Explorer la souveraineté numérique et son impact sur l'Internet

Décembre 2022

Synthèse

Au début de l'année, une large alliance de citoyens a publié une charte de souveraineté numérique au Brésil.[1] Dans cette charte, ils déplorent l'extraction et la manipulation effrénées des données locales par les grandes entreprises technologiques et exhortent le gouvernement à soutenir les technologies interopérables et ouvertes, ainsi que les centres de données à usage commun.

À l'autre bout du monde, dans un autre pays vaste et peuplé, le gouvernement indien a demandé à tous les fournisseurs de services de conserver pendant cinq ans les informations concernant leurs utilisateurs et de synchroniser les horloges de leurs systèmes avec une seule source de temps : les serveurs du gouvernement. Ces dispositions figurent dans les nouvelles directives de sécurité de l'Équipe indienne d'intervention en cas d'urgence informatique (CERT-In)[2], dans le but d'augmenter le nombre de rapports d'incidents de sécurité et de protéger l'infrastructure numérique du pays.

Ces deux prises de position projettent une vision de la souveraineté dans le cyberespace, mais la manière dont ils veulent parvenir à cette vision, et les acteurs qui la conduisent, sont radicalement différents.

L'Internet Society a lancé cette étude dans le but de définir une position sur la souveraineté numérique. Loin d'être un idéal monolithique, nous avons découvert une notion large et mal définie que différents groupes interprètent et appliquent de manière diverse à travers le monde. On peut citer par exemple les gouvernements qui souhaitent contrôler la manière dont les opérations et les ressources Internet sont gérées, les entreprises locales qui dénoncent la domination des plateformes technologiques étrangères, les communautés autochtones qui veulent sauvegarder les connaissances et les ressources locales, et les individus qui veulent

1 « Programa de Emergência para a soberania digital. »https://cartasoberaniadigital.lablivre.wiki.br/carta/

2 CERT-In Ministère indien de l'électronique et des technologies de l'information (MeitY) Équipe indienne d'intervention d'urgence informatique (CERT-In), 2022.https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

affirmer leur autonomie dans leurs interactions avec les appareils, les plateformes et la façon dont ils gèrent leurs données.

Ce rapport cherche à comprendre les différentes approches qui existent, sachant que chacune aura un impact différent sur Internet, et à proposer un cadre pour analyser cet impact. En ce sens, il ne cherche pas à consolider ou à approuver une définition ou une position unique de la souveraineté numérique.

Cette étude restreint sa portée à l'examen des politiques gouvernementales qui ont explicitement adopté la souveraineté numérique. Elle les regroupe en fonction de leurs objectifs déclarés et évalue leur impact sur le fondement technique d'Internet. Notre objectif est de fournir un guide nuancé pour déterminer si les politiques de souveraineté numérique peuvent nous faire passer d'un Internet qui profite à tous à une série de réseaux fragmentés et fermés où les opportunités qui découlent de la connexion mondiale se perdent.[3]

Nous présentons d'abord un résumé des tendances de politiques en Asie-Pacifique, en Afrique et en Europe (y compris en Russie), puis nous regroupons les politiques et les mesures en fonction (a) de leurs objectifs, et (b) des acteurs habilités à atteindre ces objectifs. Cette catégorisation a mis en évidence deux approches distinctes de la souveraineté numérique :

1. Les politiques qui assurent la **sécurité nationale par un contrôle accru de l'État** ont pour ambition de faire appliquer des lois dans le domaine numérique afin de renforcer la sécurité nationale. Cette approche s'appuie sur des acteurs étatiques habilités à centraliser le contrôle des opérations du réseau, à concentrer le pouvoir dans les mains de l'État et à limiter le pouvoir des opérateurs. Ce type de souveraineté numérique présente des risques importants pour les caractéristiques et les valeurs fondamentales d'Internet et pourrait conduire à une fragmentation directe de celui-ci.
2. Les politiques qui recherchent **l'autodétermination économique dirigée par les acteurs économiques** veulent renforcer les acteurs de l'économie nationale et, dans une moindre mesure, assurer la résilience de la chaîne d'approvisionnement. Ces mesures n'interfèrent pas intentionnellement avec les opérations du réseau d'Internet. Elles tentent plutôt de stimuler les économies numériques locales en

3 Bien que nous apprécions le discours académique sur la souveraineté en tant que concept politique, ce rapport se concentre sur les conséquences de la mise en œuvre pratique de cette notion sur Internet - en particulier, comment les politiques numériques menées par l'État ont un impact sur les fondements techniques et l'évolution d'Internet.

> créant des conditions de concurrence équitables et en réduisant les obstacles à leur accès en rendant les données et autres ressources plus accessibles. Certaines politiques peuvent être protectionnistes et interférer avec les opérations du réseau. Globalement, elles cherchent à accroître les opportunités créées par un réseau mondial et des sociétés et économies connectées, et sont susceptibles d'améliorer les conditions qui permettent aux acteurs locaux de tirer parti d'Internet.

Ce rapport montre que les politiques de souveraineté numérique peuvent avoir un impact négatif sur le fonctionnement d'Internet et, plus important encore, sur notre capacité à utiliser Internet. Afin de minimiser le risque de perturber le fonctionnement de cette ressource mondiale dont nos économies et nos sociétés dépendent de plus en plus, nous encourageons vivement les personnes chargées de l'élaboration des politiques à réaliser une évaluation de l'impact sur Internet dans le cadre de leurs processus, en particulier dans le cadre de mesures visant à relever les défis de l'environnement numérique.

Notre analyse initiale se concentre sur trois régions, mais reconnaît que la souveraineté numérique, qu'elle soit implicite ou explicitement déclarée, gagne du terrain dans les ordres du jour politiques du monde entier. D'autres études sur cette question pourraient bénéficier de l'utilisation de ce cadre et de la boîte à outils « Mode de fonctionnement du réseau Internet », pour évaluer l'effet que les politiques de souveraineté numérique peuvent avoir sur l'Internet mondial, indépendamment de l'endroit où elles se trouvent.

Table des matières

I. Introduction : Qu'est-ce que la souveraineté numérique ?

La notion de « souveraineté numérique » est historiquement associée aux tentatives des gouvernements non démocratiques de contrôler les opérations et les ressources Internet à l'intérieur de leurs frontières.[4] Dans les discussions de politique internationale, ce concept a été utilisé pour remettre en question les approches existantes de la gouvernance de l'Internet qui reposent sur des processus décentralisés et multipartites[5].

Aujourd'hui, la « souveraineté numérique » est utilisée plus largement dans
différents contextes à travers le monde, et à des fins différentes.

Elle peut inclure des interventions visant à donner aux individus et aux groupes un plus grand contrôle sur l'information, mais aussi des mesures qui donnent aux ministères de la justice et de l'intérieur un contrôle direct sur le trafic Internet au quotidien. Bon nombre de ces politiques couvrent différentes facettes du domaine numérique. Cette étude se concentre uniquement sur celles qui peuvent avoir un impact sur le fonctionnement d'Internet.

Les interventions qui relèvent de la souveraineté numérique peuvent avoir un impact sur Internet, mais le terme lui-même ne nous dit pas grand-chose sur la nature de cet impact. En raison de cette ambiguïté, l'Internet Society ne prend pas position sur la souveraineté numérique en tant que concept. L'objectif de ce rapport est d'évaluer comment les différentes politiques qui la mettent en œuvre peuvent interagir avec Internet.

1.1 Le concept de souveraineté tel que nous le connaissons

Les perceptions de la souveraineté numérique varient considérablement, en raison des différentes interprétations du concept de souveraineté lui-même. La souveraineté évoque des idées d'autorité et de contrôle, tant au niveau individuel qu'au niveau de l'État, et ces idées sont fortement

4 Adam Segal, « Le régime alternatif de cybergouvernance de La Chine », Council of Foreign Relations, 13 mars 2020 https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf

5 Julien Nocetti. « Concours et conquête : la Russie et la gouvernance mondiale de l'Internet. » Affaires internationales 91.1 (2015) : 111-130. Milton L Mueller., « China and Global Internet Governance: A Tiger by the Tail », éditions de Ronald Deibert et autres, Access Contested: Security, Identity, and Resistance in Asian Cyberspace (Cambridge, MA, 2011; éd. en ligne, MIT Press Scholarship Online, 22 août 2013)

marquées par l'histoire, la culture et le contexte. L'un des aspects de la souveraineté est la capacité de l'État à exercer un pouvoir et un contrôle sur les ressources et les personnes d'un territoire donné. Dans les discussions sur la souveraineté numérique, cette notion s'étend à la capacité des États à faire respecter leurs lois dans le domaine numérique et à limiter l'influence des acteurs extérieurs, notamment la domination du marché par des entreprises étrangères et leur influence sur les questions nationales.

La souveraineté peut également être comprise par rapport à d'autres États, comme une question d'indépendance vis-à-vis de la pression ou de l'influence extérieure, et dans le contexte national comme une affirmation de la légitimité politique et de l'État de droit. La reconnaissance de la souveraineté d'un État par d'autres États constitue la base du droit international, ainsi que des traités et accords qui s'y rapportent. Dans le contexte de la souveraineté numérique, cette perspective tournée vers l'extérieur peut se traduire par des préoccupations quant à l'autodétermination et à la légitimité de la participation des acteurs non étatiques aux processus de gouvernance.

Enfin, la souveraineté est également évoquée pour exprimer la capacité des individus, et des communautés culturellement distinctes, à agir avec un degré raisonnable d'autonomie et à prendre des décisions de manière indépendante. Ce point de vue implique que la légitimité à gouverner provient du consentement des citoyens et, par conséquent, du droit à l'autodétermination de l'individu ou du groupe. Par conséquent, certaines questions de souveraineté numérique se concentrent sur les droits du citoyen à la confidentialité et à la liberté d'expression dans l'espace numérique, notamment en relation avec le contrôle de leurs données. (L'« identité auto-souveraine » ou « décentralisée », c'est-à-dire les mécanismes non dépendants d'une plateforme qui permettent aux individus d'administrer directement leur propre identité numérique sur le web, n'est pas couverte par ce rapport).

Pour compliquer ces interprétations, la souveraineté numérique est souvent utilisée de manière superposée et interchangeable avec d'autres expressions similaires telles que « souveraineté technologique », « souveraineté de l'information », « cyber-souveraineté », « souveraineté de l'Internet » et « souveraineté sur les données ».

Le terme a été vulgarisé dans les déclarations du gouvernement de la République populaire de Chine il y a près de vingt ans.[6] Plus récemment, il a été utilisé par les pays du Sud pour répondre à la consolidation croissante et au pouvoir des entreprises sur Internet. Dans ce contexte, la souveraineté numérique est un moyen de contrer le « colonialisme numérique » [7]des pays industrialisés.

1.2 Objectif de ce rapport

Ce rapport ne vise pas à fournir une description définitive de la souveraineté numérique, ni à étudier les nuances de son utilisation dans le discours politique, mais à accepter que ces variations existent et à analyser comment les différentes interprétations de la souveraineté numérique peuvent avoir des influences très différentes sur le fondement technique d'internet.

Il résume tout d'abord les tendances récentes en Asie-Pacifique, en Afrique et en Europe (y compris la Russie), dans les régions où la souveraineté numérique s'est manifestée de la manière la plus explicite dans les affaires publiques et le discours des gouvernements. Il décrit ensuite notre méthodologie d'analyse des mesures politiques pertinentes, ainsi que les principaux types de politiques que nous avons observés. Nous avons évalué ces types à l'aide de la **Boîte à outils pour l'évaluation de l'impact sur Internet**[8] de l'Internet Society et des tendances régionales, afin de déterminer les diverses influences des politiques de souveraineté numérique sur le **Mode de fonctionnement du réseau Internet**[9] et les caractéristiques clés de l'Internet ouvert, mondialement connecté, sécurisé et digne de confiance.

II. Tendances régionales en matière de souveraineté numérique

6 Ministère des Affaires étrangères de la République populaire de Chine, « Remarques de S.E. Xi Jinping, président de la République populaire de Chine, lors de la cérémonie d'ouverture de la deuxième Conférence mondiale sur Internet », 16 décembre 2015, https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.

6 China.org.cn, « Texte intégral : Stratégie internationale de coopération sur le cyberespace », 7 mars 2017, http://www.china.org.cn/chinese/2017-03/07/content_40424606_2.htm.

7 Julia Pohle et Thorstein Thiel. « Souveraineté numérique ». Examen de la politique Internet, 5 décembre 2020.https://doi.org/10.14763/2020.4.1532]

8 Internet Society, « Boîte à outils pour l'évaluation de l'impact sur Internet », https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

9 Internet Society, « Le mode de fonctionnement du réseau Internet » ; Défendre un Internet prospère pour tous », https://www.internetsociety.org/action-plan/2022/internet-way-of-networking/

Ce rapport a examiné les politiques gouvernementales de trois régions qui ont ouvertement défendu la
souveraineté numérique.[10]

Il n'existe pas de discours unique pour décrire les politiques de souveraineté
numérique dans les régions ou dans le monde.

Cela reflète bien les différentes compréhensions et utilisations du terme, ainsi que les objectifs multiples et parfois contradictoires des politiques mises en place pour promouvoir la souveraineté numérique.

Pour notre analyse, nous avons sélectionné des lois nationales, des propositions de politique, des documents de stratégie et d'autres éléments liés aux affaires publiques qui[11] mentionnaient explicitement la souveraineté numérique, ou une variante de celle-ci, dans le discours politique, ou qui étaient présentés ou rendus publics d'une manière qui mettait le terme en évidence.Bien que nous ayons trouvé de nombreuses politiques dans le monde susceptibles de poursuivre la souveraineté numérique, ce rapport exclut les politiques qui ne la mentionnent pas clairement comme un objectif. Ainsi, on évite d'attribuer faussement la souveraineté numérique à une politique qui peut avoir d'autres motivations.

