière au commerce numérique » et une menace pour les libertés dans le cyberespace (OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, 2017). L'année précédente, seules les exigences de localisation de données posées par les gouvernements russe et indonésien ont été soulignées comme susceptibles d'entraver la réalisation d'économies d'échelle, de décourager l'investissement étranger et de faire obstacle à la circulation des données transfrontières qui sont autant d'ingrédients essentiels au commerce électronique (OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE, 2016). À la différence des barrières tarifaires, « [l]a menace [que les obstacles non tarifaires constituent] pour le système commercial multilatéral est d'autant plus insidieuse que leur application se fait de façon sournoise et que la seule limite à leur multiplication est l'imagination humaine » (BARTENSTEIN & LAVALLÉE, 2003, p. 371). À cet égard, l'Accord Canada-États-Unis-Mexique (ACEUM), entré en vigueur en juillet 2020, tout en insistant sur « les avantages économiques et sociaux qu'apporte la protection des renseignements personnels des usagers du commerce numérique » (art. 19.8), défend aux parties d'interdire ou de limiter « le transfert transfrontières de renseignements, y compris de renseignements personnels, par voie électronique si cette activité s'inscrit dans le cadre d'activités commerciales exercées par une personne visée » (art. 19.11). Une partie ne doit pas non plus exiger des entreprises que leurs installations informatiques soient situées sur son territoire « comme condition à l'exercice des activités commerciales sur ce territoire » (art. 19.12). Ce dispositif a bien sûr tout à voir avec la domination des États-Unis du marché de l'infonuagique (*cloud computing*). Les exigences des États-Unis quant à la localisation sur leur territoire des données personnelles des usagers américains de TikTok, pour des raisons de sécurité nationale, démontrent bien que le principe de la libre circulation des données relève plus d'un artifice rhétorique que d'une exigence juridique ou éthique stricte pour l'hégémon. Les considérations relatives à la sécurité nationale dans le cadre de l'utilisation de TikTok s'avèrent également dénuées de

54 Il s'agit du *Bouclier de protection des données UE-États-Unis*, tel qu'adopté au niveau de l'Union européenne par la *Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis*, Journal officiel L 207, 1er août 2016. Depuis la décision de juillet 2020 rendue par la Cour de justice européenne, un accord de principe a été conclu en mars 2022 entre la Commission européenne et les États-Unis. Il s'agit du nouveau *Cadre transatlantique de protection des données personnelles* qui cherche tant à favoriser les flux de données transatlantiques qu'à répondre aux préoccupations exprimées dans l'affaire *Schrems II* de juillet 2020 : COMMISSION EUROPÉENNE, *Déclaration conjointe de la Commission européenne et des États-Unis sur le cadre transatlantique de protection des données personnelles*, communiqué de presse, Bruxelles, 25 mars 2022, en ligne : <https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_2087>. Le Cadre transatlantique a fait l'objet d'une décision d'adéquation de la Commission européenne le 10 juillet 2023 : COMMISSION EUROPÉENNE, *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework*, C(2023)4745 final, Bruxelles, 10 juillet 2023.

fondement, comme le souligne une étude récente de Georgia Tech (MUELLER & FARHAT, 2023) que nous verrons plus amplement ci-après.

2. DES PRÉOCCUPATIONS RELATIVES À LA SÉCURITÉ NATIONALE AU REGARD D'UNE TECHNOLOGIE DUALE

[74] La prégnance de la technologie dans l'activité humaine et ses multiples usages soulève pour les États de sérieuses préoccupations relatives à la sécurité nationale. D'une juridiction à l'autre, l'expression « sécurité nationale » a toujours été investie d'une ambiguïté sémantique. Comme l'affirme l'historien américain Melvyn P. Leffler :

> To be sure, national security […] is an ambiguous symbol. Security is used to encompass so many goals that there is no uniform agreement on what it encompasses and hence no universal understanding of the concept. Certainly it involves more than national survival. But just what is involved is often left vague and indeterminate. (LEFFLER, 1990, p. 144; aussi FORCESE, 2015).

[75] Outre la sûreté de l'État au sens strict, elle renvoie à cette « raison d'État » faisant prévaloir l'intérêt – politique – de la conservation de l'État / du Prince / du Monarque sur toute autre considération. Au-delà de l'expression consacrée par Botero (1589) – homme politique et penseur italien de la Renaissance, le « discours de la raison d'État » (TARANTO, 2001; MEINECKE, 1973; BENYEKHLEF, 2014) remonte loin dans l'histoire de l'État. Dans sa conception moderne, la sécurité nationale est aussi un autre héritage de Westphalie :

> The new idea of the nation-state took a different approach. Peace and stability could be better served if people were not slaughtering each other over some universal principle – in that case, religion. It would be far better to have an international system based on the equilibrium of nation-states dedicated to the limited purposes of national sovereignty and self-defense. (HOLMES, 2015, p. 17).

[76] Sans doute l'exception relative à la « sécurité nationale » est-elle indispensable pour préserver les intérêts de l'État. En l'absence d'une définition précise et échappant par ce fait à un contrôle juridictionnel strict, la « sécurité nationale » peut devenir une hydre à mille têtes susceptible de justifier des prises de position arbitraires, voire contradictoires, qui, sous couvert de secret d'État, sont pourtant soustraites à toute critique et discussion[55]. Les multiples usages possibles de l'IA rendent cette technologie sensible au regard des intérêts de sécurité nationale de l'État. Les décisions récentes de l'administration Biden relatives à l'interdiction d'exportation vers la Chine de certains types de semi-conducteurs confirment que l'IA constitue un enjeu stratégique majeur (CLARK & SWANSON, 2022). Est-il besoin de rappeler cet énoncé de mission de la

55 Lire aussi Harro HÖPFL, *sub verbo* « Reason of State », dans *Encyclopedia of Medieval Philosophy*, Springer, Dordrecht, 2011, p. 1113, DOI : <https://doi.org/10.1007/978-1-4020-9729-4_433> : « More narrowly, reason of state meant a "Machiavellian" disregard for legal, moral, and religious considerations when the "interests of the state" or "necessity" required it. Particularly contentious were the justifiability of dishonesty, duplicity, breach of faith and even treaty obligations, violence against opponents and competitors, illegal taxation, disregard of the claims of traditional institutions and officeholders, and the practice of religious toleration. »

DARPA : « make pivotal investments in breakthrough technologies for national security »[56]? Ainsi, selon le Pentagone :

> AI systems will […] be used in the pursuit of power. We fear AI tools will be weapons of first resort in future conflicts. AI will not stay in the domain of superpowers or the realm of science fiction. AI is dual-use, often open-source, and diffusing rapidly. State adversaries are already using AI-enabled disinformation attacks to sow division in democracies and jar our sense of reality. States, criminals, and terrorists will conduct AI-powered cyber-attacks and pair AI software with commercially available drones to create 'smart weapons'. It is no secret that America's military rivals are integrating AI concepts and platforms to challenge the United States' decades-long technology advantage. We will not be able to defend against AI-enabled threats without ubiquitous AI capabilities and new warfighting paradigms. We want the men and women in national security departments and agencies to have access to the best technology in the world to defend themselves and us, and to protect our interests and those of our allies and partners. (U.S. NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE, 2021, p. 1–2).

[77] Dans le contexte des menaces à la « sécurité nationale », ces *smart weapons* renvoient en l'occurrence à l'instrumentalisation de l'IA dans les campagnes de désinformation. Cette instrumentalisation illustre le rôle du web intelligent en tant que nouvel acteur géopolitique aux côtés des médias traditionnels. Son champ d'influence dépasse la désinformation électorale :

> Elections are one example of the many domains where this can occur. Financial markets, which can be subject to short-term manipulation, are another example. Foreign affairs could be affected as rumors spread quickly around the world through digital platforms. Social movements can also be targeted through dissemination of false information designed to spur action or reaction among either supporters or opponents of a cause. » (VILLASENOR, 2020, nos soulignés).

