

Input du cep

No 2 | 2025

14 janvier 2025

Comment l'Europe peut-elle s'orienter sur la corde raide de la réglementation ?

Compromis et risques dans la politique numérique de l'UE

Anselm Küsters et Cecilia Emma Sottilotta



Source : Figure générée par DALL-E

La création récente du poste de commissaire européen chargé de la souveraineté technologique, de la sécurité et de la démocratie souligne la volonté nouvelle de l'Union européenne d'affirmer son rôle dans le paysage numérique mondial. Toutefois, cette ambition s'accompagne d'un réseau complexe de compromis qui, s'ils ne sont pas reconnus, posent des risques pour l'élaboration de la future politique numérique de l'UE. Cette note politique explore et catégorise ces compromis et propose des solutions pour y remédier.

- ▶ De par sa nature même, l'élaboration des politiques de l'UE implique des compromis. Par exemple, les décisions visant à renforcer la souveraineté technologique peuvent entraver la compétitivité du marché ou étouffer l'innovation. Le fait de ne pas reconnaître ces compromis peut avoir des conséquences inattendues, telles que l'excès de réglementation ou la réduction de la coopération.
- ▶ En l'absence de leadership technologique, il existe un trilemme critique entre la souveraineté technologique, la sécurité et la démocratie, où l'amélioration d'un aspect peut compromettre les autres. Nous analysons ce trilemme pour l'UE à travers des études de cas sur la vie privée contre l'innovation dans le GDPR, la réglementation contre la liberté d'expression dans la loi sur les services numériques, les risques de cybersécurité et les incitations économiques dans le développement européen des TIC, l'éthique contre la compétitivité dans la réglementation de l'IA, l'autonomie contre la coopération concernant l'infrastructure informatique, et le bien-être du consommateur contre les valeurs externes dans la politique de concurrence de la Big Tech.
- ▶ Nous proposons qu'une coopération accrue avec les partenaires internationaux et la diplomatie numérique puissent aider l'UE à atténuer certains compromis. Dans l'ensemble, la reconnaissance et la gestion stratégique des compromis en matière de politique numérique sont essentielles pour que l'UE puisse réaliser ses ambitions en matière de souveraineté technologique sans compromettre ses principes fondateurs.

Sommaire

1	Introduction.....	3
2	Schéma général d'analyse des compromis de la politique numérique de l'UE.....	4
3	Études de cas individuels	11
3.1	Protection des données : Vie privée contre innovation	11
3.2	Modération des plateformes : Réglementation vs. liberté d'expression, compétitivité et sécurité	13
3.3	Lignes directrices sur la cybersécurité : Sécurité et intérêts économiques	16
3.4	Réglementation de l'IA : Normes éthiques et compétitivité.....	19
3.5	Infrastructure informatique : Autonomie stratégique ou coopération mondiale	21
3.6	Politique de concurrence : Bien-être des consommateurs et intérêts publics plus larges .	24
4	Dimension externe : Aborder les compromis par le biais de partenariats	26
5	Conclusion : La hiérarchie des compromis	33

Figures

Fig. 1 :	Trilemme généralisé dans l'élaboration de la politique numérique de l'UE.....	7
Fig. 2 :	Capacité de production de semi-conducteurs par région, 1990-2020	21
Fig. 3 :	Investissements dans les puces, 2021-2023	22
Fig. 4 :	Modélisation de scénarios : coalitions d'investissement possibles	32
Fig. 5 :	Résumé des résultats.....	34

1 Introduction

Les progrès technologiques rapides, associés à l'évolution de la géopolitique, ont intensifié les défis que doit relever l'Union européenne (UE) dans la gestion de l'espace numérique. La nomination d'un nouveau commissaire européen chargé de la "souveraineté technologique, de la sécurité et de la démocratie" marque une étape stratégique dans la résolution de ces problèmes complexes. Toutefois, cette évolution met également en lumière un problème crucial : les politiques numériques de l'UE impliquent souvent des compromis inhérents qui ne sont pas suffisamment reconnus ou débattus ouvertement, ce qui crée à son tour une incertitude et des risques réglementaires. Par exemple, il est souvent avancé que des réglementations détaillées et imposées d'en haut, conçues pour protéger les citoyens, pourraient par inadvertance entraver la compétitivité des entreprises européennes sur la scène mondiale. Dans le même ordre d'idées, les efforts visant à renforcer la sécurité pourraient porter atteinte au droit à la vie privée ou étouffer les libertés civiles, ce qui serait en contradiction avec les principes démocratiques fondamentaux de l'UE.