Les déclarations des gouvernements et les dispositions légales ont été prises au pied de la lettre, c'est-à-dire que nous les avons analysées sur la base de leurs objectifs déclarés.Vous trouverez à l'annexe I des informations plus détaillées sur les politiques et les propositions de chaque région.

2.1 Asie-Pacifique

Les principaux moteurs des mesures de souveraineté numérique dans les pays que nous avons couverts (Australie,
Chine, Inde et Viet Nam) sont la protection de la sécurité nationale, des citoyens et de la stabilité sociale,
ainsi que le protectionnisme économique pour soutenir l'industrie nationale. Parmi les autres

10 Alors que le discours public sur la souveraineté numérique est façonné par de multiples parties prenantes, y compris les universités et la société civile, ce rapport se concentre sur les politiques que les gouvernements eux-mêmes ont mises en place, avec l'intention et la proclamation explicites de renforcer leur souveraineté sur une multitude d'aspects concernant Internet

11 Pour être concis, nous utilisons le terme « politiques » afin d'englober toutes ces mesures et communications.

motivations, on peut citer la sauvegarde des normes et valeurs sociales et culturelles (telles que définies par l'État) et l'aide apportée aux personnes pour qu'elles contrôlent leurs données.

La Chine est un pionnier régional et mondial dans la définition, la mise en œuvre et l'exportation d'une approche de la souveraineté numérique centrée sur l'État, caractérisée par un plus grand contrôle de l'État sur Internet et la localisation des données. D'autres gouvernements comme le Viet Nam semblent être attirés par ce modèle et par les possibilités d'investissement accru dans les infrastructures publiques et l'économie qu'offre l'initiative chinoise « Ceinture et Route ».

La Chine a été l'un des premiers pays à formuler le concept de souveraineté numérique. En 2015, le président chinois, Xi Jinping, a défini la souveraineté numérique comme le droit de chaque État-nation de choisir sa propre voie de cyber-développement et son propre modèle de réglementation et de politiques Internet, sans l'ingérence d'autres pays.[12] Fait inhabituel, la loi chinoise sur la sécurité des données (2021), qui tend à préserver « la souveraineté, la sécurité et les intérêts de développement de l'État », a une portée extraterritoriale et attribue une responsabilité juridique aux entités qui violent les lois et les intérêts de la Chine par le traitement de données à l'étranger.[13]

La Chine a également mis en œuvre la souveraineté numérique par le biais de régimes de localisation des données.Son règlement de 2017 sur les noms de domaine Internet[14] soutiennent la tendance croissante en faveur de la localisation. Plus précisément, les règles qui exigent que les opérateurs de serveur racine et les registres et bureaux d'enregistrement de noms de domaine, soient basés dans le pays.[15]

Le contrôle de l'État est également considéré comme un moyen de stimuler l'économie numérique nationale et d'accorder un traitement préférentiel aux entreprises chinoises.[16]

---

12 Ministère des Affaires étrangères de la République populaire de Chine, « Remarques de S.E. Xi Jinping, président de la République populaire de Chine, lors de la cérémonie d'ouverture de la deuxième Conférence mondiale sur Internet », 16 décembre 2015, https://www.fmprc.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html.

13 L'Assemblée populaire nationale de la République populaire de Chine, « Loi sur la sécurité des données de la République populaire de Chine », 10 juin 2021, http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml.

14 Centre d'information sur le réseau Internet de Chine, « Réglementation sur les noms de domaine Internet », 26 octobre 2017, https://www.cnnic.com.cn/PublicS/fwzxxgzcfg/201710/t20171026_69608.htm.

15 Rogier Creemers, « L'approche chinoise de la cybersouveraineté », Konrad-Adenauer-Stiftung, 2020, https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537.

16 Jane Li, « Pékin dispose d'une nouvelle architecture juridique pour un contrôle étendu sur les données des utilisateurs », Quartz, 30 août 2021, https://qz.com/2051268/china-aims-to-control-but-also-unleash-the-economic-power-of-data/; et Rogier Creemers, « L'approche chinoise de la cybersouveraineté », Konrad-Adenauer-Stiftung, 2020, https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537.

La stratégie australienne de cybersécurité de 2020 aspire à stimuler « les nouvelles compétences et entreprises australiennes souveraines en matière de cybersécurité » et à « promouvoir l'innovation dans la recherche et[17] le développement [18]en matière de cybersécurité souveraine ». Cependant, il s'agit dans l'ensemble d'un effort visant à équilibrer les intérêts de sécurité nationale avec un programme commercial libéralisé. Toutefois, l'Australie n'a pas encore exigé la localisation des données. Sa stratégie nationale d'hébergement ne préconise pas la propriété et le contrôle nationaux, ni la localisation des données gouvernementales. Elle a récemment été modifiée pour permettre aux entreprises non australiennes de se qualifier.[19]

L'Inde, quant à elle, souhaite accroître le pouvoir de l'État et l'accès aux données, mais se base davantage sur des intérêts économiques que sur des intérêts purement sécuritaires. Son projet de loi sur la localisation des données a récemment été mis au placard, et l'approche du gouvernement est globalement conçue pour protéger les infrastructures et les données critiques à la suite de violations de données, et pour renforcer la capacité d'hébergement et l'économie numérique.

2.2 Afrique

Le concept de souveraineté numérique en Afrique est relativement récent. Il a gagné en importance et en popularité
au cours des cinq dernières années.

Le discours sur la souveraineté numérique est marqué par l'histoire coloniale de l'Afrique
, dans le contexte de l'inégale répartition
des richesses et du pouvoir.

Les espaces numériques de nombreux pays africains restent largement dépendants des entreprises étrangères (principalement occidentales, mais aussi chinoises depuis peu) et les pays

17 L'Australie envisage un régime de localisation des données. Voir Justin Hendry. « Les géants de la technologie se mobilisent contre la localisation des données en Australie », InnovationAus.com, 7 septembre 2022.https://www.innovationaus.com/tech-giants-rally-against-data-localisation-in-australia/

18 Gouvernement australien, « La stratégie 2020 de la cybersécurité australienne », https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

19 Joseph Brookes, « Certified Strategic data centres double » (Le doublement des centres de données stratégiques certifiés), InnovationAus.com, 20 août 2021, https://www.innovationaus.com/certified-strategic-data-centres-double/.

africains ont peu de contrôle sur les données et l'infrastructure dont ils dépendent, et n'en tirent pas les bénéfices économiques escomptés.[20]

La souveraineté numérique, telle qu'elle est utilisée par les gouvernements africains, est généralement présentée comme une extension de la souveraineté nationale et s'enracine dans la conception politique de la souveraineté promue par la Chine.[21] Il existe relativement peu de cadres politiques et réglementaires ou de décisions sur la souveraineté numérique dans les cinquante-quatre pays africains, et jusqu'à présent, l'idée tend à être articulée par des déclarations politiques. Les politiques qui existent, telles que la Stratégie de transformation numérique pour l'Afrique de l'Union africaine, le projet de politique sur les données et le cloud[22] de l'Afrique du Sud et la politique sur la révolution des données[23] du Rwanda, mettent l'accent sur l'autodétermination économique en garantissant la propriété et le contrôle locaux des données générées localement.

On observe une tendance croissante à reproduire le modèle chinois de gouvernance des données, qui exige que tous les serveurs soient situés à l'intérieur des frontières d'un pays, afin que l'État puisse accéder plus facilement aux informations. Les gouvernements du Nigéria et du Sénégal associent de plus en plus la souveraineté numérique à la protection ou au renforcement du rôle de l'État. Les gouvernements cherchent également à répondre à leurs propres préoccupations concernant le contrôle politique et les avantages économiques de l'Internet qui sort de leur pays.

2.3 Europe, y compris la Russie

La région européenne abrite l'Union européenne (UE) et la Fédération de Russie, deux grandes puissances qui ont des visions distinctes de l'avenir d'Internet. Les pays ou entités analysés exercent une influence internationale et ont formulé et mis en œuvre une vision de la souveraineté numérique. Deux camps principaux ont été identifiés dans la région.

20 David Monyae, Centre d'études Afrique-Chine de l'Université de Johannesburg, « La souveraineté numérique de l'Afrique, un débat opportun et pertinent », 28 septembre 2021 https://www.uj.ac.za/news/africas-digital-sovereignty-a-timely-and-relevant-debate/

21 Monyae, 2021

21 Union africaine, « La stratégie de transformation numérique pour l'Afrique (2020-2030) »

22 Gouvernement sud-africain, Département des communications et des technologies numériques, « Invitation à soumettre des observations écrites sur la proposition de politique nationale en matière de données et de cloud », https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

23 « La révolution des données nationales au Rwanda et le Big data », 2017 http://statistics.gov.rw/publication/rwanda-national-data-revolution-and-big-data

Le premier camp (l'UE et ses États membres, comme la France, l'Allemagne et l'Italie) conçoit la souveraineté numérique principalement dans le contexte de la compétitivité économique, du développement de l'industrie locale et de la protection contre les cyberattaques.

> La souveraineté économique peut impliquer de réduire les dépendances de la chaîne d'approvisionnement afin que les infrastructures clés ne soient pas trop dépendantes de fournisseurs étrangers, et d'encourager le développement d'alternatives aux entreprises non européennes actuellement dominantes.

Dans une moindre mesure, certaines politiques cherchent à renforcer la souveraineté de l'individu sur ses données. La Loi sur les services numériques[24] et la Loi européenne sur les données[25] visent à donner aux entreprises et aux particuliers plus de choix en matière de services et de contrôle sur les données générées par les utilisateurs, en s'appuyant sur des mesures réglementaires.

Si ces encadrements ont tendance à être initiés par les gouvernements, ils ne placent pas exclusivement l'autorité étatique au centre. Les politiques qu'ils mettent en œuvre impliquent des rôles accrus pour les organismes de réglementation mais ont pour objectif déclaré de responsabiliser les entreprises ou les particuliers.

Le deuxième camp dans cette région (la Fédération de Russie en est l'exemple le plus frappant) assimile la souveraineté numérique à un contrôle accru de l'État sur le domaine numérique et les informations qui y transitent, notamment les données qui circulent à l'intérieur du pays.

La Fédération de Russie ne fait pas couramment référence à la « souveraineté numérique » dans ses documents politiques, mais le fait dans les communiqués de presse et les déclarations publiques du gouvernement. Un règlement de 2019, officieusement appelé « Loi pour un Internet souverain », vise à garantir la continuité du lien Internet en cas d'attaque des infrastructures par des acteurs étrangers.[26]

---

24 Commission européenne, « La loi sur les services numériques : garantir un environnement en ligne sûr et responsable », https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

25 Commission européenne, « Loi sur les données », https://digital-strategy.ec.europa.eu/en/policies/data-act

26 'Федеральный закон от 01.05.2019 № 90-ФЗ "О внесении изменений в Федеральный закон "О связи" и Федеральный закон "Об информации, информационных технологиях и о защите информации"', http://publication.pravo.gov.ru/Document/View/0001201905010025

III. Objectifs et résultats : Approches de la souveraineté numérique

Les politiques et mesures couvertes par ce rapport sont explicitement motivées par la souveraineté numérique, mais elles varient dans les objectifs officiellement déclarés et peuvent permettre à différents acteurs, parfois non étatiques, d'atteindre leurs objectifs.

3.1 Les quatre objectifs principaux des politiques

1. **La sécurité nationale et la capacité à faire appliquer les lois :** Ces politiques traitent des menaces pour la **sécurité nationale**, notamment les cyberattaques étrangères et les vulnérabilités en ligne. Grâce à elles, l'État entend sécuriser le domaine numérique à l'intérieur de ses frontières. Elles peuvent couvrir la cybersécurité des infrastructures critiques jusqu'à l'utilisation des technologies Internet dans les processus et les changements politiques. De nombreux gouvernements ont rencontré des difficultés à exercer leur autorité sur les biens et services numériques opérant ou mis à disposition localement et souhaitent réaffirmer leur **capacité à établir et à faire appliquer des lois** sur leur territoire. Cela caractérise généralement les politiques qui permettent un accès légal à l'information par les organismes chargés de l'application de la loi, les autorités en charge de la concurrence et d'autres organismes de réglementation. Au-delà du contrôle des données générées localement, cette autorité peut s'étendre à la manière dont les services et les logiciels fonctionnent dans un contexte national spécifique.
2. **L'autodétermination économique** : Ces politiques renforcent le développement de l'industrie locale en créant davantage de possibilités de concurrence pour les entreprises nationales, souvent dans un environnement considéré comme dominé par les entreprises technologiques des États-Unis et, de plus en plus, dans certains pays, de la Chine.[27] Certaines politiques tentent d'atteindre cet objectif par des mesures protectionnistes strictes, tandis que d'autres renforcent les forces du marché pour créer des conditions de concurrence plus équitables.
3. **Protection des droits et responsabilisation des citoyens/utilisateurs et des communautés :** Ces politiques renforcent l'autonomie individuelle et collective vis-à-vis des plateformes technologiques avec lesquelles ils interagissent, notamment en donnant aux citoyens et aux communautés la possibilité d'agir et de prendre des décisions concernant leurs données et leurs activités numériques.

27 Julia Pohle et Thorstein Thiel. Souveraineté numérique. Examen de la politique Internet, 9(4), 5 décembre 2020. https://doi.org/10.14763/2020.4.1532]

4. **Maintien des normes et valeurs sociétales :** Ces politiques préservent les normes et traditions locales, ou celles qu'un gouvernement souhaite encourager, face à l'afflux de technologies, de normes et de services qui sont considérés comme incarnant ou promouvant d'autres valeurs sociales, culturelles et politiques. Cet objectif est souvent secondaire par rapport aux autres. Autrement dit, il est rarement l'objectif dominant.