[78] L'avènement du cyberespace transforme la nature même de la guerre et de la domination et donne lieu à l'émergence de nouvelles stratégies de puissance. Les préoccupations relatives à la cybersécurité font planer le spectre d'une « guerre cognitive » (ISAAC, 2022) où on observe une multiplication des rançongiciels ciblant « des personnes, des infrastructures essentielles, des entreprises et tous les ordres de gouvernement » (SÉCURITÉ PUBLIQUE CANADA, 2022; aussi SAVOLLE, 2023), l'accroissement des cyberattaques parrainées par des États. Au surplus, des stratégies de désinformation, de manipulation et d'ingérence étrangère ainsi que de corruption de l'intégrité des infrastructures informatiques, participent à alimenter la guerre par, sur et au-delà du cyberespace (ISAAC, 2022).

[79] L'exemple qui a attiré le plus d'attention des États et du public sont ces opérations d'influence ou de désinformation menées lors d'élections. Certaines techniques faisant appel à l'intelligence artificielle, comme les *deepfakes*, le clonage de la voix et la

56 Defense Advanced Research Projects Agency (DARPA), *Mission*, en ligne : <https://www.darpa.mil/about-us/mission>.

génération automatique de textes (HELMUS, 2022; HONIGBERG, 2022) – dont les résultats atteignent un réalisme stupéfiant – peuvent être instrumentalisés à des fins de désinformation, de propagande et de manipulation malveillantes.

[80] Le 10 mars 2023, le ministère de la Sécurité publique du Canada a lancé une consultation publique sur la mise en œuvre d'un « registre visant la transparence en matière d'influence étrangère pour renforcer la protection contre l'influence étrangère malveillante » (SÉCURITÉ PUBLIQUE CANADA, 2023) et les mesures qui pourraient être adoptées à cette fin. Selon le document de consultation, une « influence étrangère malveillante » comprend une série d'activités entreprises par des gouvernements étrangers ainsi que leurs mandataires pour influencer l'opinion publique canadienne et conduire à l'adoption de politiques favorables aux intérêts étrangers au détriment du Canada (SÉCURITÉ PUBLIQUE CANADA, 2023). Or, ces activités, lorsque facilitées, voire conduites, par des technologies intelligentes et autonomes, risquent de ne pas être régies par les régimes législatifs en vigueur pour accroître la transparence et gérer les conflits d'intérêt[57]. Ceux-ci visent en effet les personnes physiques plutôt que les machines.

[81] Cela étant dit, l'influence des médias, souvent considérée déterminante dans l'opinion publique, doit être relativisée. Dès 1948, LAZARSFELD, BERELSON & GAUDET ont relevé que les discussions informelles influeraient davantage l'opinion politique, surtout des indécis, que des sources d'information plus formelles, comme celles des médias. Dans leur étude, trois quarts des répondants qui, à un moment donné, avaient voulu s'abstenir de voter, ont mentionné l'influence des amis, de la famille et des connaissances personnelles pour expliquer qu'ils se soient finalement ravisés.

[82] L'étude de Lazarsfeld, Berelson et Gaudet rejoint les résultats d'études plus récentes relativisant l'hypothèse de l'*agenda-setting*, selon laquelle les perceptions du public relatives à certains sujets sont causalement déterminées par l'importance que les médias accordent à ces derniers. Cette hypothèse, formulée pour la première fois par les professeurs MCCOMBS et SHAW en 1972, a évolué depuis vers celle d'un *agenda-building* insistant plutôt sur l'influence réciproque et conjointe des différentes sources d'information dans la « construction » de l'agenda, qu'il s'agisse des journalistes, des médias, des décideurs politiques et du public (CHARRON, 2009).

[83] Ainsi, l'étude longitudinale des flux Twitter, évoquée plus haut, n'a relevé aucune relation significative entre l'exposition des utilisateurs aux « interférences » russes aux élections présidentielles de 2016 et le changement des comportements électoraux et des attitudes politiques (EADY et al., 2023). Tout comme dans l'étude de Lazarsfeld, Berelson et Gaudet, l'*influence* étrangère se serait restreinte à un sous-groupe d'utilisateurs dont les convictions républicaines étaient déjà résolues (EADY et al., 2023). Il ne s'agit donc pas tant d'« influencer » que de « conforter »; plus d'effet bulle

57 Dont la *Loi sur le lobbying*, L.R.C. 1985, c. 44 (4e suppl.), la *Loi sur les conflits d'intérêts*, L.C. 2006, c. 9 et la *Loi électorale du Canada*, L.C. 2000, c. 9. La *Loi sur le lobbying* oblige les lobbyistes-conseils à divulguer des renseignements concernant l'identité de leur client, qui peut être un gouvernement étranger, lorsque le lobbyiste-conseil communique directement ou indirectement, contre rémunération, avec un titulaire d'une charge publique sur un sujet de lobbying réglementé. La *Loi sur les conflits d'intérêts* impose aux titulaires d'une charge publique une obligation de prévenir les conflits entre leurs intérêts privés et les devoirs publics, y compris après leur mandat. La *Loi électorale du Canada* interdit aux personnes qui ne sont pas citoyens et résidents permanents du Canada de participer aux activités électorales.

que d'*agenda-setting*. Aussi, selon les études de cas des chercheurs BENKLER, FARIS et ROBERTS (2018), la crise de démocratie que les Américains ont connue à ce jour s'avère plus structurelle que technologique. La polarisation politique résulte moins de l'avènement de l'Internet et du cyberespace que du réalignement des élus eux-mêmes ainsi que d'un écosystème médiatique de droite alimentant asymétriquement une rhétorique fortement partisane.

[84] Au-delà de la désinformation et des manipulations électorales, la sécurité nationale a été également mise de l'avant pour justifier des restrictions de plus en plus importantes au libre commerce et aux accords de libre-échange :

> **National security** is used for trade protectionist policies since the industries involved include defense-related companies, high-tech firms, and food producers. The argument here is that industries such as aerospace, advanced electronics, and semi-conductors are vital components of national defense policy and that relying on foreign manufacturers would seriously affect a nation's defense in time of war. By having manufacturing for defense items protected from foreign competition, trade protectionism is necessary for a nation's existence. (GUARINO, 2018)

[85] Ainsi, au soutien de l'imposition par l'administration Trump des droits de douane sur l'acier et l'aluminium importés de plusieurs pays, les États-Unis invoquent l'article 232 du *Trade Expansion Act of 1962*[58]. Cette loi du Congrès autorise le président américain à limiter, par des tarifs douaniers ou autrement, les importations de produits ou de matériaux provenant d'autres pays dans des circonstances qui menacent la sécurité nationale. Selon les résultats de l'enquête menée à l'initiative de l'*US Secretary of Commerce*, la hausse des importations d'acier et d'aluminium de l'étranger ferait peser un risque substantiel sur la capacité des industries nationales de produire de l'acier et de l'aluminium pour les infrastructures critiques et la défense nationale, et ce, surtout en période de crise. Ces mesures protectionnistes ont été contestées par plusieurs États-parties auprès de l'OMC. Même si l'article XXI de l'Accord général sur les tarifs douaniers et le commerce (GATT) permet d'imposer des restrictions au commerce international sur la base de la sécurité nationale, l'OMC a rejeté les prétentions des États-Unis dans une série de décisions liées rendues le 9 décembre 2022. Les panels ont considéré que les préoccupations des États-Unis ne renvoient pas à une situation de gravité suffisante au plan international qui soit constitutive d'un « temps de guerre ou [un] cas de grave tension internationale » au sens du paragraphe XXI(b)(iii) du GATT[59].

[86] Dans la même veine, la *Federal Communications Commission* (FCC) a estimé, en mars 2021, que les entreprises chinoises Huawei, ZTE, Hytera Communications,

---

58 *Trade Expansion Act of 1962*, Pub. L. 87-794, 76 Stat. 872. Sur l'interprétation que fait le Congrès américain de la portée de l'article 232, lire : CONGRESSIONAL RESEARCH SERVICE, *Section 232 of the Trade Expansion Act of 1962*, mis à jour le 1er avril 2022, en ligne : <https://crsreports.congress.gov/product/pdf/IF/IF10667#:~:text=Section%20232%20of%20the%20Trade%20Expansion%20Act%20of%201962%20(19,also%20self%2Dinitiate%20an%20investigation>

59 Lire les décisions (rapports) nO DS544 (Chine), DS552 (Norvège), DS556 (Suisse), DS564 (Turquie) de l'OMC rendues le 9 décembre 2022, en ligne : <https://www.wto.org/french/news_f/news22_f/544_552_556_564r_f.htm>. Le 26 janvier 2023, les États-Unis ont notifié leur intention d'appeler ces décisions rendues par l'Organe de règlement des différends (ORD) de l'OMC.