CepInput analyse ces compromis souvent méconnus. En examinant des études de cas spécifiques, nous visons à découvrir plus en détail l'équilibre délicat requis entre des objectifs concurrents et à mettre en évidence les risques potentiels liés à la négligence de ces complexités. Notre analyse couvre un certain nombre de domaines critiques en relation avec la politique numérique européenne, y compris la vie privée contre l'innovation dans les règles de protection des données, la réglementation contre la liberté d'expression dans la modération des plateformes, les risques de cybersécurité et les incitations économiques dans le développement européen des TIC, les normes éthiques contre la compétitivité dans la réglementation de l'IA, l'autonomie stratégique contre la coopération mondiale dans la construction d'une infrastructure informatique à grande échelle, et le bien-être des consommateurs contre les intérêts publics plus larges dans le contexte d'une politique de concurrence axée sur la technologie.

Un thème général se dégage de ces études de cas. Les menaces que les avancées technologiques et les politiques numériques font peser sur la démocratie et la sécurité sont souvent multi-causales, défiant ainsi les explications causales simplistes. Cette complexité est aggravée par la nouveauté relative de nombreux compromis sous-jacents, ce qui entraîne un manque de données empiriques à long terme et de consensus scientifique. Toutefois, ce manque d'analyses systématiques et la nature ouverte de la recherche empirique ne diminuent pas l'importance de l'impact de la technologie sur la démocratie et la sécurité, et ne dispensent pas la politique numérique de l'UE de répondre à ces préoccupations. Au contraire, la protection des valeurs fondamentales est une tâche intrinsèquement préventive, qui nécessite des mesures politiques proactives.

Il est essentiel de reconnaître et d'aborder les compromis dans la politique numérique de l'UE afin d'éviter la discrétion et de permettre un apprentissage politique ultérieur au fil du temps tout en favorisant un écosystème numérique résilient, innovant et démocratique en Europe. Ce défi est particulièrement pertinent à la lumière des plans de l'UE visant à unifier et à harmoniser les règles numériques entre les États membres au cours du prochain mandat, dans le but de simplifier le paysage réglementaire tout en maintenant l'efficacité. Alors que le nouveau commissaire européen chargé de la souveraineté technologique, de la sécurité et de la démocratie prend ses fonctions, notre analyse suggère qu'aucune approche politique unique ne peut répondre de manière adéquate à toutes les préoccupations sans compromettre potentiellement d'autres objectifs importants de politique publique. Dans

cette optique, nous suggérons - peut-être de manière contre-intuitive - qu'une coopération renforcée et stratégique avec les partenaires internationaux et la diplomatie numérique pourrait aider l'UE à atténuer certains des compromis.

Sur la base de cette motivation, notre document est structuré comme suit. Tout d'abord, nous nous appuyons sur la littérature et les théories existantes pour élaborer un cadre général d'analyse des compromis dans la politique numérique de l'UE (section 2). Le cœur de notre analyse est consacré à six études de cas individuelles, chacune mettant en lumière un domaine spécifique de la politique numérique de l'UE où des compromis importants et les risques qui en résultent sont évidents (section 3). Après ces études de cas, nous nous intéressons à la dimension extérieure de la politique numérique de l'UE (section 4). Nous explorons ici la manière dont les partenariats et la coopération internationale peuvent potentiellement contribuer à résoudre certains des compromis identifiés et offrir une voie vers une politique plus efficace. Enfin, nous concluons (section 5).

2 Schéma général d'analyse des compromis de la politique numérique de l'UE

Le trilemme, également connu sous le nom de "trinité impossible", est un cadre conceptuel populaire en économie internationale qui met en évidence les compromis inhérents auxquels les décideurs politiques sont confrontés dans la gestion de leurs économies dans un monde de plus en plus globalisé.¹ Le trilemme macroéconomique classique, conceptualisé pour la première fois par Mundell et Fleming dans les années 1960, stipule qu'un pays ne peut pas réaliser simultanément un taux de change fixe, un compte de capital libre et une politique monétaire indépendante.² Selon cette théorie, les décideurs politiques doivent choisir seulement deux de ces trois objectifs, car il est impossible d'atteindre les trois en même temps. Il existe de nombreux exemples historiques de ce type d'arbitrage : en adoptant une monnaie commune, par exemple, les pays de la zone euro ont effectivement choisi d'avoir des taux de change fixes entre eux et de permettre la libre circulation des capitaux - au prix du sacrifice d'une politique monétaire indépendante.³ Dans le même ordre d'idées, Schoenmaker a proposé un "trilemme fiscal" qui s'applique spécifiquement à la politique budgétaire.⁴ Ce trilemme suggère que les pays ne peuvent pas atteindre simultanément la stabilité financière, l'intégration financière et la politique fiscale nationale. Rey a remis en question le trilemme traditionnel en soutenant que dans un monde où la mobilité des capitaux est élevée, une politique monétaire indépendante n'est possible

¹ Joshua Aizenman, Menzie David Chinn, et Hiro Ito, "The 'Impossible Trinity' Hypothesis in an Era of Global Imbalances : Measurement and Testing", *Review of International Economics* 21, no. 3 (août 2013) : 447–58, <https://doi.org/10.1111/roie.12047>.