Les politiques ont souvent plusieurs objectifs qui se recoupent : une politique de localisation des données peut affirmer les droits des citoyens sur leurs données tout en empêchant ces données d'être stockées à l'étranger pour des raisons de sécurité. Les politiques peuvent également avoir des objectifs implicites. La localisation des données peut également permettre aux services de renseignement et aux organismes de maintien de l'ordre d'accéder plus facilement aux données des citoyens, ou de générer des activités pour les centres de données locaux.

3.2 Acteurs habilités à atteindre les objectifs des politiques

Des politiques ayant des objectifs similaires peuvent avoir des effets différents sur Internet, selon les personnes qui sont habilitées à les réaliser. Il peut s'agir (1) de l'État, en renforçant l'autorité de ses institutions ; (2) des acteurs économiques, en favorisant un environnement équitable et concurrentiel pour les entreprises ; et/ou (3) des citoyens, en élargissant leurs droits et leurs privilèges, et en s'appuyant sur la réglementation pour affirmer leur volonté.

Ces objectifs et acteurs habilités ne sont pas exhaustifs, car ils ont été tirés de politiques étudiées dans trois régions seulement. Nous sommes conscients que de nouvelles politiques en matière de souveraineté numérique voient le jour dans le monde entier, et nous proposons que le cadre analytique présenté ici puisse s'appliquer à d'autres politiques sur cette question, dans les régions que nous avons étudiées et dans d'autres.

IV. Approches communes de la souveraineté numérique et leur impact sur Internet

La plupart des pays ont un mélange d'objectifs politiques et d'entités habilitées, mais après avoir évalué 34 politiques, deux approches distinctes de la souveraineté numérique ont émergé au-dessus des autres :

(1) **La sécurité nationale motivée par un contrôle accru de l'État** et
(2) **L'autodétermination économique motivée par les acteurs économiques**

Plusieurs politiques visaient à accroître la souveraineté des individus et/ou des communautés, principalement en donnant aux citoyens et/ou aux groupes culturels plus de contrôle sur leurs données personnelles, mais les exemples de mise en œuvre de ces politiques n'étaient pas assez nombreux pour mériter une troisième distinction. Pour de plus amples informations sur la méthodologie et les politiques incluses dans l'analyse, voir les annexes III et IV.

Pour analyser si et comment la souveraineté numérique affecte l'Internet, nous utilisons la Boîte à outils pour l'évaluation de l'impact sur Internet,[28] un cadre qui décrit les conditions dont Internet a besoin pour exister et prospérer en tant que bien public. Nous évaluons chaque type de politique par rapport à chaque propriété critique du « Mode de fonctionnement du réseau Internet »[29] et aux instruments[30] qui sous-tendent un Internet ouvert, mondialement connecté, sécurisé et digne de confiance. Ces deux éléments sont présentés de manière plus détaillée à l'annexe II.

Des facteurs tels que le système politique, l'État de droit, les mises en œuvre techniques antérieures ou la protection des libertés civiles peuvent influencer l'effet d'une politique mais ne sont pas pris en compte dans cette analyse.

4.1 Approche 1 : La sécurité nationale assurée par un contrôle accru de l'État

Objectif : La sécurité nationale et, dans une moindre mesure, la capacité à faire respecter les lois dans le monde numérique
Entité habilitée : l'État
Juridictions concernées : Australie, Chine, Nigéria, Russie, Viet Nam
Cette approche se caractérise par des politiques de sécurité nationale qui cherchent à renforcer l'autorité de l'État sur son territoire et sa capacité à faire appliquer ses lois dans le domaine numérique. Elle met fortement l'accent sur le rôle de l'État dans sa mise en œuvre, et accroît invariablement le pouvoir, et souvent la capacité, de l'État à avoir un impact sur Internet.[31]

28 Internet Society, « Boîte à outils pour l'évaluation de l'impact sur Internet », https://www.internetsociety.org/issues/internet-way-of-networking/internet-impact-assessment-toolkit/

29 Internet Society, « Le mode de fonctionnement du réseau Internet », « Propriétés critiques », https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet/

30 Internet Society, « Facilitateurs d'un Internet ouvert, globalement connecté, sécurisé et digne de confiance », https://www.internetsociety.org/resources/doc/2021/enablers-of-open-globally-connected-secure-trustworthy-internet/

31 Plusieurs politiques ont exprimé le désir de limiter la désinformation et la mésinformation pour favoriser une société plus cohésive. Celles-ci ont parfois été interprétées comme des efforts pour contrôler le flux d'informations à l'intérieur des frontières d'un pays. Ce rapport s'abstient d'adopter ces interprétations pour éviter les suppositions, en se concentrant strictement sur les objectifs déclarés des politiques.

Impact sur le mode de fonctionnement du réseau Internet

La centralisation du contrôle des infrastructures est la conséquence la plus courante et la plus préoccupante des politiques de sécurité nationale sur Internet. Celles-ci cherchent généralement à ce que l'État contrôle les principales infrastructures de mise en réseau (telles que le nommage et l'adressage) qui sont décentralisées et distribuées sur Internet. Ces politiques renforcent souvent l'autorité de l'État pour diriger les opérations de réseau, et dans certains cas, même pour les gérer.

On peut citer à titre d'exemple les « Règles de gestion centralisée d'un réseau de communication public » de la Russie, qui font partie de la législation connue sous le nom de « Loi pour un Internet souverain » et qui tendent à imposer un contrôle accru des flux de trafic à l'intérieur du pays. En déléguant des pouvoirs à l'agence fédérale Roskomnadzor, ces règles imposent l'installation de serveurs intermédiaires pour filtrer et surveiller le trafic sur les réseaux russes. Cela interfère directement avec la capacité des opérateurs de réseaux russes à gérer leurs propres réseaux, en les obligeant à se conformer aux exigences de la politique de routage de Roskomnadzor.

On trouve des dispositions similaires dans la « Loi sur la cybersécurité » du Viet Nam, qui délègue des pouvoirs importants à l'Autorité de cybersécurité pour restreindre et suspendre les opérations du réseau, y compris en filtrant les informations considérées comme susceptibles de perturber la sécurité ou de troubler l'ordre public.

La centralisation s'étend à d'autres fonctions techniques. En Inde, les « directives de cybersécurité du CERT-in » étendent le contrôle de l'État à la coordination de l'heure du réseau, en exigeant que toutes les entités et tous les serveurs se connectent aux serveurs NTP (Network Time Protocol) du gouvernement.[32] Ces lois interfèrent avec le fonctionnement distribué du routage (via le Border Gateway Protocol, ou BGP) et de la résolution de noms (via le Domain Name System, ou DNS).

Certaines politiques **restreignent le déploiement volontaire de certaines technologies et de certains protocoles d'infrastructure**, ce qui peut nuire gravement à l'interopérabilité. Par exemple, les lois chinoises et vietnamiennes sur la cybersécurité exigent que des intermédiaires de l'Internet surveillent le contenu. Cela les empêche d'utiliser des modules de sécurité développés par la communauté et largement adoptés (par exemple, Transport Layer Security,

32 Internet Society, « Dossier d'impact sur Internet : Inde Directives de cybersécurité 2022 CERT-In », https://www.internetsociety.org/resources/doc/2022/internet-impact-brief-india-cert-in-cybersecurity-directions-2022/

ou TLS 1.3) et d'autres pratiques exemplaires qui reposent sur le cryptage.Pour suivre ou analyser les contenus, les intermédiaires de l'infrastructure peuvent être amenés à se spécialiser et à adapter leurs services à des types de contenus spécifiques, **ce qui nuit considérablement à la nature technologiquement neutre et polyvalente d'Internet**.

Souvent, les politiques de souveraineté numérique en matière de sécurité nationale perturbent directement les opérations sur Internet. Elles présentent des risques importants pour l'Internet mondial en provoquant une fragmentation du réseau **en raison de l'interférence avec l'ensemble partagé d'identifiants de l'Internet**. Par exemple, les documents d'accompagnement de la Loi russe pour un Internet souverain imposent l'utilisation de modules de résolution de DNS contrôlés par le gouvernement. En exigeant des opérateurs russes qu'ils n'utilisent que ces modules de résolution de DNS, le gouvernement pourra modifier unilatéralement la résolution des noms en Russie[33] et créer potentiellement une alternative russe au DNS mondial.

En résumé, les politiques de souveraineté numérique en matière de sécurité nationale peuvent avoir de graves répercussions sur
le modèle de mise en réseau d'Internet et nuire considérablement à cette
plateforme ouverte et mondialement connectée.

Impact sur l'Internet ouvert, mondialement connecté, sécurisé et digne de confiance

En plus de porter atteinte aux attributs qui permettent à Internet de fonctionner correctement, ces politiques peuvent également affecter les facteurs plus généraux d'un Internet ouvert, mondialement connecté, sécurisé et digne de confiance. L'une des pertes les plus évidentes est la **fiabilité** d'Internet, qui diminue avec l'interférence sur les fonctions de base comme le nommage et l'adressage. Si l'augmentation unilatérale du contrôle de l'État ne s'accompagne pas d'une transparence dans la prise de décision, elle peut également dégrader la **responsabilité** dans l'environnement en ligne. Si les lois peuvent être complétées par une documentation plus détaillée sur les mesures de responsabilisation, nous n'avons pas été en mesure d'en trouver dans les politiques que nous avons étudiées.

Le dénominateur commun de toutes les politiques de cette nature est le nombre d'activités vaguement définies qui relèvent de l'autorité élargie de l'État, avec peu de contrôles ou de conditions sur la façon dont ces pouvoirs sont exercés. Les directives de cybersécurité révisées du CERT-In[34] indien transforment le rôle du CERT-In, qui passe d'une entité faisant autorité dans

33 Принят закон о «суверенном интернете»', http://duma.gov.ru/news/44551/

34 CERT-In Ministère indien de l'électronique et des technologies de l'information (MeitY) Équipe indienne d'intervention d'urgence informatique (CERT-In), 2022. https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

un système de collaboration volontaire et de partage d'informations, à un quasi organisme de réglementation, voire à une agence d'application de la loi.

Les techniques de filtrage et de suivi réduisent la **confidentialité et l'intégrité des informations.** La Russie, par exemple, impose des équipements d'interception pour analyser et filtrer les contenus.[35] Ces équipements, ainsi que les exigences extrêmement larges en matière de conservation des données en Inde et la vérification des données personnelles au Viet Nam, menacent gravement la confidentialité des utilisateurs. L'exigence de la Chine selon laquelle les services doivent obtenir le consentement des utilisateurs lorsqu'ils collectent des informations personnelles pourrait améliorer la **confidentialité** des utilisateurs, mais elle est fortement contrebalancée par les obligations de surveillance de masse et de signalement du « comportement inacceptable » des utilisateurs et de la transmission d'« informations interdites ».

Le contrôle centralisé des fonctions clés et l'application de moyens techniques pour intercepter et surveiller le trafic diminuent également la **résilience, la disponibilité et la fiabilité** des services en réseau. La proposition indienne de sécurité de synchronisation (NTP) risque de créer un point de défaillance unique préjudiciable à tous les services du pays, y compris aux technologies de cryptage qui dépendent de cette fonction. L'utilisation par la Russie d'équipements d'écoute du réseau peut provoquer des pannes importantes sur le réseau à une plus grande échelle si ces dispositifs et leurs logiciels associés fonctionnent mal. En effet, ce type de panne a déjà été signalé[36] et la loi elle-même reconnaît ce risque en permettant de contourner l'équipement en cas de dysfonctionnement.

Les politiques analysées sont globalement préjudiciables à un Internet ouvert et mondialement connecté. La **collaboration** entre les parties prenantes, qui a été la norme en matière de gouvernance et de fonctionnement de l'Internet, est supplantée par un contrôle étatique centralisé, qui compromet les avantages importants offerts par le modèle de mise en réseau. Les politiques visant à restreindre et à diriger l'**accessibilité** du réseau, notamment en interférant avec les décisions de DNS et de routage, limitent les ressources disponibles pour les utilisateurs aux seules ressources autorisées par le gouvernement. Il y a également des conséquences indirectes : les nouvelles exigences opérationnelles et l'augmentation des coûts de mise en conformité créent des obstacles pour les opérateurs de réseaux et les intermédiaires, ce qui limite finalement la **facilité d'accès** à Internet.

35 Une introduction de dix minutes aux boîtiers intermédiaires http://yuba.stanford.edu/~huangty/sigcomm15_preview/mbpreview.pdf

36 '«Суверенный интернет» засбоил. Проблемы с оборудованием привели к системным сбоям', 2021, https://kapital-rus.ru/articles/article/suverennyi_internet_zasboil_problemy_s_oborudovaniem_priveli_k_sistemnym_sb/

4.2 Approche 2 : L'autodétermination économique pilotée par les acteurs économiques

Objectif : Autodétermination économique, c'est-à-dire renforcer les acteurs de l'économie nationale et assurer la résilience de la chaîne d'approvisionnement
Entité habilitée : Acteurs économiques, généralement des entreprises
Juridictions concernées : Afrique du Sud, Inde, Rwanda, UE

Cette approche se caractérise par des politiques qui affirment l'autodétermination économique en renforçant l'économie nationale. Elle vise à réduire la domination et la dépendance à l'égard des fournisseurs de technologies et de services étrangers en (1) créant davantage d'opportunités de concurrence pour les entreprises locales, parfois avec un certain degré de protectionnisme, et (2) en cultivant la résilience de la chaîne d'approvisionnement pour le secteur numérique local.Si ces politiques ont souvent cherché à étendre l'autorité de l'État, par exemple en élargissant les attributions des organismes de réglementation de la concurrence, elles ont également cherché à donner du pouvoir aux acteurs de l'économie au sens large.