Hangzhou Hikvision Digital Technology et Dahua Technology faisaient peser un « risque inacceptable » pour la sécurité nationale des États-Unis (BERMAN, MAIZLAND & CHATZKY, 2023; KHAN, 2022). Dans la foulée, le premier ministre canadien a annoncé l'interdiction d'utiliser le nouvel équipement 5G de Huawei et de ZTE ainsi que les services gérés par ces derniers au motif que ces fournisseurs étrangers « pourraient être contraints à se conformer à des directives extrajudiciaires d'un gouvernement étranger qui iraient à l'encontre des lois canadiennes ou seraient préjudiciables aux intérêts du Canada » (INNOVATION, SCIENCES ET DÉVELOPPEMENT ÉCONOMIQUE CANADA, 2022, par. 5).

[87] Un autre exemple d'actualité est la saga TikTok. Alors que la version « internationale » de l'application TikTok[60] est elle-même bannie en Chine continentale pour des raisons liées à la censure du Web, plusieurs autorités gouvernementales – suivant sur cette voie les États-Unis – ont exprimé des préoccupations relatives à la sécurité nationale en raison du contrôle de TikTok par une société mère (ByteDance) basée en Chine. Des législatures aux médias, les discussions publiques semblent avoir été alimentées par de simples allégations en l'absence de données probantes sur la question[61]. Beaucoup ont exprimé la crainte que l'algorithme de recommandation de TikTok puisse être contrôlé et manipulé par le gouvernement communiste chinois à des fins de propagande et de désinformation. Or, la faculté d'user d'algorithmes de recommandation pour influencer, c'est-à-dire changer l'opinion publique, reste à démontrer. Cette recommandation tendrait principalement à renforcer les opinions et préférences existantes. Tel que mentionné plus haut, une étude longitudinale des flux Twitter d'un échantillon représentatif de répondants américains n'a relevé aucune relation significative entre l'exposition des utilisateurs aux « interférences » russes aux élections présidentielles de 2016 et le changement des comportements électoraux et des attitudes politiques (EADY et al., 2023). Ces interférences étrangères auraient été concentrées sur un sous-groupe d'utilisateurs qui s'identifiaient déjà fortement comme républicains (EADY et al., 2023), en raison, selon nous, du jeu des algorithmes de recommandation qui tendent à rejoindre les utilisateurs qui sont déjà réceptifs ou qui partagent des convictions du même ordre que le contenu de la propagande. Il en irait ainsi de la popularité des réseaux sociaux et, partant, de l'efficacité des opérations d'influence. Quand bien même des algorithmes de recommandation puissent être recâblés pour exposer les utilisateurs à des contenus plus diversifiés, allant même à l'encontre de leurs intérêts exprimés, il est probable que la popularité de telles

60 Pellaeon Lin, de The Citizen Lab, nous présente en ces termes les 2 versions de TikTok : « The app started in China under the name Douyin, and was released as TikTok tailored for the international market. The two versions continue to be maintained for these separate markets. TikTok and Douyin are both for sharing short videos and have similar interfaces. However, they are entirely separate apps that have access to two separate platforms. However, they are entirely separate apps that have access to two separate platforms. Users on these two platforms cannot interact with each other. These platforms also have different registration processes, policies, and content ». Pellaeon LIN, *TikTok vs Douyin. A Security and Privacy Analysis*, Citizen Lab Research Report nO 137, University of Toronto, 22 mars 2021, p. 2, en ligne : <https://tspace.library.utoronto.ca/bitstream/1807/123974/1/Report%23137--TikTok.pdf>.

61 Voir notamment Milton L. MUELLER et Karim FARHAT, *TikTok and US national security*, Georgia Institute of Technology, School of Public Policy, Internet Governance Project, 8 janvier 2023, p. 5, en ligne : <https://www.internetgovernance.org/wp-content/uploads/TikTok-and-US-national-security-3.pdf> : « When one investigates the statements and motives of TikTok's critics, one finds that many think any exports from China, or any trades with that country, should be treated as if they were weapons ». Pellaeon LIN, *TikTok vs Douyin. A Security and Privacy Analysis*, Citizen Lab Research Report nO 137, University of Toronto, 22 mars 2021, p. 2, en ligne : <https://tspace.library.utoronto.ca/bitstream/1807/123974/1/Report%23137--TikTok.pdf> : « These bans centre on concerns that because TikTok's parent company ByteDance is headquartered in Beijing, the Chinese government could compel it to share personal data of foreign nationals. Although this type of cooperation is a possible scenario, little research has been done to understand how and to what degree the Chinese government dictates control over TikTok's operation ».

plateformes, et partant, de l'efficacité des opérations d'influence conduites, déclinera d'elle-même[62].

[88] En tout état de cause, l'utilisation des données collectées par TikTok à des fins qui compromettraient la sécurité nationale ne peut l'être que dans la mesure où ces données elles-mêmes concernent *a priori* la sécurité nationale (p. ex. secret militaire, contrôle et emplacement d'infrastructures critiques) et ont été partagées de manière à exposer des renseignements sensibles. Or, les données collectées par TikTok ont trait principalement aux habitudes de divertissement et aux centres d'intérêts de ses utilisateurs et leur valeur est avant tout commerciale, en ce qu'elles permettent la mise en place de stratégies d'écoute de médias sociaux, de présence et de publicité. Si menace à la sécurité nationale il y a, il s'agirait d'un risque commun à toutes les plateformes. Et ce risque ne s'atténuerait pas en bannissant une seule (des nombreuses) plateforme. Compte tenu de la quantité phénoménale d'informations que les médias sociaux rendent publiques et de celles que les utilisateurs partagent sur différentes plateformes, il n'est pas nécessaire de contrôler une seule application (parmi d'autres) pour « espionner » les utilisateurs. Plusieurs outils de renseignement de sources ouvertes (OSINT) permettent déjà une collecte extensive et une analyse croisée des données, et ce, sans requérir une assistance active des fournisseurs de services comme TikTok.

[89] La comparution récente du directeur général de TikTok au Congrès[63] montre bien que la polémique autour de ce réseau s'inscrit dans la rivalité de puissance entre les États-Unis et la Chine. Le *Center for Strategic & International Studies* (CSIS), évoquant les exigences de localisation des données, est d'avis que justifier ces restrictions au motif de la sécurité nationale représente une tentative à peine voilée d'affirmer sa souveraineté nationale et de raffermir le contrôle de ses citoyens dans le domaine du numérique aux dépens d'autres libertés et droits individuels ainsi que des intérêts économiques (YAYBOKE, RAMOS & SHEPPARD, 2021).

CONCLUSION

[90] L'Internet et l'IA sont devenus « à la fois un champ spécifique des rivalités des grandes puissances mondiales et […] un instrument particulier pour atteindre d'autres objectifs géopolitiques » (ISAAC, 2022, p. 4; aussi BENYEKHLEF, 2015). En effet, l'IA est un enjeu de pouvoir en ce qu'elle reconfigure tant les espaces que les acteurs et les règles du jeu géopolitique. Si l'effacement des frontières n'a pas attendu la « quatrième révolution industrielle », la prolifération d'outils numériques renforce et accélère ce processus avec l'émergence du cyberespace et de métavers se superposant aux espaces géopolitiques traditionnels. Le cyberespace est un nouveau terrain de jeu pour

62 Milton L. MUELLER et Karim FARHAT, *TikTok and US national security*, Georgia Institute of Technology, School of Public Policy, Internet Governance Project, 8 janvier 2023, p. 15, en ligne : <https://www.internetgovernance.org/wp-content/uploads/TikTok-and-US-national-security-3.pdf> : « TikTok's success – both as a commercial enterprise and as a point of convergence for the exchange of cultural products at scale – is based on identifying what people want, and giving it to them. Even if one considers TikTok (like other social media) to be the digital equivalent of an addictive drug, the chemistry of this drug requires letting users freely choose to engage with the content that interests them. Only then do platforms acquire data that trains effective AI recommendations. Without this feedback, the 'drug' doesn't work. Not many Americans get their endorphins from videos of Xi Jinping, the 17th 5-year plan, or militant images of Chinese nationalism ».