² R. A. Mundell, "Capital Mobility and Stabilization Policy Under Fixed and Flexible Exchange Rates", *Canadian Journal of Economics and Political Science* 29, no. 4 (novembre 1963) : 475–85, <https://doi.org/10.2307/139336> ; J. Marcus Fleming, "Domestic Financial Policies under Fixed and under Floating Exchange Rates", *Staff Papers - International Monetary Fund* 9, no. 3 (novembre 1962) : 369, <https://doi.org/10.2307/3866091>.

³ Maurice Obstfeld, Jay C. Shambaugh et Alan M. Taylor, "The Trilemma in History : Tradeoffs Among Exchange Rates, Monetary Policies, and Capital Mobility", *Review of Economics and Statistics* 87, no. 3 (août 2005) : 423–38, <https://doi.org/10.1162/0034653054638300>. Pendant le système de Bretton Woods (1944 à 1971), les pays maintenaient des taux de change fixes par rapport au dollar américain et disposaient d'une autonomie en matière de politique monétaire, mais les contrôles de capitaux étaient largement utilisés. Maurice Obstfeld et Alan Taylor, "The Great Depression as a Watershed : International Capital Mobility over the Long Run" (Cambridge, MA : National Bureau of Economic Research, mars 1997), <https://doi.org/10.3386/w5960>.

⁴ Dirk Schoenmaker, "The Financial Trilemma", *Economics Letters* 111, no. 1 (avril 2011) : 57–59, <https://doi.org/10.1016/j.econlet.2011.01.010>.

que si le compte de capital est géré.⁵ Cette perspective suggère que certains trilemmes peuvent évoluer avec le temps - dans ce cas, ils se transforment en un dilemme entre l'autonomie de la politique monétaire et la mobilité des capitaux. Plus récemment, les observateurs ont commencé à se demander si un trilemme pouvait également exister dans le domaine de la politique numérique.⁶

En effet, l'élaboration des politiques en matière de technologie est jalonnée de compromis complexes qui, s'ils sont négligés, peuvent conduire à des politiques qui vont à l'encontre de leurs propres objectifs.⁷ Au sein de l'UE, trois objectifs ont été mis en avant à plusieurs reprises, notamment par les commissaires européens lors de leurs auditions parlementaires et dans des rapports récents tels que ceux publiés par Draghi et Letta : la compétitivité économique et l'innovation, la sécurité et la souveraineté, ainsi que les droits fondamentaux et la cohésion sociale (figure 1). L'UE vise à être un leader mondial de l'innovation numérique, en favorisant un environnement dans lequel les entreprises peuvent prospérer et les avancées technologiques telles que l'intelligence artificielle (IA) peuvent être rapidement adoptées grâce à des plans tels que les "usines d'IA" ou l'initiative "Appliquer l'IA". Dans le même temps, elle doit protéger son infrastructure numérique et ses données contre les acteurs extérieurs afin de garantir son autonomie stratégique, par exemple dans l'espace cloud. Il est au moins aussi important de s'engager à respecter la vie privée, la liberté d'expression et d'autres droits fondamentaux qui sont profondément ancrés dans son cadre juridique et dans les traités fondateurs. En bref, la rhétorique officielle suggère fortement que la politique numérique de l'UE vise à équilibrer la compétitivité, la souveraineté et les droits .

Pour distinguer d'emblée les trois objectifs concurrents, nous proposons les définitions suivantes : (1) Compétitivité économique (et innovation) : La capacité des entreprises de l'UE (y compris les start-ups, les PME et les grandes entreprises) à innover et à se développer sur le marché numérique mondial, ce qui favorise la prospérité économique. (2) Sécurité (et souveraineté) : La protection des infrastructures numériques critiques, des données et de l'autonomie stratégique. La souveraineté englobe à la fois les intérêts nationaux en matière de sécurité et la capacité collective de l'UE à définir ses propres orientations politiques à l'abri de toute domination extérieure. (3) Droits fondamentaux (et cohésion sociale) : Sauvegarde de la vie privée, de la liberté d'expression et d'autres droits légaux inscrits dans les traités et chartes de l'UE dans le domaine virtuel, y compris la garantie d'une participation égale à la société numérique. Nous supposons qu'une importance excessive accordée à une dimension a souvent des répercussions sur une autre.