Impact sur le mode de fonctionnement du réseau Internet

Les politiques à caractère économique que nous avons analysées n'interfèrent pas directement avec les opérations du réseau d'Internet. Conscientes des opportunités créées par un réseau mondial et des sociétés connectées, ces politiques cherchent le plus souvent à améliorer les conditions qui permettent aux acteurs locaux de tirer parti d'internet.

Dans de nombreux cas, elles visent explicitement à renforcer des caractéristiques importantes du modèle de mise en réseau. Par exemple, la « Stratégie de transformation numérique pour l'Afrique (2020-2030) » de l'Union africaine encourage les approches technologiquement neutres pour l'interopérabilité transfrontalière. Dans le même esprit, la politique indienne en matière de centres de données préconise l'adoption volontaire des normes mondiales établies.

À première vue, les politiques analysées soutiennent l'Internet ouvert et mondial comme un atout à soutenir et à exploiter pour le progrès économique régional et national.

Impact sur l'Internet ouvert, mondialement connecté, sécurisé et digne de confiance

Les politiques de souveraineté numérique visant à l'autodétermination économique soutiennent en grande partie les éléments moteurs d'un Internet ouvert, mondialement connecté, sécurisé

et digne de confiance. **L'accès et la réduction des barrières à l'entrée** sont considérés comme essentiels pour qu'Internet soit synonyme d'opportunités. La « Stratégie de transformation numérique pour l'Afrique (2020 - 2030) » de l'Union africaine vise à rendre les appareils et les services plus abordables, en soulignant le rôle des gouvernements dans le développement des infrastructures pour élargir l'accès et les **capacités**. Cela inclut des points d'interconnexion Internet (IXP) pour améliorer l'interconnexion et l'échange de trafic, ainsi qu'un environnement réglementaire qui soutient de manière proactive les solutions d'accès telles que les réseaux communautaires.[37] Au-delà du déploiement de l'infrastructure, la loi européenne sur les données vise à réduire les obstacles « juridiques, économiques et techniques » à l'accès aux données, notamment en exigeant des fournisseurs qu'ils disposent d'outils techniques permettant aux utilisateurs de contrôler la manière dont leurs données sont partagées avec des tiers. La Commission européenne affirme que le fait de mettre davantage de données à disposition pour être réutilisées ajoutera 270 milliards d'euros au PIB de la région d'ici 2028.[38]

Toutefois, ces politiques peuvent également limiter la flexibilité du **déploiement technique**. Par exemple, la politique indienne en matière de centres de données favorise le matériel et les logiciels indigènes afin de réduire les importations globales du pays. Une application stricte peut limiter l'utilisation de technologies potentiellement plus rentables et plus adaptées, mais non indiennes. De même, le mandat de normes spécifiques de la loi européenne sur les données, destiné à encourager une plus grande interopérabilité, peut empêcher les entreprises de développer des technologies innovantes.

Néanmoins, ces politiques reconnaissent que le choix et la disponibilité des technologies font partie intégrante d'un environnement numérique **fiable et résilient**.

Qu'il s'agisse de l'Inde, qui encourage la fiabilité de l'approvisionnement en électricité des centres de données, de l'UE, qui renforce l'approvisionnement en composants numériques, ou de l'Union africaine, qui soutient la sécurité du routage pour renforcer la sécurité numérique, de nombreuses politiques favorisent la résilience de la

37 Plan d'action 2022 de l'Internet Society, dernière modification le 6 septembre 2022.https://www.internetsociety.org/action-plan/2022/community-networks/

38 « Loi sur les données : la Commission propose des mesures pour une économie des données équitable et innovante », 23 février 2022.https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

chaîne d'approvisionnement
en tant qu'aspect essentiel de la souveraineté numérique économique.

Contrairement aux politiques de sécurité nationale, ces mesures à vocation économique préservent la **confidentialité et l'intégrité** des informations, par exemple en renforçant le cryptage. Dans la Stratégie de transformation numérique de l'Union africaine, cet accent est allé de pair avec le renforcement du contrôle des données personnelles par les utilisateurs et d'autres améliorations en matière de **confidentialité**.

4.3 Autres approches de la souveraineté numérique

Une troisième approche consiste à aligner la souveraineté numérique avec la souveraineté individuelle et/ou collective. Cela se manifeste par des mesures visant à renforcer les droits des individus et/ou des communautés en ce qui concerne les données les concernant ou créées par eux. Dans ses orientations sur la souveraineté des données[39], le gouvernement néo-zélandais appelle les institutions à choisir des services de cloud qui respectent les droits des données des Māori autochtones. Il soutient la Charte de souveraineté sur les données des Māori,[40] qui préconise un plus grand accès des Māori aux données recueillies à leur sujet par d'autres entités, ainsi que la propriété de ces données, et qui donne aux Māori le pouvoir de gouverner leurs données selon leurs coutumes et leurs priorités.[41]

Parallèlement, la Loi européenne sur les données rend les données disponibles dans différents secteurs de l'économie en donnant aux propriétaires de données, particuliers et entreprises, un plus grand contrôle sur la manière dont leurs données sont partagées avec des tiers. Cette approche est très proche du concept de « souveraineté individuelle », l'autorité étant décentralisée et déléguée aux entités propriétaires des données, conformément au principe de subsidiarité qui veut que les décisions soient prises aussi près que possible de l'endroit où elles ont un impact...

Cette approche s'éloigne du
concept classique de souveraineté, centré sur l'État et le territoire[42], et

39 Gouvernement numérique néo-zélandais. « Souveraineté sur les données. »https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/help/data-sovereignty/

40 « Charte maorie sur la souveraineté des données ». https://static1.squarespace.com/static/58e9b10f9de4bb8d1fb5ebbc/t/5913020d15cf7dde1df34482/1494417935052/Te+Mana+Raraunga+Charter+%28Final+%26+Approved%29.pdf

41 « Principes de la souveraineté des données maories. » Octobre 2018.https://cdn.auckland.ac.nz/assets/psych/about/our-research/documents/TMR%2BM%C4%81ori%2BData%2BSovereignty%2BPrinciples%2BOct%2B2018.pdf

42 Julia Pohle et Thorstein Thiel. Souveraineté numérique. Examen de la politique Internet, 5 décembre 2020.https://doi.org/10.14763/2020.4.1532]

vise à donner aux individus les moyens d'agir et de décider de manière consciente, délibérée et indépendante.

De cette façon, la Loi sur les données facilite la disponibilité, la portabilité et l'utilisation des données, mais en créant des barrières à l'entrée pour les technologies non européennes. En clarifiant les rôles et les responsabilités des entités de la chaîne de valeur, elle simplifie la responsabilisation, et renforce ainsi la fiabilité d'Internet. Mais la Loi sur les données contient également des dispositions plus communément associées à la souveraineté traditionnelle des États, telles que des restrictions au transfert international de données ou des mandats potentiels en matière d'interopérabilité et de normes spécifiques. Ces dispositions peuvent avoir un impact négatif non seulement sur les facilitateurs d'Internet, mais aussi sur le mode de mise en réseau d'Internet.[43]

Enfin, une quatrième approche se concentre sur la sauvegarde des normes et valeurs culturelles. Cet objectif est souvent combiné à d'autres, tels que la sécurité nationale ou l'autodétermination économique, et n'occupe pas une place importante dans les politiques de souveraineté numérique.

V. Conclusion

En tant que réseau mondial de réseaux, Internet ne se conforme pas à la notion de frontières nationales. Les réseaux peuvent fonctionner dans certaines juridictions, mais leur topologie et leurs points d'interconnexion sont définis par l'objectif d'optimiser le trafic, plutôt que de suivre une carte politique. Les règles d'interconnexion ne sont pas définies par des traités mais reposent sur des processus volontaires qui fonctionnent bien et sur la collaboration entre les réseaux.

C'est dans ce contexte que l'on retrouve la notion de souveraineté, antérieure à Internet, de plus en plus appliquée au domaine numérique. Les politiques de souveraineté numérique poursuivent des objectifs variés, allant du maintien des données à l'intérieur des frontières nationales à l'exploitation de la technologie pour stimuler le développement indigène, et leurs effets sur Internet peuvent être minimes ou nuls, potentiellement risqués ou directement préjudiciables, au risque de fragmenter l'Internet mondial.

43 Une autre politique souvent associée à un contrôle accru des données personnelles est le règlement général sur la protection des données (RGPD) de l'UE. Si le RGPD fait effectivement écho aux sentiments de souveraineté individuelle, il a été exclu du champ de cet article car le texte du règlement ne fait pas référence à la souveraineté numérique et le règlement est antérieur à l'utilisation du terme dans les documents de stratégie de l'UE.

Le concept de souveraineté numérique lui-même reste vague et décousu, d'où la difficulté de généraliser son impact. Pour mieux comprendre ses nombreuses facettes, ce rapport s'est concentré sur la manière dont la souveraineté numérique est appliquée dans les affaires publiques. En évaluant plusieurs dizaines de politiques publiques dans différents pays d'Asie-Pacifique, d'Europe et d'Afrique, nous avons déterminé comment les diverses approches gouvernementales de la souveraineté numérique peuvent avoir un effet différent sur Internet.

Les politiques qui visent à renforcer la sécurité nationale par une autorité étatique accrue concentrent le contrôle sur le gouvernement et limitent excessivement l'autonomie des réseaux. Ces mesures risquent d'endommager Internet en imposant des exigences techniques spécifiques et en s'appuyant sur un modèle de « commande et contrôle », plutôt que sur la collaboration et la coordination entre pairs. Certaines politiques contrarient directement les propriétés critiques qui permettent à Internet de fonctionner correctement, telles que sa gestion décentralisée et son utilisation d'identifiants mondiaux (nommage et adressage). Les efforts qui modifient fondamentalement le fonctionnement d'Internet limitent la valeur que nous pouvons tirer de celui-ci en tant que ressource ouverte et mondialement connectée.

Les politiques qui visent l'autodétermination économique en donnant des moyens d'action aux acteurs économiques ont tendance à se concentrer sur la stimulation des économies numériques locales en uniformisant les règles du jeu et en réduisant les obstacles à l'entrée en rendant les ressources (telles que les données) plus accessibles. Ces politiques tendent à être mieux alignées sur le fonctionnement d'Internet, car elles ne sont pas en contradiction avec ses propriétés et ses outils. Cependant, certaines des mesures traitées dans ce rapport comportent des éléments significatifs de protectionnisme, par exemple en limitant la disponibilité et le choix des produits et services. Mais dans l'ensemble, ces politiques ne peuvent causer que des dommages minimes, et dans certains cas, elles peuvent même améliorer et renforcer l'utilité d'Internet.

Une approche émergente, moins courante, que l'on retrouve dans la loi européenne sur les données et dans les lignes directrices de la Nouvelle-Zélande sur la souveraineté des données, évoque la souveraineté de l'individu et de communautés distinctes, en particulier leur capacité d'agir et de décider par eux-mêmes pour ce qui est de leur présence numérique. Cette orientation semble plus conforme au fonctionnement d'Internet et à ses principes : gestion décentralisée des réseaux, utilisation libre des technologies, accessibilité sans restriction, transparence et responsabilité dans l'utilisation des ressources d'Internet. Bien que les exemples de cette approche soient limités, elle représente une vision de la souveraineté centrée sur l'utilisateur dans le monde numérique.

En général, les stratégies de souveraineté numérique comportent un mélange d'approches, bien qu'une ou deux dominent habituellement. En distillant les objectifs politiques dominants, nous

avons pu évaluer l'impact qu'une approche spécifique de la souveraineté numérique peut avoir sur les fondements d'Internet.

La souveraineté numérique est un concept en pleine expansion, et la notion seule ne nous dit pas grand-chose sur la façon dont elle peut remodeler l'environnement en ligne. En fin de compte, ce sont les politiques qui en résultent et les acteurs qu'elles centrent et habilitent qui définissent l'impact de la souveraineté numérique sur Internet.

Comme tout écosystème vivant, Internet est en perpétuelle évolution. Cette évolution continue, sans plan ni autorité centralisés, est à la base de sa valeur pour le monde. Mais comme Internet a fini par imprégner la plupart de nos vies, les gouvernements et les entreprises prennent de plus en plus de décisions qui ont un impact sur lui.

Chaque nouvelle politique proposée au nom de la souveraineté numérique doit être évaluée afin de s'assurer qu'elle ne porte pas atteinte aux éléments qui rendent Internet utile pour nous, et qu'elle ne nous rapproche pas d'une série de réseaux fragmentés et fermés où les opportunités qui découlent de la connexion mondiale sont perdues.

Ce rapport montre comment cette évaluation peut être réalisée, à la fois sur les politiques que nous examinons ici et sur celles à venir.

Annexe I - Tendances régionales en matière de souveraineté numérique

A. Asie-Pacifique

La région Asie-Pacifique comprend les pays les plus peuplés du monde, comme la Chine et l'Inde, mais aussi certains des plus petits pays du monde. Les pays que nous avons examinés sont de grandes économies qui ont une influence géopolitique considérable dans la région et dans le monde. Ils ont rédigé ou adopté une ou plusieurs politiques, lois, règlements et/ou stratégies faisant référence à la souveraineté numérique ou à des termes similaires,[44] mais font preuve d'une grande diversité dans l'interprétation et la mise en œuvre de la souveraineté numérique.