63 L'audition peut être visionnée en rediffusion sur le site Web de la commission parlementaire : U.S. HOUSE OF REPRESENTATIVES (Committee on Energy and Commerce), « TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms », 23 mars 2023, en ligne : <https://energycommerce.house.gov/events/full-committee-hearing-tik-tok-how-congress-can-safeguard-american-data-privacy-and-protect-children-from-online-harms>.

les acteurs tant étatiques que privés : en témoigne leur course à l'hégémonie *de* l'IA et *par* l'IA. Nous avons mis en lumière la manière dont les États tentent de monopoliser cette (nouvelle) ressource stratégique et le rôle charnière de celle-ci non seulement dans le contrôle des espaces géopolitiques existants, mais aussi dans l'appropriation de nouveaux espaces d'allégeance, de solidarité, de rivalité et de souveraineté. Loin d'être un espace d'émancipation affranchi de la surveillance des États, le cyberespace – et l'IA qui l'instrumentalise – est devenu bel et bien un (nouvel) espace de domination politico-culturelle et d'alliances stratégiques où les États westphaliens occupent une place prépondérante. Cela étant, il s'avère difficile de réguler ce cyberespace dont la consolidation et la vitalité ne dépendent pas que du pouvoir régalien des États, mais bien de l'expertise hautement technique d'acteurs économiques bien souvent privés.

RÉFÉRENCES BIBLIOGRAPHIQUES

Table de la législation

- **Textes canadiens**

Liste des marchandises et technologies d'exportation contrôlée, DORS/89-202

Loi électorale du Canada, L.C. 2000, c. 9

Loi sur le lobbying, L.R.C. 1985, c. 44 (4e suppl.)

Loi sur les conflits d'intérêts, L.C. 2006, c. 9

- **Textes américains**

CHIPS and Science Act of 2022, Pub. L. 117-167

Trade Expansion Act of 1962, Pub. L. 87-794, 76 Stat. 872

- **Textes européens**

Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, Journal officiel L 207, 1er août 2016

Législation sur l'intelligence artificielle de l'UE, 2024
Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), Journal officiel, L 119, 4 mai 2016

Règlement (UE) 2021/821 du Parlement européen et du Conseil du 20 mai 2021 instituant un régime de l'Union de contrôle des exportations, du courtage, de

l'assistance technique, du transit et des transferts en ce qui concerne les biens à double usage (refonte)

Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques), Journal officiel L 265 du 12 octobre 2022

Règlement (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques), Journal officiel L 277 du 27 octobre 2022

Table des jugements

- **Jurisprudence canadienne**

Nevsun Resources Ltd. c. *Araya*, 2020 CSC 5.

- **Jurisprudence internationale**

Affaire du temple de Préah Vihéar (Cambodge c. Thaïlande), C.I.J. Recueil 1962, p. 6 (15 juin 1962).

- **Monographies et ouvrages collectifs**

ANGHIE, A., *Imperialism, Sovereignty and the Making of International Law*, Cambridge, Cambridge University Press, 2004.

BENKLER, Y., R. FARIS et H. ROBERTS, *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*, Oxford University Press, 2018, DOI : https://doi.org/10.1093/oso/9780190923624.001.0001.

BENYEKHLEF, K., *Une possible histoire de la norme. Les normativités émergentes de la mondialisation* (2e éd.), Montréal, Thémis, 2015.

BENOÎT, F., *The Valley. Une histoire politique de la Silicon Valley*, Paris, Les Arènes, 2019.

BEUCHER, S. et A. CIATTONI (dir.), *Dictionnaire de géopolitique*, Paris, Hatier, 2021.
CHAMPEIL-DESPLATS, V. et D. LOCHAK (dir.), *Libertés économiques et droits de l'homme*, Presses universitaires de Paris Ouest, 2011.

CREMONA, M. et J. SCOTT (dir.), *EU Law Beyond EU Borders: The Extraterritorial Reach of EU Law*, Oxford University Press, 2019, DOI : https://doi.org/10.1093/oso/9780198842170.001.0001.

DEBRAY, R., *Éloge des frontières*, Gallimard, 2013.

DURAND, C., *Technoféodalisme. Critique de l'économie numérique*, La Découverte, Paris, 2020.

FOUCAULT, M., *Sécurité, territoire et population. Cours au Collège de France 1977-1978*, Paris, Gallimard-Éditions du Seuil, 2004.

FOUCHER, M., *Fronts et frontières. Un tour du monde géopolitique* (2e éd.), Paris, Fayard, 1991.

GOLDSMITH, J. et T. WU, *Who Controls the Internet? Illusions of a Borderless World*, New York (NY), Oxford University Press, 2006.

GREENWALD, G., *No place to hide. Edward Snowden, the NSA and the Surveillance State*, Signal, 2014.

GUTHLEBEN, D., *La fabuleuse histoire des inventions – de la maîtrise du feu à l'intelligence artificielle*, Dunod, 2021.

LACOSTE, Y., *La géographie, ça sert, d'abord, à faire la guerre*, 2e éd., La Découverte, 2014.

LAÏDI, A., *Le droit, nouvelle arme de guerre économique*, Paris, Actes Sud, 2019.

LAZARSFELD, P.F., B. BERELSON et H. GAUDET, *The People's choice: How the Voter Makes Up His Mind in a Presidential Campaign*, Columbia University Press, 1948.

LATIL, A., *Le droit du numérique. Une approche par les risques*, Paris, Dalloz, 2023.

MCFARLAND, T., *Autonomous Weapon Systems and the Law of Armed Conflict. Compatibility with International Humanitarian Law*, Cambridge, Cambridge University Press, 2020.

MCLUHAN, M. et Q. FIORE, *War and Peace in the Global Village*, McGraw-Hill, 1968.

MEARSHEIMER, J.J., *The Tragedy of Great Power Politics* (version mise à jour), WW. Norton, New York, 2014.

MEINECKE, F., *L'idée de la raison d'État dans l'histoire des temps modernes*, Genève, Droz, 1973.

MORIN, M., *L'usurpation de la souveraineté autochtone. Le cas des peuples de la Nouvelle-France et des colonies anglaises de l'Amérique du Nord*, Boréal, 1997.

MOROZOV, E., *The Net Delusion: The Dark Side of Internet Freedom*, PublicAffairs, 2012.

MULDER, N., *The Economic Weapon. The Rise of Sanctions as a Tool of Modern War*, New Haven, Yale University Press, 2022.

Ó TUATHAIL, G., S. DALBY et P. ROUTLEDGE, *The Geopolitcs Reader* (2e éd.), London, Routledge, 2006.

ROCHER, G., *Traité de sociologie du droit et des ordres juridiques*, Montréal, Thémis, 2022.

ROMANO, S., *L'ordre juridique*, Dalloz, 2002.

ROSIÈRE, S., *Géographie politique & Géopolitique* (3e éd.), Paris, Ellipses, 2021.

SAUL, S., *L'impérialisme, passé et présent : un essai*, coll. « 5 points », Les Indes savantes, 2022.

SAULNIER, A., *Les barbares numériques : Résister à l'invasion des GAFAM*, coll. « Polemos », Écosociété, 2022.

SIMPSON, G., *Great Powers and Outlaw States. Unequal Sovereigns in the International Legal Order*, Cambridge, Cambridge University Press, 2004.

SNOWDEN, E., *Permanent Record*, Macmillan, 2020.

TUFEKCI, Z., *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, Yale University Press, 2017.

VON JHERING, R., *L'esprit du droit romain dans les diverses phases de son développement* (traduit par O. DE MEULENAERE), t. 1, 2e éd., Marescq, Paris, 1880.
WERBACH, K., *The Blockchain and the New Architecture of Trust*, MIT Press, 2023.

- **Articles de revues et études d'ouvrages collectifs**

AGUITON, C. et D. CARDON, « Web participatif et innovation collective », (2008) 50-1 *Hermès* 75, DOI : https://doi.org/10.4267/2042/24155.

ALFONSI, C., « Taming Tech Giants Requires Fixing the Revolving Door », *Kennedy School Review* (18 février 2020).

AUDIER, S., « Hégémonie industrialiste et utopisme technologique », dans S. AUDIER (dir.), *L'âge productiviste : Hégémonie prométhéenne, brèches et alternatives écologiques*, Paris, La Découverte, 2019, 89.