Peut-on dès lors parler d'un trilemme de politique numérique auquel l'UE est confrontée aujourd'hui ? En général, de nombreux compromis politiques du monde réel se manifestent en termes de paires. Dans le contexte macroéconomique, un trilemme apparaît lorsqu'il est *structurellement* impossible de poursuivre simultanément les trois objectifs. Dans notre contexte de politique numérique, nous

⁵ Hélène Rey, "Dilemma Not Trilemma : The Global Financial Cycle and Monetary Policy Independence" (Cambridge, MA : National Bureau of Economic Research, mai 2015), <https://doi.org/10.3386/w21162>.

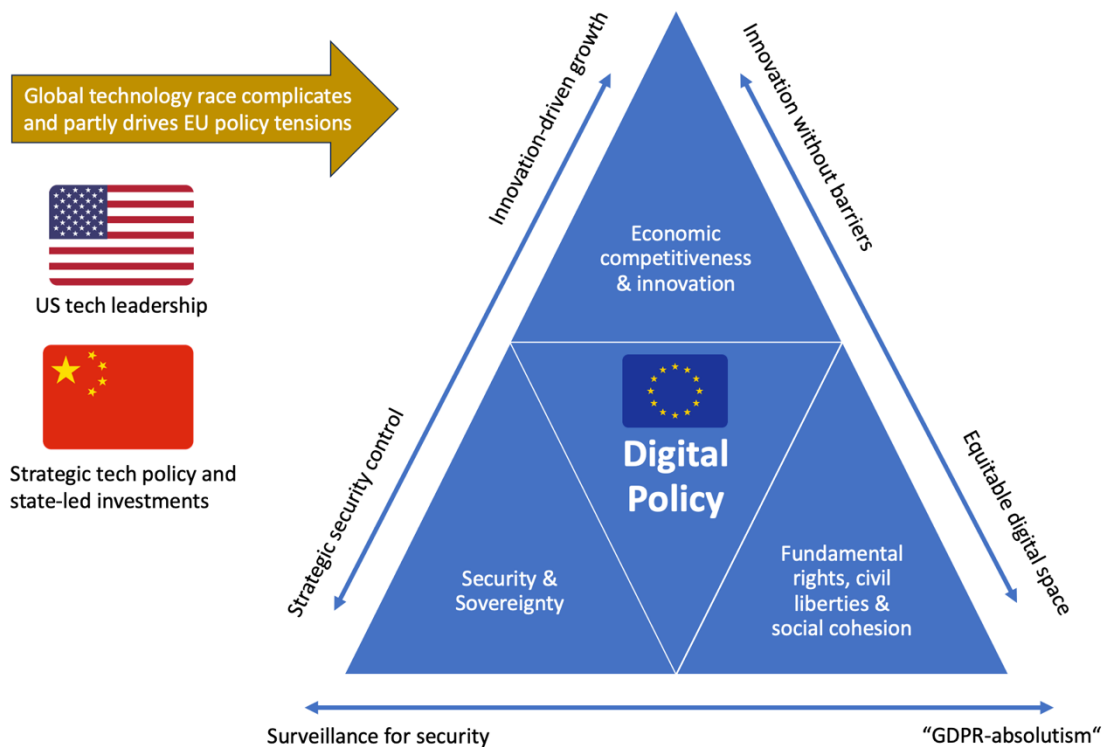
⁶ José Ignacio Torreblanca et Giorgos Verdi, "Innovate, Protect, and Influence : The EU's Technology Trilemma and How to Solve It", *Conseil européen des relations étrangères*, juin 2024, <https://ecfr.eu/article/innovate-protect-and-influence-the-eu-technology-trilemma-and-how-to-solve-it/>.