44 Par exemple, le Vietnam utilise fréquemment le terme « souveraineté nationale dans le cyberespace ».

Australie - En Australie, les politiques axées sur la souveraineté numérique visent à améliorer la cybersécurité. Sa Stratégie de gouvernement numérique vise à protéger et à gérer les informations publiques avec « des contrôles appropriés en matière de confidentialité, de souveraineté et de sécurité »[45] et est soutenue par une Stratégie d'hébergement qui traite des « risques pour la souveraineté des données détenues dans les centres de données du gouvernement australien ».[46] De manière indirecte, ces stratégies encouragent la construction de centres de données nationaux.

Malgré l'absence d'exigences en matière de localisation forcée des données en Australie, de récents rapports officiels mettent en évidence des niveaux sans précédent d'ingérence étrangère visant à porter atteinte à la souveraineté nationale de l'Australie.[47] En réponse, les chercheurs ont demandé instamment davantage de mesures de souveraineté numérique pour protéger à la fois la sécurité nationale[48] et les intérêts économiques,[49] ainsi que des exigences de localisation des données pour les données gouvernementales.[50]

Chine – La Chine, étant l'un des premiers pays à avoir adopté le concept de souveraineté numérique, a eu le plus de temps pour concrétiser sa vision. Elle exerce son influence en définissant une approche spécifique de la souveraineté numérique dans la région et dans le monde.

Le point de vue de la Chine a façonné de nombreuses politiques et lois dans le pays, bien que ce ne soit pas toujours explicitement énoncée. L'objectif de maintenir la « souveraineté cybernétique ou Internet » se trouve dans la loi sur la cybersécurité (2017), la loi sur la sécurité des données (2021) et la stratégie internationale de coopération sur le cyberespace (2017). Grâce à de telles mesures et dans des récits politiques de haut niveau, la Chine considère la souveraineté numérique comme un moyen d'assurer la sécurité nationale, de protéger le pays

45 Agence de transformation numérique, gouvernement australien, « Stratégie gouvernementale numérique », 2021, https://www.dta.gov.au/sites/default/files/2021-12/Digital%20Government%20Strategy_web-ready_FA.pdf.

46 Agence de transformation numérique, gouvernement australien, « Stratégie d'hébergement pangouvernementale : aperçu », https://www.dta.gov.au/our-projects/hosting-strategy/overview.

47 Observateur indépendant de la législation sur la sécurité nationale, gouvernement australien, « Rapport annuel 2020-2021 », 2021, https://www.inslm.gov.au/sites/default/files/2022-01/inslm-annual-report_2020-21.pdf.

48 Andrew Mitchell, « Un cadre pour les données souveraines du gouvernement australien », Institut australien de politique stratégique, 11 août 2021, https://www.aspistrategist.org.au/a-sovereign-australian-government-data-framework/

49 Marcus Thompson, « Les actifs de l'Australie peuvent assurer la résilience numérique nationale », The Mandarin, 6 mai 2022, https://www.themandarin.com.au/188379-australias-own-assets-can-ensure-national-digital-resilience/.

50 Andrew D. Mitchell et Theodore Samlidis, « Services cloud et souveraineté numérique du gouvernement en Australie et au-delà », Revue internationale du droit et des technologies de l'information, janvier 2022, https://www.researchgate.net/publication/358197261_Cloud_services_and_government_digital_sovereignty_in_Australia_and_beyond.

contre les cybermenaces[51] et de construire l'économie numérique locale en accordant un traitement préférentiel aux entreprises chinoises.[52] [53]

Plusieurs lois affirment l'intention de la Chine de prendre des mesures extraterritoriales, telles que la mise sur liste noire des entreprises étrangères qui ne respectent pas ses réglementations. La loi sur la cybersécurité (2017) oblige les opérateurs de réseaux des secteurs critiques à stocker en Chine toutes les données qu'ils collectent ou produisent dans le pays. Les informations commerciales et les données sur les citoyens chinois recueillies en Chine doivent être conservées sur des serveurs nationaux et ne pas être transférées à l'étranger sans autorisation. Ces dispositions sont renforcées dans la loi sur la protection des informations personnelles (2021).[54]

Inde – Les mesures de souveraineté numérique pertinentes en Inde, limitées aux exigences de localisation des données et aux politiques qui font explicitement référence à ce terme, sont pour la plupart à l'état de projet. Ces politiques donnent la priorité aux infrastructures critiques et à la protection des données à la suite de violations de données et renforcent la capacité d'hébergement du pays. La souveraineté numérique est citée comme un élément moteur du projet de politique indienne sur les centres de données (2020)[55] qui, parallèlement aux objectifs de sécurité, aspire à réduire les dépendances dans la chaîne d'approvisionnement. Elle s'aligne sur la récente initiative « Atmanirbhar Bharat » (traduite grossièrement par une « Inde autonome et autosuffisante »), ayant pour but d'encourager le développement économique.

Vietnam – La souveraineté numérique, traduite par « souveraineté nationale dans le cyberespace », a été adoptée dans la loi vietnamienne sur la cybersécurité (2018). Il enhardit le ministère de la Sécurité publique à « prévenir et combattre l'utilisation du cyberespace pour porter atteinte à la souveraineté, à la sécurité et aux intérêts nationaux, à l'ordre social et à la sûreté. »[56] Cela comprend la lutte contre la désinformation et l'amélioration de la défense en

51 China.org.cn, « Texte intégral : Stratégie internationale de coopération sur le cyberespace », 7 mars, http://www.china.org.cn/chinese/2017-03/07/content_40424606_2.htm.

52 Jane Li, « Pékin dispose d'une nouvelle architecture juridique pour un contrôle étendu sur les données des utilisateurs », Quartz, 30 août 2021, https://qz.com/2051268/china-aims-to-control-but-also-unleash-the-economic-power-of-data/; et Rogier Creemers, « L'approche chinoise de la cybersouveraineté », Konrad-Adenauer-Stiftung, 2020, https://www.kas.de/documents/252038/7995358/China%E2%80%99s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606143361537.

53 L'Assemblée populaire nationale de la République populaire de Chine, « Loi sur la sécurité des données de la République populaire de Chine », 10 juin 2021, http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml.

54 Digi China, Université de Stanford, « Traduction : Loi sur la protection des informations personnelles de la République populaire de Chine — En vigueur le 1er novembre 2021 », 7 septembre 2021, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/.

55 MeitY, « Politique relative aux centres de données 2020 : ébauche pour discussion », https://www.meity.gov.in/writereaddata/files/Draft%20Data%20Centre%20Policy%20-%2003112020_v5.5.pdf.

56 Traduction non officielle de la loi sur la cybersécurité, 12 juin 2018, https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf.

détectant, en contrant et en prévenant les attaques dans le cyberespace. La loi exige que les fournisseurs étrangers de services en ligne localisent le stockage des données et disposent d'un bureau dans le pays. Les services réseau de données et de contenu peuvent être interrompus sur ordre des autorités. La loi fait allusion à une « autonomie » croissante en matière de cybersécurité et de protection de l'enfance, mais définit le terme de manière vague et ne précise pas comment cela sera garanti.

Ailleurs, la stratégie du Vietnam pour la protection nationale dans le cyberespace[57] fait référence à la souveraineté numérique centrée sur l'État. Le concept apparaît également dans les discours politiques.[58] Il est appliqué par le ministère de la Défense nationale dans le contexte militaire du Vietnam, le plaçant au cœur de la défense contre les menaces extérieures. Le Vietnam a créé un Cyber Command pour « protéger la souveraineté nationale dans le cyberespace ».[59] En résumé, malgré quelques moments de résistance à l'influence croissante de la Chine, le[60] Vietnam consolide son cadre et son approche de la souveraineté numérique à travers plusieurs lois et politiques qui s'inspirent du modèle chinois. [61] [62]

B. Afrique

Union africaine – En 2020, la stratégie de transformation numérique de l'Union africaine pour l'Afrique a défini une stratégie économique sur dix ans qui prévoit l'appropriation par l'Afrique des outils numériques en localisant les infrastructures et le stockage des données.[63] Elle compte réduire la domination des entreprises technologiques principalement américaines et européennes en construisant une infrastructure locale, financée par un fonds de souveraineté numérique,[64] qui devrait réduire les coûts et la latence de la connectivité internationale et

57 Anh Kiet, « Le Viet Nam renforce la protection de la souveraineté nationale dans le cyberespace », Hanoi Times, 9 décembre 2021, https://hanoitimes.vn/vietnam-tightens-national-sovereignty-protection-in-cyberspace-319495.html.

58 Ibid.

59 Ministère de la Défense nationale du Viet Nam, « Le Cyber Command a demandé de sauvegarder la souveraineté nationale dans le cyberespace »,
1er septembre 2018, https://vietnamnews.vn/politics-laws/420790/cyber-command-asked-to-safeguard-national-sovereignty-in-cyberspace.html

60 Justin Sherman, « Le contrôle d'Internet au Viet Nam : suivre les traces de la Chine ? » The Diplomat, 11 décembre 2019, https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/.

61 Justin Sherman, « Le contrôle d'Internet au Viet Nam : suivre les traces de la Chine ? » The Diplomat, 11 décembre 2019, https://thediplomat.com/2019/12/vietnams-internet-control-following-in-chinas-footsteps/.

62 Deborah Elms, « Souveraineté numérique : protectionnisme ou autonomie ? » Fondation Hinrich, septembre 2021, https://www.hinrichfoundation.com/research/wp/digital/digital-sovereignty-protectionism-or-autonomy/.

63 Union africaine, « La stratégie de transformation numérique pour l'Afrique (2020-2030) » https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

64 Créer un environnement harmonisé nécessaire pour garantir l'investissement et le financement en créant un fonds de souveraineté numérique afin de combler le déficit d'infrastructure numérique et de parvenir à un haut débit accessible, abordable et sécurisé, à travers la démographie, le genre et la géographie, https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf

accroître le contrôle local sur les communications, permettant finalement à l'Afrique de répondre à ses besoins. Elle appelle à une infrastructure de centre de données en Afrique pour héberger des serveurs et des systèmes critiques et aspire à localiser les données personnelles des citoyens.

Afrique du Sud – Le projet de politique sur les données et le cloud[65] traite les données comme un atout à protéger et à exploiter, en améliorant la capacité d'analyse des données du pays et en exigeant que toutes les « informations critiques » soient stockées et traitées localement. Il affirme la propriété de toutes les données générées en Afrique du Sud [66]et aborde la souveraineté numérique comme un moyen de développement économique.

Rwanda – Le gouvernement rwandais a été parmi les premiers à soutenir explicitement la souveraineté numérique, revendiquant la propriété du pays de toutes les données générées à l'intérieur de ses frontières. Sa « Politique de révolution des données au Rwanda »[67] de 2017 tend à créer une industrie basée sur les données et à localiser les données pour assurer la sécurité et la confidentialité.

Nigéria – Une mesure, la politique nigériane de cloud computing de 2019,[68] invoque explicitement la souveraineté des données. Elle encourage l'adoption par le secteur public des services cloud et de nouvelles exigences pour le traitement des données nationales. La souveraineté numérique a également figuré en bonne place dans la rhétorique politique, en particulier après l'interdiction de Twitter dans le pays en 2021-2022[69]. Préoccupé par le fait que les citoyens utilisaient des réseaux privés virtuels (VPN) pour contourner l'interdiction, le bureau nigérian de la présidence a discuté de la construction d'un pare-feu Internet avec l'Administration du cyberespace de Chine[70]. L'interdiction de Twitter a été levée après avoir accepté de payer une « taxe applicable » et d'établir un bureau local dans le pays.[71]

Sénégal – Une déclaration de haut niveau du président Macky Sall en 2021 a ordonné au gouvernement de migrer toutes les données de l'État des serveurs étrangers vers un centre de

65 David Monyae, 2021

66 Département de la communication et des technologies numériques, « Ébauche de politique nationale sur les données et le cloud », 2021.https://www.gov.za/sites/default/files/gcis_document/202104/44389gon206.pdf

67 « La révolution des données nationales au Rwanda et le Big data », 2017 http://statistics.gov.rw/publication/rwanda-national-data-revolution-and-big-data

68 Agence nationale de développement des technologies de l'information, « Politique du Nigéria sur le cloud computing », 2019 https://nitda.gov.ng/wp-content/uploads/2020/11/NCCPolicy_New1.pdf

69 « Le Nigéria interdit Twitter après la suppression du tweet du président » 5 juin 2021, The New York Times.https://www.nytimes.com/2021/06/05/world/africa/nigeria-twitter-president.html

70 Socrates Mbamalu, « La présidence rencontre le cyberrégulateur chinois pour construire un pare-feu Internet nigérian », 6 juin 2021, Fondation pour le journalisme d'investigation https://fij.ng/article/exclusive-presidency-meets-with-chinas-cyber-regulator-to-build-nigerian-internet-firewall/

71 Adeyemi Adepetun, « Nigéria, l'accord sur Twitter risque de s'effondrer à cause de la restructuration mondiale », 8 novembre 2022, The Guardian.https://guardian.ng/news/nigeria-twitter-agreement-risks-collapse-over-global-restructuring/

données national financé par le gouvernement chinois,[72] après avoir conclu que la majorité des données générées dans le pays sont stockées à l'étranger.[73] Le Sénégal semble adopter une vision de la souveraineté numérique centrée sur l'État, rendue possible par les investissements de la Chine et les équipements auprès de fournisseurs chinois. La politique souhaite saisir la valeur économique des données et empêcher l'accès des étrangers à celles-ci, bien que la manière dont elle remédiera au manque relatif de champions nationaux du numérique ne soit pas très claire.