BADIE, B., « Introduction. Comment l'hégémonie américaine s'est faite, puis défaite », (2019) *Fin du leadership américain?* 9. https://doi.org/10.3917/dec.badie.2019.01.0009.

BARRIER, F., « Les systèmes armés létaux autonomes (Sala) : vers une nouvelle course à l'armement ? », (2018) 810 *Revue Défense Nationale* 19.

BARTENSTEIN, K. et S. LAVALLÉE, « L'écolabel est-il un outil du protectionnisme "vert" », (2003) 44-3 *C. de D.* 361, 371, DOI : https://doi.org/10.7202/043757ar .

BAUDER, H. et R. MUELLER, « Westphalian Vs Indigenous Sovereignty: Challenging Colonial Territorial Governance », (2021) *Geopolitics*, DOI : https://doi.org/10.1080/14650045.2021.1920577.

BELLAYER-ROILLE, A., « Entre souveraineté et transnationalité, les défis du droit de la mer », (2014) 95-3 *Revue internationale et stratégique* 111, DOI : https://doi.org/10.3917/ris.095.0111.

BENYEKHLEF, K., « Introduction. Les secrets du droit », dans K. BENYEKHLEF (dir.), *Les secrets du droit*, Montréal, Thémis, 2014, p. 1.

BODÓ, B., J. K. BREKKE et J.-H. HOEPMAN, « Decentralisation in the blockchain space », (2021) 10-2 *Internet Policy Review*, DOI : https://doi.org/10.14763/2021.2.1560.

BOUQUET, B., « La complexité de la légitimité », (2014) 8-4 *Vie sociale* 13, DOI : https://doi.org/10.3917/vsoc.144.0011.

BROMLEY, M. et K. BROCKMANN, « Controlling technology transfers and foreign direct investment : The limits of export controls », dans Stockholm International Peace Research Institute (SIPRI), *Yearbook 2019. Armaments, Disarmament and International Security. 10. Dual-Use and Arms Trade Controls*, Oxford University Press, 2019, p. 538. https://www.sipri.org/sites/default/files/SIPRIYB19c10sV.pdf.

BROMLEY, M. et P.D. WEZEMAN, « Multiplateral embargoes on arms and dual-use items », dans Stockholm International Peace Research Institute (SIPRI), *Yearbook 2019. Armaments, Disarmament and International Security. 10. Dual-Use and Arms Trade Controls*, Oxford University Press, 2019, p. 511. https://www.sipri.org/yearbook/2019/10.

CAMPAGNA, N., « III. La liberté », dans Norbert CAMPAGNA (dir.), *Thomas Hobbes. L'Ordre et la liberté*, Paris, Michalon, 2000, p. 85.
CASEY, A. et A. NIBLETT, « Self-Driving Contracts », (2017) 43-1 *The Journal of Corporation Law* 1.

CASEY, A. et A. NIBLETT, « Self-Driving Laws », (2016) 66 *University of Toronto Law Journal* 429.

CATTARUZZA, A. (2019a), « Approche géopolitique des frontières » dans *Introduction à la géopolitique*, Paris, Armand Colin, 2019, p. 84.

CATTARUZZA, A. (2019b), « Introduction » dans *Introduction à la géopolitique*, Paris, Armand Colin, 2019, p. 15.

CATTARUZZA, A. et K. LIMONIER, « Le territoire entre jeux de pouvoir et représentations » dans *Introduction à la géopolitique*, Paris, Armand Colin, 2019, p. 56.

CERUZZI, P.E., « Aux origines américaines de l'Internet : projets militaires, intérêts commerciaux, désirs de communauté », (2012) 18-1 *Le Temps des médias* 15, DOI : https://doi.org/10.3917/tdm.018.0015.

CHARRON, J., « Médias et sources : Les limites du modèle de l'agenda-setting », dans Arnaud MERCIER (dir.), *Le journalisme*, Paris, CNRS Éditions, 2009, DOI : https://doi.org/10.4000/books.editionscnrs.13917.

DABONÉ, Z., « Les groupes armés dans un système de droit international centré sur l'État », (2011) 93-2 *Revue internationale de la Croix-Rouge* 85.

DEMCHAK, C.C. et F. SPIDALIERI, « Tallying Unlearned Lessons from the First Cybered Conflict Decade, 2010-2020 », (2022) *The Cyber Defense Review* 15.

DE SOUSA SANTOS, B., « Droit : une carte de la lecture déformée. Pour une conception post-moderne du droit », (1988) 10 *Droit et société* 363.

DOUZET, F., « La géopolitique pour comprendre le cyberespace », (2014) 1-2 *Hérodote* 3, https://doi.org/10.3917/her.152.0003.

DOUZET, F. et A. DESFORGES, « Du cyberespace à la datasphère. Le nouveau front pionnier de la géographie », (2018) 32 *Netcom* 87. https://journals.openedition.org/netcom/3419.

EADY, G., T. PASKHALIS, J. ZILINSKY, R. BONNEAU, J. NAGLER et J. A. TUCKER, « Exposure to the Russian Internet Research Agency foreign influence campaign on Twitter in the 2016 US election and its relationship to attitudes and voting behavior », (2023) 14 *Nature Communications*, DOI : https://doi.org/10.1038/s41467-022-35576-9.

EL YAHYAOUI, Y., « Chapitre troisième. Les plateformes numériques « globales » : puissance et abus de position », dans Y. EL YAHYAOUI (dir.), *Économie des plateformes numériques. Captation de la valeur, pouvoir de marché et communs collaboratifs*, Paris, L'Harmattan, 2021, 149.

FARIS, D.M., « La révolte en réseau : le "printemps arabe" et les médias sociaux », (2012) 1 *Politique étrangère* 99, DOI : https://doi.org/10.3917/pe.121.0099.

FARR, J., « Point: The Westphalia Legacy and the Modern Nation-State », (2005) 80-3/4 *International Social Science Review* 156.

FLIGSTEIN, N., « Le mythe du marché », (2001) 139-4 *Actes de la recherche en sciences sociales* 3, DOI : https://doi.org/10.3917/arss.139.0003.

FOISNEAU, L., « Chapitre VII. La puissance absolue du souverain », dans Luc

FOISNEAU (dir.), *Hobbes et la toute-puissance de Dieu*, Paris, Presses Universitaires de France, 2000, 257. https://www.cairn.info/hobbes-et-la-toute-puissance-de-dieu--9782130509561-page-257.htm.

FORCESE, C., « Through a Glass Darkly: The Role and Review of "National Security" Concepts in Canadian Law », (2015) 43-4 *Alberta Law Review* 963.

FOUCHER, M., « Sciences et géopolitique », (2014) *La science en question(s)* 213, DOI : https://doi.org/10.3917/sh.wievi.2014.01.0213.

HÖPFL, H., *sub verbo* « Reason of State », dans *Encyclopedia of Medieval Philosophy*, Springer, Dordrecht, 2011, p. 1113, DOI : https://doi.org/10.1007/978-1-4020-9729-4_433.

I VIDAL, J.B., M. DRACA et C. FONS-ROSEN, « Revolving Door Lobbyists », (2012) 102-7 *American Economic Review* 3731.

JEANGÈNE VILMER, J.-B., « Chapitre II. Le réalisme », dans Jean-Baptiste JEANGÈNE VILMER (dir.), *Théories des relations internationales*, Paris cedex 14, Presses Universitaires de France, 2020, 23. https://www.cairn.info/theories-des-relations-internationales--9782130785644-page-23.htm.

JOHNSON, D., « Les tigres et dragons asiatiques : un modèle de *leapfrog* pour les lions africains? », (2018) 69 *France Forum*. https://www.institutjeanlecanuet.org/content/les-tigres-et-dragons-asiatiques-un-modele-de-leapfrog-pour-les-lions-africains.

KADIOĞLU KUMTEPE, C., « A Brief Introduction to Blockchain Dispute Resolution », (2021) 14-2 *J. Marshall L. J.* 138.

KLÖTGEN, P., « La frontière et le droit, esquisse d'une problématique », (2012) 1962 *Revue générale du droit* 45.