⁷ Pour les compromis entre la concurrence et l'innovation sur les marchés numériques, voir : Avi Goldfarb et Catherine Tucker, "Digital Economics", *Journal of Economic Literature* 57, no 1 (1er mars 2019) : 3–43, <https://doi.org/10.1257/jel.20171452>. Pour les compromis autour de la vie privée, de la concurrence et de l'innovation, voir : Alessandro Acquisti, Curtis Taylor et Liad Wagman, "The Economics of Privacy", *Journal of Economic Literature* 54, no 2 (1er juin 2016) : 442–92, <https://doi.org/10.1257/jel.54.2.442>. Pour les compromis dans la gouvernance de l'IA, voir : Luciano Floridi, "The Fight for Digital Sovereignty : What It Is, and Why It Matters, Especially for the EU", *Philosophy & Technology* 33, no. 3 (1er septembre 2020) : 369–78, <https://doi.org/10.1007/s13347-020-00423-6>.

soutenons plutôt que l'intensification d'un objectif (par exemple, l'augmentation de la compétitivité économique à tout prix) tend à créer des tensions avec au moins l'un des deux autres (sécurité/souveraineté ou droits fondamentaux). Au fil du temps, un décideur politique qui tente de préserver une souveraineté et des droits fondamentaux forts tout en poussant à une compétitivité maximale est susceptible d'être limité dans au moins un domaine. Contrairement à la "trinité impossible" classique, où le choix entre deux objectifs macroéconomiques sacrifie inévitablement le troisième, nous utilisons le terme "trilemme" dans un sens plus *heuristique* : l'interaction entre les trois objectifs peut devenir si contraignante que le fait de donner la priorité à un ou deux objectifs rend plus difficile la pleine réalisation du troisième. Bien qu'une appellation plus précise sur le plan technique puisse être un triangle à trois objectifs présentant de multiples compromis bilatéraux (figure 1), l'idée principale demeure : Les responsables de la politique numérique de l'UE doivent reconnaître que les efforts déployés pour soutenir un objectif peuvent limiter les autres et que le fait de donner la priorité à deux objectifs impose souvent des contraintes au troisième, en particulier dans le contexte d'une course mondiale à la technologie. En ce sens, la pression externe générée par le leadership technologique des États-Unis pourrait être considérée comme un facteur externe qui lie davantage ce qui pourrait autrement apparaître comme des compromis distincts par paires.

On peut donc se demander si le "trilemme" de l'UE n'est pas simplement dû au fait que d'autres juridictions, notamment les États-Unis, ont choisi un équilibre différent entre ces trois objectifs. Bien entendu, les défis de l'UE en matière de politique numérique n'existent pas dans le vide et sont façonnés par des facteurs externes tels que la suprématie technologique des États-Unis et le rôle croissant de la Chine, que nous examinons tous deux ci-dessous. Les décisions prises dans des juridictions dotées de vastes marchés intérieurs et/ou de "champions numériques" mondiaux limitent la marge de manœuvre de l'UE si elle veut rester compétitive. Cependant, nous soulignons également que, dans une large mesure, le cadre politique de l'UE découle de ses valeurs fondamentales et des engagements du traité, qui mettent l'accent sur les droits fondamentaux, la cohésion sociale et l'intégration du marché en tant que principes de base. Ainsi, la forme spécifique du trilemme de la politique numérique de l'UE reflète en partie les différentes priorités sociétales et juridiques, mais elle est également influencée par la réalité du leadership du marché américain dans des technologies telles que l'IA, les médias sociaux et l'informatique en nuage (dont la future présidence Trump 2.0 est clairement consciente et qu'elle cherche à exploiter). Ce dernier aspect du trilemme implique que les Européens ne sont tout simplement pas toujours libres de choisir pleinement en fonction de leurs préférences sociétales, un problème qui peut également se poser dans d'autres domaines de l'élaboration des politiques.

Fig.1 : Trilemme généralisé dans l'élaboration de la politique numérique de l'UE



Source : Illustration personnelle.

Pour illustrer notre triangle à trois objectifs, qui présente de multiples compromis bilatéraux, examinons tour à tour chaque côté du "trilemme" (figure 1). Tout d'abord, la relation entre la compétitivité économique (et l'innovation) et la sécurité (et la souveraineté) illustre la première dimension du trilemme de l'UE. D'une part, les politiques visant à promouvoir la compétitivité donnent souvent la priorité à la création d'un environnement propice à l'expansion des entreprises et au progrès technologique. Cette approche implique généralement la réduction des charges réglementaires afin de permettre aux entreprises d'innover librement et d'être compétitives au niveau mondial. Toutefois, cela peut involontairement créer des vulnérabilités en matière de sécurité, par exemple si cela n'est pas soigneusement équilibré avec des normes de cybersécurité ou des considérations sur les dépendances de la chaîne d'approvisionnement. À l'inverse, l'accent mis sur la sécurité et la souveraineté peut conduire à la mise en œuvre de mesures strictes de cybersécurité et de protocoles de protection des données pour se prémunir contre l'influence étrangère et protéger les infrastructures critiques. Si ces mesures renforcent la sécurité, elles augmentent également les coûts de mise en conformité pour les entreprises et restreignent les flux de données, ce qui pourrait entraver la croissance des entreprises basées dans l'UE, tirée par l'IA. Des politiques plus strictes réglementant les mouvements transfrontaliers et l'utilisation nationale des données électroniques entravent considérablement les performances des entreprises dépendantes des données, avec des effets plus marqués dans les pays dotés de réseaux technologiques avancés et pour les entreprises de services.⁸