C. Europe, y compris la Russie

Union européenne – La souveraineté numérique dans l'Union européenne est une vision de haut niveau qui n'est pas directement intégrée dans les propositions réglementaires et législatives, permettant ainsi son application fluide à travers un large éventail d'objectifs politiques. Il n'existe pas de terme unique convenu dans le cadre de l'élaboration des politiques de l'UE, les termes « souveraineté numérique »,[74] « souveraineté technologique »[75] et « économie numérique européenne souveraine »[76] étant tous utilisés dans les documents de stratégie et les déclarations publiques sans que l'on sache clairement en quoi ces termes diffèrent, le cas échéant. La nature évolutive de la souveraineté numérique dans le contexte de l'UE se prête également à une variété d'objectifs politiques dans les domaines de la cybersécurité, de la compétitivité économique, de la recherche, de la sécurité de la chaîne d'approvisionnement et de la protection des données.

« Une Europe adaptée à l'ère numérique, » une stratégie de 2019 visant à définir l'agenda numérique de l'UE, considère la région comme un acteur mondial de la normalisation et souligne la nécessité de « renforcer sa souveraineté numérique ».[77] La stratégie a inspiré la loi sur les

72 « Le Sénégal vise la souveraineté numérique avec un nouveau centre de données soutenu par la Chine » Reuters, 22 juin 2021 https://www.reuters.com/article/senegal-datacenter-idINL5N2O44D3

73 « Le Sénégal ouvre un centre de données national au nom de la souveraineté numérique », Le Figaro, 22 juin 2021 https://www.lefigaro.fr/flash-eco/le-senegal-ouvre-un-centre-de-donnees-national-au-nom-de-la-souverainete-numerique-20210622

74 Commission européenne, « Une Europe adaptée à l'ère numérique Donner aux citoyens les moyens d'accéder à une nouvelle génération de technologies », https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

75 Commission européenne, « COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL La stratégie de cybersécurité de l'UE pour la décennie numérique », https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN

76 Commission européenne, « Loi sur les données : la Commission propose des mesures pour une économie des données équitable et innovante », https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113

77 Commission européenne, « Une Europe adaptée à l'ère numérique Donner aux citoyens les moyens d'accéder à une nouvelle génération de technologies », https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

marchés numériques (DMA),[78]la loi sur les services numériques (DSA)[79] et la loi européenne sur les puces[80].

La stratégie 2020 de l'UE en matière de cybersécurité pour la décennie numérique oriente les investissements vers l'atténuation des risques technologiques et géopolitiques pour la sécurité de l'UE. Le document appelle à « la souveraineté et au leadership technologiques »,[81] tout en soulignant l'engagement de l'UE en faveur d'un Internet mondial et libre. Parmi ses axes de travail figure un « Résolveur de système européen de noms de domaine »,[82] appelé DNS4EU, pour renforcer les redondances dans l'infrastructure Internet mondiale. Ces projets[83] sont destinés à une utilisation volontaire pour créer de la résilience et compléter les options mondiales existantes. Ces propositions dressent un tableau à multiples facettes de la souveraineté numérique qui peut être divisé en quatre thèmes :

Concurrence économique : la DMA et la DSA cherchent à réduire la domination des marchés technologiques, généralement par des entreprises américaines opérant au niveau de la couche application, y compris les médias sociaux, la recherche et la messagerie. La souveraineté numérique signifie ici créer les conditions permettant aux entreprises européennes de concurrencer les fournisseurs étrangers, à la fois pour maintenir l'influence mondiale de l'Europe et garantir les droits fondamentaux de ses citoyens. Dans ce cadre, la souveraineté numérique signifie la capacité de l'Europe à développer ses propres fournisseurs numériques pour que la région puisse déterminer son propre avenir.

Résilience de la chaîne d'approvisionnement : des mesures telles que la loi européenne sur les puces et l'initiative DNS4EU répondent à la préoccupation selon laquelle la dépendance excessive à l'égard des fournisseurs étrangers dans la chaîne d'approvisionnement et la fourniture d'infrastructures constitue une vulnérabilité stratégique. L'European Chip Act aspire à réduire la dépendance vis-à-vis des puces à semi-conducteurs provenant de l'étranger, principalement de la Chine et de Taïwan. L'appel d'offres DNS4EU s'oriente vers la création d'un résolveur volontaire du système européen de noms de domaine comme alternative aux plus

78 Commission européenne, « Loi sur les marchés numériques », https://competition-policy.ec.europa.eu/sectors/ict/dma_en

79 Commission européenne, « Paquet législatif relatif aux services numériques », https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

80 Commission européenne, « La loi européenne sur les puces, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

81 Commission européenne, « La stratégie de l'UE en matière de cybersécurité », https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

82 Union européenne, « Communication conjointe au Parlement européen et au Conseil : La stratégie de l'UE en matière de cybersécurité pour la décennie numérique », https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN

83 Commission européenne, Opportunités de financement et d'appel d'offres, « Équiper les réseaux fédérateurs d'infrastructures de résolution DNS hautes performances et sécurisées - Identifiant du sujet Works : CEF-DIG-2021-CLOUD-DNS-WORKS », https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/cef-dig-2021-cloud-dns-works

grands services mondiaux que la plupart des fournisseurs utilisent actuellement, et qui, selon certains, pourraient constituer des points d'étranglement en cas d'attaque importante. Cependant, en plus de bloquer du contenu tel que les messages d'hameçonnage et les logiciels malveillants, comme le font régulièrement d'autres résolveurs DNS, l'appel d'offres exige également que les fournisseurs potentiels bloquent le « contenu illégal » sur l'ensemble du continent.[84] Nous notons que le filtrage DNS présente des inconvénients potentiellement importants, qui doivent être pris en considération lors de l'élaboration d'une politique. [85]

Protection contre les cyberattaques : la stratégie de cybersécurité de l'UE[86] s'incarne dans des mesures telles que la mise à jour de la directive sur la sécurité des réseaux et de l'information (NIS2)[87] visant à établir un niveau commun de sécurité et de résilience des infrastructures numériques dans tous les États membres, ainsi qu'un réseau de centres d'opérations qui forment un « bouclier de cybersécurité » pour la détection précoce des cyberattaques.

Autonomisation de l'individu : la DSA a pour but d'assurer « un contrôle et une surveillance démocratiques accrus sur les plateformes systémiques ».[88] L'initiative DNS4EU ambitionne de fournir une résolution DNS par des fournisseurs basés dans l'UE qui respectent la confidentialité des données des utilisateurs, en empêchant la monétisation des requêtes DNS des Européens. Les décideurs associent souvent ce concept de souveraineté numérique au « capitalisme de surveillance »[89] et soulignent la nécessité de rétablir l'équilibre des pouvoirs entre les citoyens et les entreprises.[90]

La souveraineté numérique dans l'UE a des significations, des applications et des objectifs différents. Comme l'UE est une grande puissance économique et politique à part entière, dans

84 Ernesto Van der Sar, « L'UE veut son propre résolveur DNS qui peut bloquer le trafic « illégal », 19 janvier 2022 https://torrentfreak.com/the-eu-wants-its-own-dns-resolver-that-can-block-unlawful-traffic-220119/

85 Internet Society, « Points de vue de l'Internet Society sur le filtrage du système de noms de domaine (DNS) : », https://www.internetsociety.org/wp-content/uploads/2018/10/Perspectives-on-Domain-Name-System-Filtering-en.pdf

86 Commission européenne, « Nouvelle stratégie de l'UE en matière de cybersécurité et nouvelles règles pour rendre les entités critiques physiques et numériques plus résilientes », https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2391

87 Thinktank, Briefing du Parlement européen, La directive NIS2 : un niveau commun élevé de cybersécurité dans l'UE », https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

88 Commission européenne, « La loi sur les services numériques : garantir un environnement en ligne sûr et responsable », https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

89 Le « capitalisme de surveillance » est un terme popularisé par Shoshanna Zuboff dans son essai de 2014, « A Digital Declaration : Big Data as Surveillance Capitalism » et son livre de 2019, « The Age of Surveillance Capitalism : The Fight for a Human Future at the New Frontier of Power ». Il fait référence à un système économique basé sur la collecte et la marchandisation de données sur les personnes, à des fins de profit économique, conduisant à la croissance d'entreprises quasi monopolistiques dotées d'un pouvoir économique, politique et social mondial important et largement illimité.

90 https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

les réunions multilatérales telles que le G7 et le G20, et par l'exportation de ses réglementations via « l'effet Bruxelles »,[91] ces cadrages peuvent avoir une influence mondiale.

États membres de l'UE : France, Allemagne et Italie – La France et l'Allemagne sont les premiers moteurs de la souveraineté numérique au sein de l'Union européenne et sont rapidement suivies par l'Italie, qui utilise une rhétorique similaire. La prise de position commune franco-allemande 2020 Gaia-X souhaite une « infrastructure de données souveraine » permettant aux États membres de l'UE d'échanger des données en toute sécurité. Elle traite le volume notable de données partagées et traitées entre les entreprises européennes comme une source d'innovation, de valeur et de compétitivité sur le marché numérique mondial ».[92] Elle fait également allusion à la souveraineté individuelle et fait référence à la capacité accrue des « utilisateurs [à] conserver la souveraineté sur leurs données ».[93]

La souveraineté numérique de l'Italie est vue sous l'angle de la sécurité nationale. Sa Stratégie nationale de cybersécurité 2022[94] a pour but de se protéger contre les activités hostiles des acteurs étatiques, la cybercriminalité, le cyberespionnage et les campagnes de désinformation qui cherchent à polariser l'opinion publique.

La France, l'Allemagne et l'Italie sont de grandes économies, ont une population importante et ont historiquement occupé des positions avantageuses en « exerçant leur influence » au niveau de l'UE. La souveraineté numérique ne fait pas exception à cette tendance, la France et l'Allemagne articulant leurs visions de la souveraineté numérique avant la Commission européenne.

Fédération de Russie – Le terme souveraineté numérique a été fréquemment utilisé lors des réunions annuelles du Forum Russie/Chine sur un Internet plus sûr, notamment lors d'une intervention en 2016 d'un sénateur exhortant le préfiltrage au niveau du fournisseur à protéger la « souveraineté numérique russe ».[95]

La souveraineté numérique en Russie est conçue principalement comme la souveraineté de l'État dans le domaine numérique, et les mesures pertinentes habilitent exclusivement les

91 « L'effet Bruxelles, comment l'Union européenne influence le monde », Anu Bradford, (2020) https://global.oup.com/academic/product/the-brussels-effect-9780190088583?cc=au&lang=en&

92 Position franco-allemande sur GAIA-X, https://www.bmwi.de/Redaktion/DE/Downloads/F/franco-german-position-on-gaia-x.pdf?__blob=publicationFile&v=4

93 GAIA-X, dernière modification le 6 septembre 2022 https://gaia-x.eu/

94 Gouvernement italien, « Stratégie nationale de cybersécurité, 2022-2026, https://www.acn.gov.it/ACN_EN_Strategia.pdf

95 Forum Internet sûr, Russie, « Le Forum de Moscou pour un Internet plus sûr adopte la feuille de route de la coopération russo-chinoise en matière de cybersécurité », 19 avril 2021, https://safeinternetforum.ru/en/novosti/moscow-safer-internet-forum-adopts-russia-china-cybersecurity-cooperation-roadmap.html

institutions étatiques à se protéger contre les menaces réelles ou perçues pour la sécurité nationale, telles que la désinformation, le contenu terroriste et les cyberattaques d'acteurs étatiques hostiles. Cette approche a abouti à des politiques qui coupent de plus en plus la Russie de l'Internet mondial en rendant obligatoire une infrastructure Internet construite et contrôlée par l'État en Russie.

La « loi pour un Internet souverain »[96] de 2019 et les « règles de gestion centralisée d'un réseau de communication public »[97] connexes imposaient aux opérateurs de réseaux de fournir des informations techniques et un accès à l'organisme de réglementation, Roskomnadzor,[98] afin qu'il puisse « assurer le fonctionnement des ressources Internet russes dans le cas où les opérateurs de télécommunications russes ne pourraient pas se connecter à des serveurs racine [DNS] étrangers ».[99] Cela a permis à l'organisme de réglementation de couper la connectivité ou les services internationaux (par exemple, les services cloud) et d'augmenter sa capacité à intercepter et à bloquer le trafic. Le concept d'un Internet souverain pour la Russie est un concept qui ne peut être déconnecté ou perturbé par des acteurs étrangers hostiles, mais sa mise en œuvre permet un contrôle important sur les flux de communication et d'information en Russie. Elle rend également obligatoire l'utilisation d'outils techniques pour filtrer et censurer le contenu en ligne au nom de la lutte contre les « faux messages » et les contenus terroristes.[100] [101]

Indirectement, le Conseil allemand des relations étrangères a établi un lien conceptuel[102] entre la conception russe de la souveraineté numérique et la loi modifiée de 2014 sur la localisation des données,[103] ainsi que les « lois Yarovaya » russes de 2016, qui ont introduit des capacités de surveillance de masse au nom de la lutte contre le terrorisme et d'autres « idéologies » en ligne.[104]

---

96 « Modifications de la loi fédérale sur les communications et de la loi fédérale sur l'information, les technologies de l'information et la protection de l'information », 22 avril 2019, http://publication.pravo.gov.ru/Document/Text/0001201905010025.