LAPERCHE, B., « Les inventions, la science et la guerre : la place du secret », (2005) 21-1 *Innovations* 109, DOI : https://doi.org/10.3917/inno.021.0109.
LAVIEC, J.-P., « Chapitre VII. Les régimes des accords d'investissement », dans *Protection et promotion des investissements. Étude de droit international économique*, Genève, Graduate Institute Publications, 1985, 241, DOI : https://doi.org/10.4000/books.iheid.4199.

LEFFLER, M.P., « National Security », (1990) 77-1 *Journal of American History* 143: https://www.jstor.org/stable/2078646.

LE MOIGN, A., « Les groupes armés non étatiques et l'internationalisation de leurs soutiens », (2018) 30-1 *Les Champs de Mars* 201, DOI : https://doi.org/10.3917/lcdm.030.0201.

LESLIE, S.W., « The biggest 'Angel' of them all: the Military and the making of Silicon Valley », dans M. KENNEY (dir.), *Understanding Silicon Valley: The anatomy of an entrepreneurial region*, Stanford University Press, 2000, p. 48.

MATHEY, N., « Les droits de l'homme et libertés fondamentales des personnes morales de droit privé », *RTDciv.* 2008.205.

MCCOMBS, M.E. et D.L. SHAW, « The Agenda-Setting Function of Mass Media », (1972) 36-2 *The Public Opinion Quarterly* 176. https://www.jstor.org/stable/2747787.

MIAILHE, N., « Géopolitique de l'Intelligence artificielle : le retour des empires? », (2018) 3 *Politique étrangère* 105. https://doi.org/10.3917/pe.183.0105.

OULD MOHAMEDOU, M.-M., « D'Al Qaïda à l'État islamique : acteurs non-étatiques mondialisés et évolution de la violence politique post-moderne », (2017) 172-4 *Relations internationales* 3, DOI : https://doi.org/10.3917/ri.172.0003.

OULD MOHAMEDOU, M.-M., « In Search of the Non-Western State: Historicising and De-Westphalianising Statehood », dans D. BERG-SCHLOSSER, B. BADIE et L. MORLINO (dir.), *The SAGE Handbook of Political Science*, SAGE Publications, 2020, p. 1335.

POHLE, J. et D. VOELSEN, « Centrality and Power. The Struggle over the Techno-Political Configuration of the Internet and the Global Digital Order », (2022) 14 *Policy & Internet* 13.

POSTEL-VINAY, K., « Géographie et pouvoir », (2001) 10-1 *Critique internationale* 51. https://doi.org/10.3917/crii.010.0051.

RACINE, J.-B., « Droit économique et droits de l'homme : introduction générale », dans L. BOY, J.-B. RACINE et F. SIIRIAINEN (dir.), *Droits économiques et droits de l'homme*, Larcier 2009, p. 7.

RASMUSSEN, A., « Sciences et guerres », dans D. PESTRE (dir.), *Histoire des sciences et des savoirs* (t. 3), Paris. Seuil, 2015, 47.

RETAILLÉ, D., « L'État, le territoire et les relations internationales, nouvelles approches géographiques », (1993) 68-69 *Revue des mondes musulmans et de la Méditerranée* 41. https://doi.org/10.3406/remmm.1993.2553.

ROUSSEAU, D., « Les droits de l'homme de la troisième génération », (1987) 19-2 *Revue interdisciplinaire d'études juridiques* 19, DOI : https://doi.org/10.3917/riej.019.0019.

SOUPIZET, J.-F., « Les géants du Net face aux États », (2021) 444-5 *Futuribles* 5, DOI : https://doi.org/10.3917/futur.444.0005.

STINE, D.D., « U.S. Civilian Space Policy Priorities: Reflections 50 Years After Sputnik », dans W.N. CALLMERS (dir.), *Space Policy and Exploration*, New York, Nova Science Publishers, 2008, p. 1.

STRICKLAND, J.M., « The Declining Value of Revolving-Door Lobbyists: Evidence from the American States », (2020) 64-1 *American Journal of Political Science* 67.

TARANTO, D., « Le discours de la raison d'État », dans A. CAILLE, C. LAZERRI et M. SENELLART (dir.), *Histoire raisonnée de la philosophie morale et politique. De l'Antiquité aux Lumières* (tome 1), Paris, Flammarion, 2001, 318.

TESCHKE, B., « La théorisation du système étatique westphalien : les relations internationales de l'absolutisme au capitalisme », (2012) 52 *Cahiers de recherche sociologique* 13. https://doi.org/10.7202/1017276ar.

THIBOUT, C., « Les GAFAM et l'État : réflexion sur la place des grandes entreprises technologiques dans le champ du pouvoir », (2022) 125 *Revue internationale et stratégique* 75.

ÜLGEN, F., « La dynamique de financement de l'innovation », (2007) 25-1 *Innovations* 45, DOI : https://doi.org/10.3917/inno.025.0045.

VIHAM, A., « Geoeconomic Analysis and the Limits of Critical Geopolitics: A New Engagement with Edward Luttwak », (2018) 23 *Geopolitics* 1.

VILLATOUX, P., « La guerre des codes : une cyberguerre avant la lettre », (2018) 814-9 *Revue Défense Nationale* 46, DOI : https://doi.org/10.3917/rdna.814.0046.

YATES, S. et É. CARDIN-TRUDEAU, « Lobbying "from within" : A new perspective on the revolving door and regulatory capture », (2021) 64-2 *Administration publique du Canada* 301. https://doi.org/10.1111/capa.12412.

- **Mémoires, thèses, rapports et conférences**

BARAN, P., *On Distributed Communications Networks*, Santa Monica (Californie), RAND Corporation, septembre 1962. https://www.rand.org/content/dam/rand/pubs/papers/2005/P2626.pdf.

BARLOW, J.P., *Déclaration d'indépendance du cyberespace*, 1996. https://doi.org/10.3917/ecla.blond.2000.01.0047.

BOULLIER, D., *Puissance des plateformes numériques, territoires et souverainetés*, Sciences Po Paris (Centre d'études européennes et de politique comparée), Document inédit, avril 2022.

COMITÉ INTERNATIONAL DE LA CROIX ROUGE, *Position du CICR sur les systèmes d'armes autonomes*, Document de référence, Genève, mai 2021. https://www.icrc.org/fr/document/position-cicr-systemes-armes-autonomes.

DANIC, O., *L'émergence d'un droit international des investissements. Contribution des traités bilatéraux d'investissement et de la jurisprudence du CIRDI – vol. 1 –*, thèse de doctorat, Université Paris Ouest Nanterre La Défense, 2012. https://hal.science/tel-02166275/document.

ELIOT, Dr. L.B., « Legal Micro-Directive Amplification Via Artificial Intelligence » (2021), DOI : https://dx.doi.org/10.2139/ssrn.3950089.

FUTURE OF LIFE INSTITUTE, « Pause Giant AI Experiments : An Open Letter », 22 mars 2023. https://futureoflife.org/open-letter/pause-giant-ai-experiments/.

GODBOUT, A.-S., Conférence « Blockchain et cryptoactifs : une entrée en la matière », conférence organisée par l'Institut intelligence et données (IID), la Chaire de recherche sur les contrats intelligents et la chaîne de blocs de la Chambre des notaires du Québec et la Faculté de droit de l'Université Laval, 10 mars 2023.

GOLDSTEIN, J.A., G. SASTRY, M. MUSSER, R. DIRESTA, M. GENTZEL et K. SEDOVA, *Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations*, Georgetown University's Center for Security and Emerging Technology OpenAI et Stanford Internet Observatory, janvier 2023, DOI : https://doi.org/10.48550/arXiv.2301.04246.

HELMUS, T.C., *Artificial Intelligence, Deepfakes, and Disinformation. A Primer*, RAND Corporation, juillet 2022. https://www.rand.org/content/dam/rand/pubs/perspectives/PEA1000/PEA1043-1/RAND_PEA1043-1.pdf.

HONIGBERG, B., *The Existential Threat of AI-Enhanced Disinformation Operations*, Just Security, 8 juillet 2022. https://www.justsecurity.org/82246/the-existential-threat-of-ai-enhanced-disinformation-operations/.

ISAAC, H., *Histoire et géopolitique de l'Internet. Une généalogie de la guerre cognitive*, Université Paris-Dauphine, Conférence du 25 octobre 2022, Montréal, Chaire LexUM en information juridique, Faculté de droit, Université de Montréal. https://basepub.dauphine.psl.eu//bitstream/handle/123456789/23310/Guerre-cognitive-Chaire-LexUM-octobre-2022.pdf?sequence=2&isAllowed=y.