Un autre aspect critique du trilemme est l'interaction entre la sécurité et les droits fondamentaux. Bien que l'UE ait progressivement intégré les droits fondamentaux dans ses lois et ses politiques, il lui

⁸ Martina Ferracane, Janez Kren et Erik Van Der Marel, "Do Data Policy Restrictions Impact the Productivity Performance of Firms and Industries", *SSRN Electronic Journal*, 2019, <https://doi.org/10.2139/ssrn.3384004>.

manque un cadre cohérent () pour rendre ces avantages plus apparents aux yeux du public.⁹ En outre, des négociations sont en cours sur la répartition des tâches judiciaires entre les tribunaux nationaux et ceux de l'UE en ce qui concerne l'interprétation et l'application des droits fondamentaux.¹⁰ Enfin, les gouvernements qui cherchent à renforcer la sécurité et la souveraineté introduisent souvent des mesures telles que des exigences en matière de surveillance ou de localisation des données afin de contrôler plus efficacement les activités numériques.¹¹ Si ces mesures peuvent renforcer la sécurité, elles se font souvent au détriment de la vie privée, ce qui peut saper la confiance du public. Toutefois, ce compromis peut dépendre du point de vue de chacun. D'un point de vue extérieur, la souveraineté de l'UE - en particulier vis-à-vis d'acteurs tels que les États-Unis ou la Chine - peut être conciliée avec la protection de la vie privée dans des cadres tels que le GDPR. Par exemple, le fait de s'assurer que les données des citoyens européens sont stockées au sein de l'UE renforce à la fois la protection de la vie privée et la souveraineté en permettant aux États membres de mettre en œuvre une vision collective à l'abri de toute influence extérieure. Toutefois, d'un point de vue interne, l'accent mis sur la surveillance pour la sécurité nationale peut en fait entrer en conflit avec une sorte d'"absolutisme du GDPR", car des lois strictes en matière de protection de la vie privée pourraient entraver le partage de données essentielles pour l'application de la loi. Les compromis entre la sécurité, la souveraineté et les droits fondamentaux ne sont donc pas absolus, mais façonnés par des priorités géopolitiques et nationales plus larges.

La dernière dimension du trilemme est la tension entre les droits/règles et la compétitivité. Lorsque la croissance économique et l'innovation priment, les politiques tendent à favoriser des contraintes réglementaires minimales, ce qui permet des progrès technologiques rapides et des solutions rentables, tout en favorisant potentiellement les risques pour la vie privée ou les inégalités socio-économiques. À l'inverse, la priorité donnée aux droits fondamentaux met l'accent sur la création d'un espace numérique équitable, mais peut introduire des barrières réglementaires fortes qui affectent l'agilité des entreprises numériques. La théorie de Bradford sur "l'effet Bruxelles" explique comment les réglementations de l'UE influencent les marchés mondiaux tout en équilibrant la compétitivité et les principes de gouvernance éthique.¹² Dans le domaine des technologies, certains ont même affirmé que la capacité de l'UE à projeter son pouvoir ne découle pas seulement de la taille de son marché, mais aussi de son processus consensuel et inclusif d'élaboration des politiques, qui garantit la sécurité juridique et la crédibilité, influençant ainsi d'autres États à adopter les normes élevées de l'UE en matière de réglementation.¹³ Récemment, cependant, certains ont mis en garde contre le risque d'érosion progressive de l'effet Bruxelles dans les années à venir, notamment en raison de l'évolution de la géopolitique.¹⁴ Même dans le cas de l'ASD et de la loi sur l'IA, largement citées, M. Šonková constate qu'il y a des

⁹ Israel Butler, "A Fundamental Rights Strategy for the European Union" (Open Society Foundations, 2014), JSTOR, <http://www.jstor.org/stable/resrep43002>.

¹⁰ Aida Torres Pérez, "La force fédéralisante de la Charte des droits fondamentaux de l'UE", *Revue internationale de droit constitutionnel* 15, no. 4 (3 novembre 2017) : 1080–97, <https://doi.org/10.1093/icon/mox075>.