97 Règles de gestion centralisée d'un réseau de communication public, approuvées par le Décret gouvernemental du 12 février 2020, 2020 N 127 : Правила централизованного управления сетью связи общего пользования

98 Federal Service for Supervision of Communications, Information Technology, and Mass Media (Service fédéral de surveillance des communications, des technologies de l'information et des médias)

99 'Принят закон о «суверенном интернете»', http://duma.gov.ru/news/44551/

100 'Федеральный закон от 06.07.2016 г. № 374-ФЗ', http://kremlin.ru/acts/bank/41108

101 'Федеральный закон от 06.07.2016 г. № 375-ФЗ', http://kremlin.ru/acts/bank/41113

102 Alena Epifanova et Philipp Dietrich, DGAP, Conseil allemand des relations étrangères, « La quête russe des ambitions, des réalités et de sa place dans le monde pour la souveraineté numérique », https://dgap.org/en/research/publications/russias-quest-digital-sovereignty

103 https://pd.rkn.gov.ru/authority/p146/p191/

104 Alena Epifanova et Philipp Dietrich, DGAP, Conseil allemand des relations étrangères, « La quête russe des ambitions, des réalités et de sa place dans le monde pour la souveraineté numérique », https://dgap.org/en/research/publications/russias-quest-digital-sovereignty

Le concept de souveraineté numérique de la Russie est important car il défend sa vision d'un contrôle étatique direct d'Internet dans des organes de gouvernance clés tels que l'Union internationale des télécommunications. Alors que le concept de souveraineté numérique gagne du terrain dans le monde, la Russie pourrait utiliser ces organisations pour influencer la réglementation d'Internet à l'échelle mondiale. Il a également une influence régionale. La Russie — avec la Chine — a une influence directe sur les membres eurasiens, dont le Kazakhstan, le Kirghizistan et le Tadjikistan, par le biais de l'Organisation de coopération de Shanghai. L'accord de coopération en matière de cybersécurité de 2015 de l'organisation vise à limiter l'utilisation de technologies conçues « pour s'immiscer dans les affaires intérieures des États ; saper la souveraineté, la stabilité politique, économique et sociale ; [et] troubler l'ordre public. »[105]

105 https://theglobalobservatory.org/2016/12/russia-china-digital-sovereignty-shanghai-cooperation-organization/

Annexe II - Le mode de fonctionnement du réseau Internet

Le mode de fonctionnement du réseau Internet

Propriété essentielle	Avantages
1. Une infrastructure accessible dotée d'un protocole commun ouvert et comportant peu de barrières d'entrée	Un accès non restreint et des protocoles communs assurent une connectivité mondiale et soutiennent le développement du réseau. Plus le nombre de participants augmente, plus la valeur d'Internet augmente pour chacun.
2. Une architecture ouverte aux composantes interopérables et réutilisables, basée sur des processus de développement de normes ouvertes adoptées volontairement par la communauté des utilisateurs	L'architecture ouverte donne naissance à des services interopérables communs, qui permettent partout une innovation rapide et non soumise à une autorisation quelconque. Grâce au processus de normalisation inclusif et à l'adoption basée sur la demande, les évolutions nécessaires sont adoptées et celles qui sont superflues disparaissent.
3. Une gestion décentralisée et un système unique de routage distribué, à la fois évolutif et agile	Le routage distribué offre un réseau résilient et adaptable de réseaux autonomes, permettant des optimisations locales tout en maintenant une connectivité mondiale.
4. **Des identifiants communs au niveau mondial** non ambigus et universels	Un ensemble d'identifiants communs permet une gestion uniformisée de l'adressage, ainsi qu'une vision cohérente de l'intégralité du réseau, sans fragmentation ni fractures.
5. Un réseau technologiquement neutre et à but général, simple et adaptable	Le caractère général assure la flexibilité. Internet sert en permanence à une communauté d'utilisateurs et d'applications diverse et en perpétuelle évolution. Il ne nécessite pas de changements importants pour prendre en charge cet environnement dynamique.

Pour plus d'informations sur la manière d'effectuer une évaluation de l'impact sur Internet, veuillez consulter notre guide en ligne : **Comment réaliser un dossier d'impact sur Internet** à

l'aide de la **boîte à outils pour l'évaluation de l'impact sur Internet.**[106]

Les facilitateurs d'un Internet ouvert, mondialement connecté, sécurisé et fiable

Soutenir un Internet ouvert	
Accès facile et sans restrictions	Il est facile de devenir une partie d'Internet, pour les réseaux comme pour les utilisateurs. Cela implique qu'Internet soit abordable pour les utilisateurs, que les services Internet soient accessibles et que les réseaux puissent facilement intégrer Internet, sans règlement ou barrières commerciales superflus, pour les utilisateurs comme pour les réseaux.
Utilisation et déploiement sans restrictions des technologies d'Internet	Les technologies et normes d'Internet sont adoptables sans restrictions. Ce facilitateur s'applique aux terminaux ; les technologies utilisées pour se connecter à Internet et l'utiliser n'exigent pas d'autorisation d'un tiers, d'un fournisseur de systèmes d'exploitation (OS), d'un fournisseur de réseau ou de tout autre tiers. L'infrastructure Internet est une ressource disponible pour quiconque souhaite l'utiliser. Les technologies existantes peuvent être combinées et utilisées pour créer de nouveaux produits et services qui élargissent les capacités d'Internet.
Développement, gestion et gouvernance collaboratifs	Les technologies et normes d'Internet sont développées, gérées et gouvernées d'une manière ouverte et collaborative. Cette collaboration ouverte s'étend à la construction et au fonctionnement d'Internet et des services construits sur Internet. Le processus de développement et de maintenance est basé sur la transparence et le consensus, et son objectif est l'optimisation de l'infrastructure et des services au bénéfice des utilisateurs de ces technologies.
Soutenir un Internet mondialement connecté	

106 Internet Society, « Comment réaliser une présentation de l'impact sur Internet – Boîte à outils pour l'évaluation de l'impact sur Internet », https://www.internetsociety.org/resources/doc/2021/how-to-conduct-an-internet-impact-brief/

Accessibilité sans restriction	Les utilisateurs d'Internet ont accès à toutes les ressources et technologies disponibles sur Internet et sont capables de rendre eux-mêmes des ressources disponibles. Une fois une ressource rendue disponible d'une manière quelconque par son propriétaire, il est impossible de bloquer un accès ou une utilisation légitime de cette ressource par des tiers.
Capacité disponible	La capacité d'Internet est suffisante pour répondre à la demande des utilisateurs. Personne ne s'attend à ce que la capacité d'Internet soit infinie, mais la capacité de connexion (ports, bande passante, services) doit être suffisante pour répondre à la demande des utilisateurs.
Soutenir un Internet sécurisé	
Confidentialité d'informations et des données des appareils et des applications	La confidentialité des données, réalisée généralement avec des outils tels que le chiffrement, permet aux utilisateurs d'envoyer des informations sensibles par Internet de façon à ce que des oreilles indiscrètes ou malveillantes ne puissent pas consulter le contenu ou savoir qui communique. Permettre le transfert de données sensibles participe à la création d'un Internet sécurisé. La confidentialité des données s'applique aussi aux données statiques et à celles conservées sur les appareils. (N.B., la « non-divulgation » contribue aussi à la confidentialité, qui relève d'un Internet fiable)
Intégrité de l'information, des applications et des services	L'intégrité des données envoyées sur Internet et stockées dans des applications n'est pas compromise. C'est-à-dire que les informations envoyées sur Internet ne peuvent pas être modifiées durant leur transit, à moins d'une demande d'une des parties communicantes (ex. : un bot de sous-titrage peut être utile pour convertir les mots parlés en texte).
Soutenir un Internet fiable	
Fiabilité, résilience et disponibilité	Internet est robuste quand des technologies et des procédés sont en place et permettent la distribution de services de la manière prévue. Si, par exemple, la disponibilité d'un service Internet est imprévisible, alors les utilisateurs considéreront cela comme un manque de fiabilité. Cela peut réduire la confiance non pas en un seul service, mais en Internet dans son ensemble. La résilience est liée à la fiabilité : un Internet résilient conserve un niveau acceptable de service même en présence

	d'erreurs, de comportements malveillants et d'autres perturbations liées à son fonctionnement normal.
Responsabilité	La responsabilité concernant Internet donne aux utilisateurs l'assurance que les organisations et les institutions avec lesquelles ils interagissent opèrent directement et indirectement de manière transparente et loyale. Dans un Internet responsable, les entités, les services et les informations peuvent être identifiés et les organisations impliquées devront rendre des comptes pour leurs actes.
Confidentialité	La confidentialité sur Internet est la capacité des individus et des groupes à comprendre et contrôler quelles informations les concernant sont recueillies et comment elles le sont, et à contrôler la façon dont elles sont utilisées et partagées. La confidentialité comprend souvent des aspects d'anonymisation, par la suppression de liens entre les données, les appareils, les sessions de communications et l'identité des personnes auxquelles ils se rattachent.

Pour plus d'informations sur la manière d'effectuer une évaluation de l'impact sur Internet, veuillez consulter notre guide en ligne : **Comment réaliser un dossier d'impact sur Internet** à l'aide de la **boîte à outils pour l'évaluation de l'impact sur Internet**.[107]

Annexe III — Méthodologie de recherche des types de souveraineté numérique

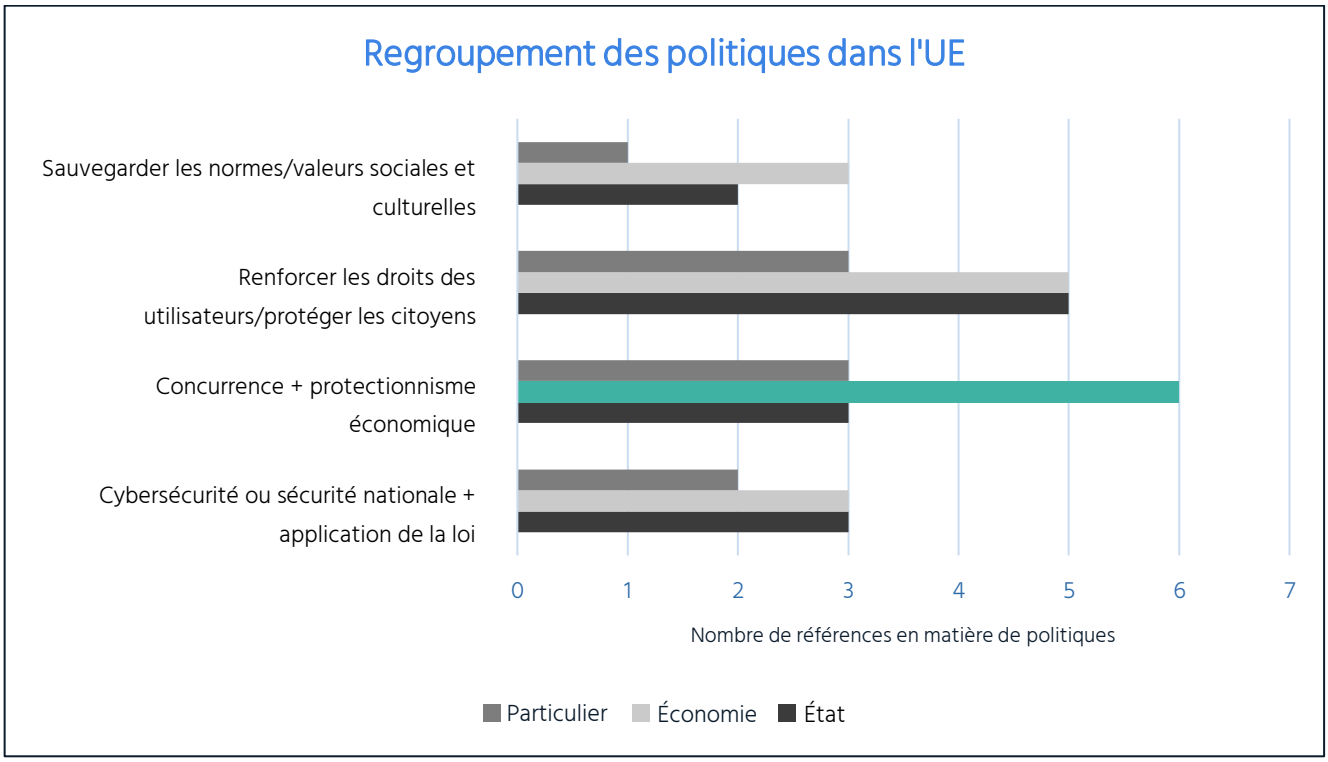
Cette étude a analysé trente-quatre politiques dans trois régions sur la base des deux catégories transversales d'objectifs politiques et d'acteurs habilités.Chaque politique est tracée sur le graphique en fonction de (a) ce qu'elle veut réaliser, et (b) qui elle habilite à réaliser la politique. Par exemple, si une politique a un objectif de sécurité nationale et habilite l'État, nous ajoutons un point à la cellule Sécurité nationale*État. Si la même politique responsabilise également l'individu, nous ajoutons un point à la cellule Sécurité nationale*Individu. Si une autre politique dans cette juridiction a également un objectif de sécurité nationale et habilite l'État, nous ajoutons un autre point à la cellule correspondante et l'additionnons jusqu'à 2.