LEWIS, A., *The Effectiveness of the Wassenaar Arrangement as the Non-Proliferation Regime for Conventional Weapons*, Freeman Spogli Institute for International Studies, Stanford University, 2015.

LIN, P., *TikTok vs Douyin. A Security and Privacy Analysis*, Citizen Lab Research Report No. 137, University of Toronto, 22 mars 2021. https://tspace.library.utoronto.ca/bitstream/1807/123974/1/Report%23137--TikTok.pdf.

LONGHAIS, S., *Document de lecture des données issues de l'inventaire sur les outils algorithmiques dans les administrations publiques*, Laboratoire de cyberjustice, août 2021. https://www.cyberjustice.ca/publications/document-de-lecture-des-donnees-issues-de-linventaire-sur-les-outils-algorithmiques-dans-les-administrations-publiques/.

MORAN, M. et M. LITWAK, « The Industry Agenda: Big Tech », Revolving Door Project (2 février 2021). https://therevolvingdoorproject.org/the-industry-agenda-big-tech/.

MUELLER, M.L. et K. FARHAT, *TikTok and US national security*, Georgia Institute of Technology, School of Public Policy, Internet Governance Project, 8 janvier 2023. https://www.internetgovernance.org/wp-content/uploads/TikTok-and-US-national-security-3.pdf.

OBSERVATOIRE DES MULTINATIONALES, *GAFAM NATION. La toile d'influence des géants du web en France*, 13 décembre 2022. https://multinationales.org/IMG/pdf/gafam_v4.pdf.

REINSCH, W.A. et T. DENAMIEL, « The CHIPS and Science Act Guardrails' Implications for the U.S. Trade Agenda », Center for Strategic & International Studies (CSIS), 13 avril 2023. https://www.csis.org/analysis/chips-and-science-act-guardrails-implications-us-trade-agenda.

SAVOLLE, A., *Les enjeux géopolitiques et économiques liés au cyberespace*, Cahier du CÉRIUM no 29, Centre d'études et de recherches internationales (CÉRIUM) de l'Université de Montréal, 2023. https://cerium.umontreal.ca/recherche-et-publications/publications/cahiers-du-cerium/un-cahier/news/detail/News/les-enjeux-geopolitiques-et-geoeconomiques-lies-au-cyberespace/.

SCHNEIDER, N., « Decentralization: An Incomplete Ambition », (2019) 12-4 *Journal of Cultural Economy* 265, DOI : https://doi.org/10.1080/17530350.2019.1589553.

SCHNEIDER-PETSINGER, M., « Reforming the World Trade Organization. Prospects for Transatlantic Cooperation and the Global Trade System », *Chatham House* (11 septembre 2020), en ligne : https://www.chathamhouse.org/2020/09/reforming-world-trade-organization/03-us-and-wto.

SHEPPARD, L.R., E. YAYBOKE et C.G. RAMOS, « The shift toward data localization », CSIS – International Security Program, juillet 2021. https://csis-website-prod.s3.amazonaws.com/s3fs-public/Sheppard_TheShiftTowardDataLocalization_PullOutSection.pdf?aqf3UcmQdpPGu9cJYmrw1uaXBw3ShbrW.

SPECIAL COMPETITIVE STUDIES PROJECT, *The Future of Conflicts and the New Requirements of Defense. Interim Panel Report*, Washington, octobre 2022: https://www.scsp.ai/wp-content/uploads/2022/10/Defense-Panel-IPR-Final.pdf.

VANEL, G., *Le concept d'hégémonie en économique politique internationale*, cahier de recherche 03-02, UQÀM (Centre d'études sur l'intégration et la mondialisation), avril 2003. https://ceim.uqam.ca/db/IMG/pdf/Cahier_Vanel.pdf.

VAZQUEZ ROJAS, T., *Projet de recherche. Algorithmes et administration publique – rapport sur l'inventaire d'outils*, Laboratoire de Cyberjustice, hiver 2021.

www.cyberjustice.ca/files/sites/102/Sylvie-Rapport_Algorithme-et-administration-publique.pdf.

VILLASENOR, J., *How to deal with AI-enabled disinformation*, rapport, 23 novembre 2020. https://www.brookings.edu/research/how-to-deal-with-ai-enabled-disinformation/.

YAYBOKE, E., C.G. RAMOS et L.R. SHEPPARD, *The Real National Security Concerns over Data Localization*, Center for Strategic & International Studies (CSIS), 23 juillet 2021. https://www.csis.org/analysis/real-national-security-concerns-over-data-localization.

- **Documents gouvernementaux**

CANADA, BUREAU DE LA CONCURRENCE, *Examen de la* Loi sur la concurrence *du Canada à l'ère numérique*, mémoire, 8 février 2022. https://ised-isde.canada.ca/site/bureau-concurrence-canada/fr/comment-nous-favorisons-concurrence/promotion-concurrence/conseils-interventions-bureau-concurrence-matiere-reglementation/examen-loi-concurrence-canada-lere-numerique.

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA), *Mission*. https://www.darpa.mil/about-us/mission.

ÉTATS-UNIS, COMMITTEE ON THE JUDICIARY OF THE HOUSE OF REPRESENTATIVES (Subcommittee on Antitrust, Commercial, and Administrative Law), *Investigation of Competition in Digital Markets*, partie 1, Washington, U.S. Government Publishing Office, July 2022. https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf.

ÉTATS-UNIS, CONGRESSIONAL RESEARCH SERVICE, *Section 232 of the Trade Expansion Act of 1962*, mis à jour le 1er avril 2022. https://crsreports.congress.gov/product/pdf/IF/IF10667#:~:text=Section%20232%20of%20the%20Trade%20Expansion%20Act%20of%201962%20(19,also%20self%2Dinitiate%20an%20investigation.

GOUVERNEMENT DU CANADA, *Guide de la Liste des marchandises et technologies d'exportation contrôlée du Canada*, version de décembre 2020. https://www.international.gc.ca/trade-commerce/guides/export_control_list-liste_exportation_controlee.aspx?lang=fra.

H.R. 3825 – Ending Platform Monopolies Act, 117e Congrès (2021-2022). https://www.congress.gov/bill/117th-congress/house-bill/3825.

INNOVATION, SCIENCES ET DÉVELOPPEMENT ÉCONOMIQUE CANADA, *Énoncé de politique – Sécuriser le système de télécommunications au Canada*, gouvernement du Canada, 19 mai 2022. https://www.canada.ca/fr/innovation-sciences-developpement-economique/nouvelles/2022/05/enonce-de-politique--securiser-le-systeme-de-telecommunications-au-canada.html.

OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE (USTR), *Fact Sheet: Key Barriers to Digital Trade*, 31 mars 2016. https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2016/march/fact-sheet-key-barriers-digital-trade.

OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE (USTR), *Key Barriers to Digital Trade*, 31 mars 2017. https://ustr.gov/about-us/policy-offices/press-office/fact-sheets/2017/march/key-barriers-digital-trade.

OFFICE OF THE UNITED STATES TRADE REPRESENTATIVE (USTR), *Statement from USTR Spokesperson Adam Hodge*, 9 décembre 2022. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/december/statement-ustr-spokesperson-adam-hodge.

SÉCURITÉ PUBLIQUE CANADA, *Accroître la transparence en matière d'influence étrangère : Examiner les mesures pour renforcer l'approche du Canada*, document de consultation du public et des intervenants, 10 mars 2023. https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2023-nhncng-frgn-nfluence/index-fr.aspx.

SÉCURITÉ PUBLIQUE CANADA, *Notes des comités parlementaires : Rançongiciels et auteurs de menaces persistantes évoluées parrainés par la Russie*, 20 avril 2022. https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20220930/05-fr.aspx.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE (GAO), *How Artificial Intelligence Is Transforming National Security*, 19 avril 2022. https://www.gao.gov/blog/how-artificial-intelligence-transforming-national-security.

U.S. HOUSE OF REPRESENTATIVES (Committee on Energy and Commerce), « TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms », 23 mars 2023. https://energycommerce.house.gov/events/full-committee-hearing-tik-tok-how-congress-can-safeguard-american-data-privacy-and-protect-children-from-online-harms.