¹¹ Rocco Bellanova, Helena Carrapico et Denis Duez, "Digital/Sovereignty and European Security Integration : An Introduction", *European Security* 31, no. 3 (3 juillet 2022) : 337–55, <https://doi.org/10.1080/09662839.2022.2101887>.

¹² Anu Bradford, *The Brussels Effect : How the European Union Rules the World* (New York : Oxford University Press, 2020).

¹³ Annegret Bendiek et Isabella Stuerzer, "The Brussels Effect, European Regulatory Power and Political Capital : Evidence for Mutually Reinforcing Internal and External Dimensions of the Brussels Effect from the European Digital Policy Debate", *Digital Society* 2, no. 1 (avril 2023) : 5, <https://doi.org/10.1007/s44206-022-00031-1>.

¹⁴ Andrea Renda, "Leveraging Digital Regulation for Strategic Autonomy", mars 2022, <https://feps-europe.eu/publication/853-leveraging-digital-regulation-for-strategic-autonomy/>.

limites à la réalisation de l'effet Bruxelles.¹⁵ Pour répondre à cette tension, l'UE a récemment cherché à affiner sa stratégie réglementaire par le biais de plusieurs mécanismes, notamment : le principe d'innovation, qui vise à garantir que les nouvelles politiques tiennent compte de leur impact potentiel sur l'innovation ; la budgétisation réglementaire, un système de plafonnement ou de compensation des coûts réglementaires visant à minimiser les charges inutiles sur les entreprises ; et l'introduction de bacs à sable réglementaires, c'est-à-dire d'environnements contrôlés qui permettent aux entreprises de tester des technologies ou des modèles d'entreprise sous surveillance réglementaire.¹⁶

Il est essentiel d'ignorer ces compromis, car cela comporte des risques importants. Si l'on ne reconnaît pas les tensions inhérentes décrites dans notre trilemme, les politiques numériques de l'UE peuvent devenir incohérentes, se contredire et aboutir à des résultats inefficaces, voire contre-productifs. Ces types de contraintes dues à des objectifs contradictoires ont affecté non seulement l'approche de l'UE en matière de gouvernance de l'internet¹⁷ et l'élaboration de règles en matière de cybersécurité,¹⁸ mais aussi des domaines politiques non numériques tels que la politique de voisinage.¹⁹ Un exemple récent de cet équilibre délicat est l'élaboration de la loi sur les marchés numériques (DMA), où les idées économiques concurrentes des acteurs politiques, à savoir les "correcteurs de marché", les "destructeurs de marché" et les "directeurs de marché", se sont contrecarrées les unes les autres.²⁰ En outre, en se concentrant sur un seul aspect, l'UE risque de réduire sa capacité à façonner les normes et standards numériques mondiaux par le biais d'une stratégie globale plus holistique, cédant ainsi le leadership à d'autres acteurs géopolitiquement stratégiques ayant une vision à plus long terme, tels que la Chine.

Alors que l'UE est aux prises avec le trilemme de sa politique numérique, il est important de noter que d'autres acteurs mondiaux majeurs sont confrontés à leurs propres compromis complexes en matière de réglementation de la sphère numérique. En Chine, le paysage réglementaire ressemble, selon Zhang, à un numéro de haute voltige caractérisé par la hiérarchie, la volatilité et la fragilité.²¹ Cette analogie illustre bien l'équilibre que les régulateurs chinois doivent maintenir entre la promotion de l'innovation, l'affirmation du contrôle de l'État et la gestion de la stabilité sociale. La nature hiérarchique du système réglementaire chinois signifie que les décisions sont souvent prises en cascade par le sommet, ce qui entraîne des changements rapides de politique. Cette volatilité peut créer de l'incertitude pour les entreprises, mais elle permet aussi une adaptation rapide aux nouveaux défis, affirme

¹⁵ Markéta Šonková, "Brussels Effect Reloaded ? The European Union's Digital Services Act and the Artificial Intelligence Act", EU Diplomacy Papers (Collège d'Europe, Département des relations internationales et des études diplomatiques de l'UE, avril 2024), https://www.coleurope.eu/sites/default/files/research-paper/EDP_4_24%20Sonkova.pdf.

¹⁶ Andrea Renda et Jacques Pelkmans, "EU Regulation : Hindering or Stimulating Innovation ?", dans *Handbook of Innovation and Regulation*, ed. Pontus Braunerhjelm et al. (Edward Elgar Publishing, 2023), 263-93, <https://doi.org/10.4337/9781800884472.00021>.