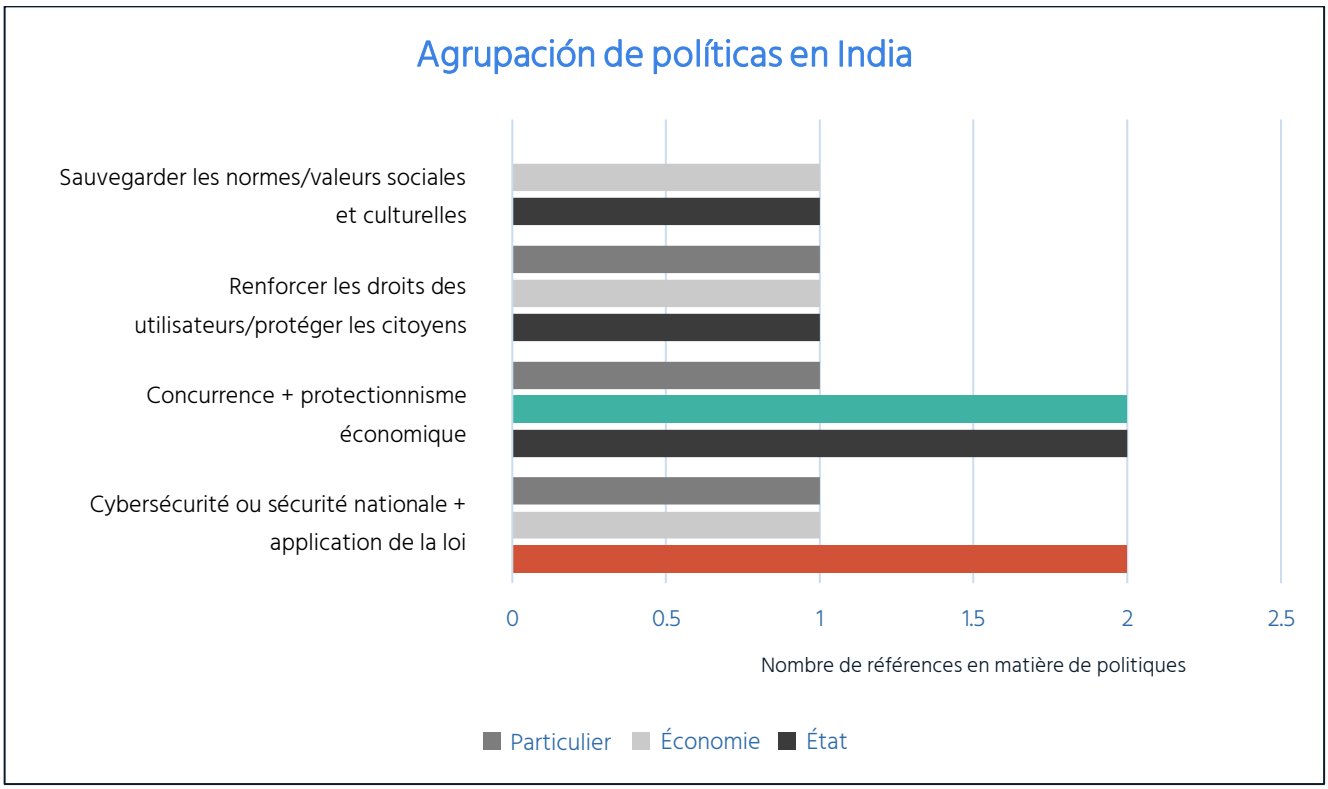
Le graphique ci-dessous montre que les politiques sont regroupées dans des domaines distincts, selon leurs objectifs. L'analyse de ces groupes par des entités habilitées a montré des groupes

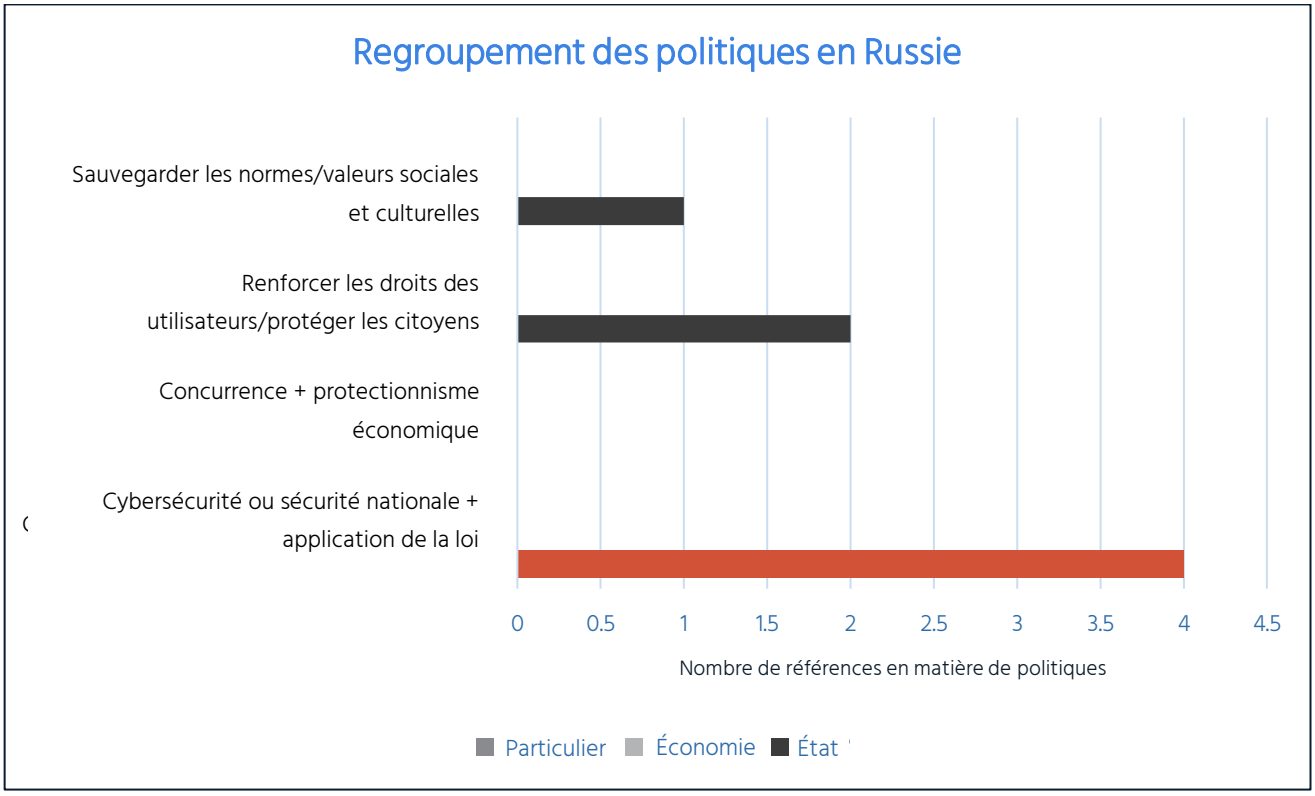
107 Internet Society, « Comment réaliser une présentation de l'impact sur Internet – Boîte à outils pour l'évaluation de l'impact sur Internet », https://www.internetsociety.org/resources/doc/2021/how-to-conduct-an-internet-impact-brief/

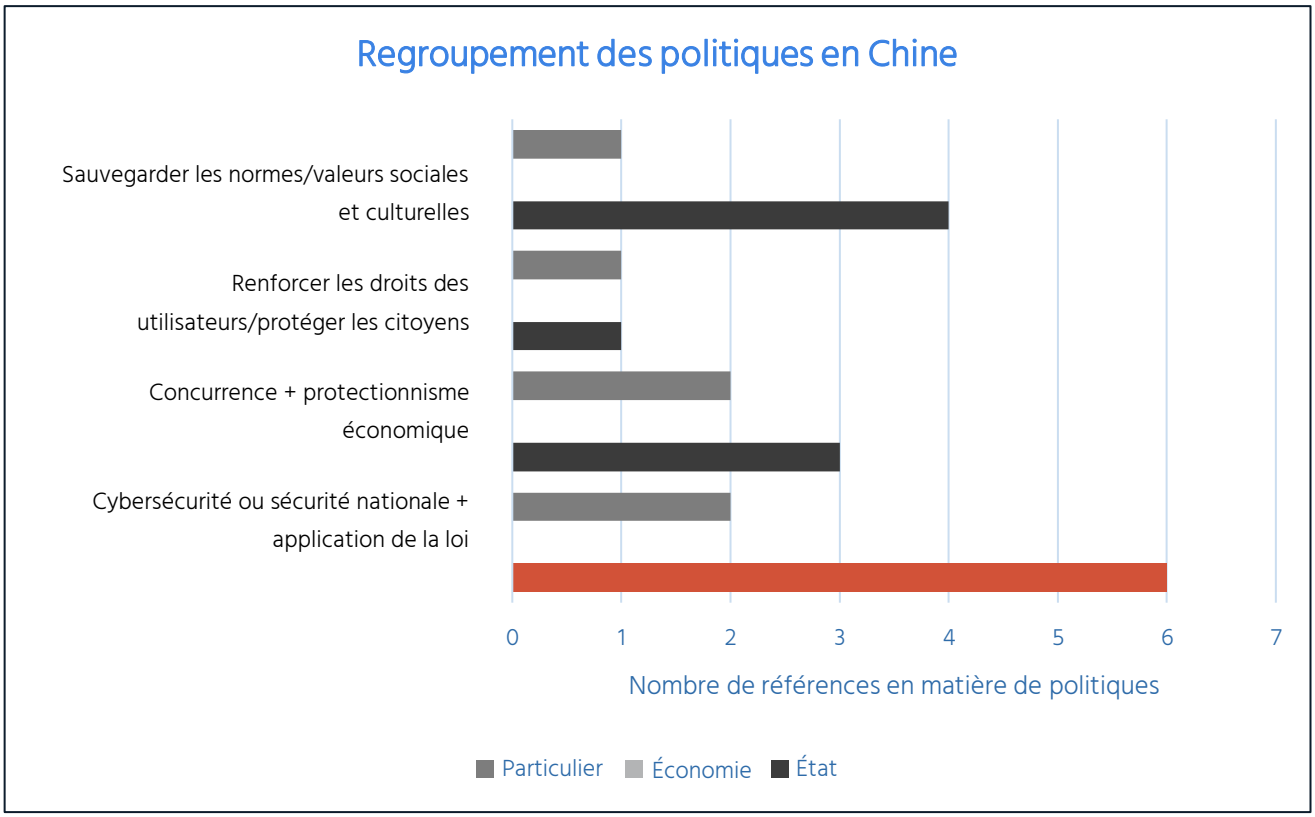
encore plus serrés qui nous ont permis d'identifier les principaux types de politiques ; un groupe distinct de politiques relève des cellules Sécurité nationale/État et Application de la loi/État, tandis que les politiques de type « axées sur l'économie » sont davantage centrées sur la concurrence/l'économie et les normes/la société). Il est important de noter que certains pays affichent un mélange des deux types dominants, tandis que d'autres ont un type qui se démarque. Le premier graphique montre plusieurs pays où ces tendances et les types correspondants sont les plus visibles.

Les modèles politiques dans différents pays exposant 2 types distincts de souveraineté numérique, marqués en rouge et vert.






Regroupement des politiques en Russie
Sauvegarder les normes/valeurs sociales et culturelles
Renforcer les droits des utilisateurs/protéger les citoyens
Concurrence + protectionnisme économique
Cybersécurité ou sécurité nationale + application de la loi
0
0.5
1
1.5
2
2.5
3
3.5
4
4.5
Nombre de références en matière de politiques
Particulier
Économie
État


Regroupement des politiques en Chine
Sauvegarder les normes/valeurs sociales et culturelles
Renforcer les droits des utilisateurs/protéger les citoyens
Concurrence + protectionnisme économique
Cybersécurité ou sécurité nationale + application de la loi
0
1
2
3
4
5
6
7
Nombre de références en matière de politiques
Particulier
Économie
État

Annexe IV — Tableaux des politiques et propositions analysées

Politiques de type sécurité nationale

Sécurité nationale et primauté du droit par l'État
Stratégie de transformation numérique en Afrique (2020 -2030)
Union africaine - Convention de Malabo - Convention sur la cybersécurité et la protection des données personnelles
Australie - Stratégie de cybersécurité (2020)
Australie - Stratégie de transformation numérique (2018)
Australie - Cadre de certification d'hébergement (2021)
Chine - Stratégie internationale de coopération sur le cyberespace (2017)
Chine - Loi sur la protection des informations personnelles (2021)
Règlement sur les noms de domaine Internet en Chine (2017)
Chine - Loi sur la cybersécurité (2017)
Chine - Loi sur la sécurité des données (2021)
UE - Loi sur les données (Proposition 2022)
UE - Stratégie de cybersécurité de l'UE pour la décennie numérique (2020)
UE - Loi sur les services numériques (Proposition - 2022)
Inde - Directives de cybersécurité CERT-In
Inde - Projet de loi sur la protection des données (2021)
Indonésie - Règlement gouvernemental (71/2019)
Italie - Stratégie nationale de cybersécurité (2022)
Russie - « Lois Yarovaya » (2016) : Loi fédérale « sur la lutte contre le terrorisme » et « Code pénal de la Fédération de Russie et Code de procédure pénale de la Fédération de Russie »
Russie - Loi sur la localisation des données (modification de 2014)
Russie - Règles pour la gestion centralisée d'un réseau de communication public (2019), largement connues sous le nom de « loi russe pour un Internet souverain »
Rwanda - Politique de révolution des données (2017)
Afrique du Sud - Politique nationale sur les données et le cloud (proposition)
Vietnam - Loi sur la cybersécurité (2018)
Vietnam - Mise en place du Cyber Command (2018)

Politiques de type renforcement de l'économie

Renforcer l'économie par la concurrence
Union africaine - Stratégie de transformation numérique de l'Afrique (2020 -2030)
UE - Loi sur les données (Proposition 2022)
UE - Loi sur les données, commentaires de Thierry Breton, commissaire au marché intérieur
UE - Loi sur les services numériques (Proposition 2022)
UE - Cloud européen (discours sur l'état de l'Union 2020 de la présidente de la CE Ursula von der Leyen) (2020)
UE - GAIA-X (2020)
UE - Façonner l'avenir numérique de l'Europe (2019)
Inde : Politique relative aux centres de données (2020)
Inde : Projet de loi sur la protection des données (2021)
Nigéria - Politique sur le cloud computing (2019)
Afrique du Sud - Politique nationale sur les données et le cloud (Proposition)