U.S. NATIONAL SECURITY COMMISSION ON ARTIFICIAL INTELLIGENCE, *Final Report*, 2021, p. 1 et 2. https://nscai.wpenginepowered.com/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

- **Documents internationaux**

Arrangement de Wassenaar sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage, Wassenaar, 19 décembre 1995.

ASSEMBLÉE GÉNÉRALE DES NATIONS UNIES, *Traité sur le commerce des armes*, New York, adopté le 2 avril 2013.

COMMISSION EUROPÉENNE, *Commission Implementing Decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*

on the adequate level of protection of personal data under the EU-US Data Privacy Framework, C(2023)4745 final, Bruxelles, 10 juillet 2023.

COMMISSION EUROPÉENNE, *Déclaration conjointe de la Commission européenne et des États-Unis sur le cadre transatlantique de protection des données personnelles*, communiqué de presse, Bruxelles, 25 mars 2022. https://ec.europa.eu/commission/presscorner/detail/fr/ip_22_2087.

COMMISSION EUROPÉENNE, *Proposition de Directive du Parlement européen et du Conseil relative à l'adaptation des règles en matière de responsabilité civile extracontractuelle au domaine de l'intelligence artificielle (Directive sur la responsabilité en matière de l'IA*, COM(2022) 496 final, Bruxelles, 28 septembre 2022.

COMMISSION EUROPÉENNE, *Proposition de Directive du Parlement européen et du Conseil relative à la responsabilité du fait des produits défectueux*, COM(2022) 495 final, Bruxelles, 28 septembre 2022.

COMMISSION EUROPÉENNE ET ÉTATS-UNIS, *Cadre transatlantique de protection des données personnelles*, mars 2022.

Convention des Nations Unies sur le droit de la mer, Montego Bay, 10 décembre 1982.

Convention relative à l'aviation civile internationale, Chicago, 7 décembre 1944.
Multi-Party Interim Appeal Arbitration Arrangement (MPIA), mars 2020.

ORGANISATION MONDIALE DU COMMERCE (OMC), « L'OMC distribue les rapports du Groupe spécial concernant les mesures des États-Unis visant les produits en acier et en aluminium », communiqué de presse, 9 décembre 2022. https://www.wto.org/french/news_f/news22_f/544_552_556_564r_f.htm.

Traité et principes des Nations Unies relatifs à l'espace extra-atmosphérique, y compris la Lune et les autres corps célestes, 27 janvier 1967.

- **Articles de journaux et sur le Web**

BASCHUK, B., « U.S. Raises Prospect of Blocking Passage of WTO Budget », *Bloomberg* (12 novembre 2019), en ligne : https://www.bloomberg.com/news/articles/2019-11-12/u-s-is-said-to-raise-prospect-of-blocking-passage-of-wto-budget#xj4y7vzkg.

BENYEKHLEF, K., « L'arrangement de Wassenaar et la réglementation des technologies de surveillance à usage double », *Conventions* (6 novembre 2012). https://convention-s.fr/decryptages/larrangement-de-wassenaar-et-la-reglementation-des-technologies-de-surveillance-a-usage-double/.

BERMAN, N., L. MAIZLAND et A. CHATZKY, « Is China's Huawei a Threat to U.S. National Security? », *Council on Foreign Relations*, 8 février 2023. https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security.

BUCKLEY, J.L., « A Technological Pearl Harbor », *The New York Times* (23 juillet 1971). https://www.nytimes.com/1971/07/23/archives/a-technological-pearl-harbor.html.

CAULIER, S., « Depuis ses débuts, le vieux Continent est hostile à l'émergence de champions », *Le Monde* (11 septembre 2022). https://www.lemonde.fr/economie/article/2022/09/11/numerique-depuis-ses-debuts-l-europe-est-ouvertement-hostile-a-l-emergence-de-champions_6141160_3234.html.

CHAPMAN, S., « Edward Snowden & the NSA PRISM Program: What You Need to Know in 2023 », *PrivacyJournal.net* (17 mai 2023). https://www.privacyjournal.net/edward-snowden-nsa-prism/.

CLARK, D. et A. SWANSON, « U.S. Restricts Sales of Sophisticated Chips to China and Russia », *New York Times* (31 août 2022). https://www.nytimes.com/2022/08/31/technology/gpu-chips-china-russia.html.

DE CATHEU, L., « Le techno-nationalisme, matrice idéologique de la confrontation technologique », *Le Grand Continent* (4 mai 2021). https://legrandcontinent.eu/fr/2021/05/04/le-techno-nationalisme-matrice-ideologique-de-la-confrontation-technologique/.

GLADWELL, M., « Small Change. Why the Revolution will not be Tweeted », *The New Yorker* (27 septembre 2010). https://www.newyorker.com/magazine/2010/10/04/small-change-malcolm-gladwell.

GONZÁLEZ, R.P., « Le technonationalisme chinois, outil d'hégémonie technologique », *Atalayar* (22 mars 2021). https://atalayar.com/fr/content/le-technonationalisme-chinois-outil-dh%C3%A9g%C3%A9monie-technologique.

GUARINO, A.S., « The Economic Effects of Trade Protectionism », *FocusEconomics* (1er mars 2018). https://www.focus-economics.com/blog/effects-of-trade-protectionism-on-economy.

HEATER, B., « Google disables Maps live traffic tools in Ukraine », *Tech Crunch* (28 février 2022). https://techcrunch.com/2022/02/28/google-disables-maps-live-traffic-tools-in-ukraine/.

HOLMES, K.R., « What Is National Security? », (2015) *Index of U.S. Military Strength* 17. https://www.heritage.org/sites/default/files/2019-10/2015_IndexOfUSMilitaryStrength_What%20Is%20National%20Security.pdf.

KHAN, I., « FCC Bans Huawei and ZTE Gear Over National Security Risk », *CNET* (29 novembre 2022). https://www.cnet.com/news/politics/fcc-bans-huawei-and-zte-gear-over-national-security-risk/.

LAURIER, P., « La Silicon Valley et le mythe de la génération spontanée », *The Conversation* (4 décembre 2018). https://theconversation.com/la-silicon-valley-et-le-mythe-de-la-generation-spontanee-108088.

LOONAM, J.P. et C. REARDON, « Extraterritoriality: The US Perspective », *Global Investigations Review* (3 janvier 2020), en ligne : https://globalinvestigationsreview.com/guide/the-practitioners-guide-global-investigations/2020/article/extraterritoriality-the-us-perspective.

MCKENNA, A. et M. BOUTROS, « L'Internet par satellite de Starlink est-il un instrument de guerre? », *Le Devoir* (29 novembre 2022). https://www.ledevoir.com/monde/772575/monde-l-internet-par-satellite-de-starlink-est-il-un-instrument-de-guerre.

METZ, C., « Paul Baran, the link between nuclear war and the internet », *WIRED* (4 septembre 2012). https://www.wired.co.uk/article/h-bomb-and-the-internet.

PRAKASH, A., « How Technology Companies Are Shaping the Ukraine Conflict », *Scientific American* (28 octobre 2022). https://www.scientificamerican.com/article/how-technology-companies-are-shaping-the-ukraine-conflict/.

REICH, R.B., « The Rise of Techno-Nationalism », *The Atlantic Monthly* (mai 1987). https://www.theatlantic.com/magazine/archive/1987/05/the-rise-of-techno-nationalism/665772/.

SANDERS, N.E. et B. SCHNEIER, « How ChatGPT Hijacks Democracy », *The New York Times* (15 janvier 2023). https://www.nytimes.com/2023/01/15/opinion/ai-chatgpt-lobbying-democracy.html.

TAPSCOTT, D. et A. TAPSCOTT, « How Canada can be a global leader in blockchain technology », *The Globe and Mail* (10 mars 2017). https://www.theglobeandmail.com/report-on-business/rob-commentary/how-canada-can-be-a-global-leader-in-blockchain-technology/article34259697/.

TAPSCOTT, D. et A. TAPSCOTT, « Une course à l'hégémonie technologique entre la Chine et les États-Unis », *Courrier international* (28 septembre 2018). https://www.courrierinternational.com/article/une-course-lhegemonie-technologique-entre-la-chine-et-les-etats-unis.