¹⁷ George Christou et Seamus Simpson, "The European Union, Multilateralism and the Global Governance of the Internet", *Journal of European Public Policy* 18, no. 2 (mars 2011) : 241-57, <https://doi.org/10.1080/13501763.2011.544505>.

¹⁸ Helena Carrapico et André Barrinha, "The EU as a Coherent (Cyber)Security Actor ? ", *JCMS : Journal of Common Market Studies* 55, no 6 (novembre 2017) : 1254-72, <https://doi.org/10.1111/jcms.12575> ; Elaine Fahey, "The EU's Cybercrime and Cyber-Security Rulemaking : Mapping the Internal and External Dimensions of EU Security", *European Journal of Risk Regulation* 5, no 1 (mars 2014) : 46-60, <https://doi.org/10.1017/S1867299X00002944>.

¹⁹ Tanja A. Börzel et Vera Van Hüllen, "One Voice, One Message, but Conflicting Goals : Cohesiveness and Consistency in the European Neighbourhood Policy", *Journal of European Public Policy* 21, no. 7 (9 août 2014) : 1033-49, <https://doi.org/10.1080/13501763.2014.912147>.

²⁰ Catherine Hoeffler et Frédéric Mérand, "Digital Sovereignty, Economic Ideas, and the Struggle over the Digital Markets Act : A Political-Cultural Approach", *Journal of European Public Policy*, 22 décembre 2023, 1-26, <https://doi.org/10.1080/13501763.2023.2294144>.

²¹ Huyue Zhang, *High Wire : How China Regulates Big Tech and Governs Its Economy*, Oxford Scholarship Online Political Science (New York, NY : Oxford University Press, 2024), <https://doi.org/10.1093/oso/9780197682258.001.0001>.

M. Zhang. Toutefois, la fragilité du système devient évidente lorsque des priorités contradictoires apparaissent. Contrairement au trilemme de l'UE, les compromis chinois privilégient souvent le contrôle de l'État et la croissance économique par rapport aux droits individuels. C'est ce qui ressort, par exemple, de la façon dont la Chine a transformé l'antitrust en une arme économique puissante, l'utilisant stratégiquement pour contrer les sanctions américaines et faire basculer le paysage concurrentiel en faveur des entreprises nationales, tout en l'utilisant également comme un instrument de politique commerciale et étrangère.²²

En revanche, les États-Unis ont un paysage réglementaire tout aussi fragmenté, voire plus, avec des divergences importantes entre les approches fédérales et étatiques en matière de politique numérique. Ce système décentralisé permet une expérimentation et une flexibilité accrues, comme en témoigne la position proactive de la Californie en matière de réglementation de l'IA. Les mesures de responsabilisation et les exigences de transparence proposées par l'État en matière d'IA () montrent comment les États peuvent servir de laboratoires pour l'innovation politique. Toutefois, cette approche disparate pose également des problèmes aux entreprises qui exercent leurs activités au-delà des frontières des États et peut entraîner des incohérences dans les normes de protection des consommateurs et de la vie privée. Plus généralement, l'approche américaine du trilemme tend souvent à privilégier la sécurité par rapport à la protection de la vie privée, comme en témoigne la législation fédérale telle que le Patriot Act, qui a renforcé les capacités d'application de la loi et les efforts de lutte contre le terrorisme au détriment d'une protection solide de la vie privée et d'une gouvernance numérique cohérente. Cette priorité donnée à la sécurité et à la compétitivité laisse des lacunes dans l'uniformité des normes de protection de la vie privée que les États doivent tenter de combler. Par conséquent, le modèle américain illustre un ensemble différent de compromis, où l'équilibre entre sécurité et vie privée penche en faveur de la première, en fonction des impératifs fédéraux et de l'innovation au niveau de l'État.

Contrairement à la Chine et aux États-Unis, l'approche de l'UE en tant qu'acteur numérique mondial se distingue par sa structure politique, ses objectifs économiques et son cadre juridique uniques.²³ En tant qu'entité supranationale, l'UE doit équilibrer les intérêts de plusieurs États membres tout en s'efforçant de créer un marché numérique cohérent, ce qui devient encore plus difficile en période de crises multiples et de votes populistes.²⁴ L'équilibre entre les relations verticales entre l'UE, ses États membres et les acteurs privés et les relations horizontales entre ses multiples institutions et agences nécessite une approche plus délibérative et consensuelle de l'élaboration des politiques, ce qui peut aboutir à une réglementation plus complète mais plus lente à mettre en œuvre. Sur le plan économique, l'UE vise à favoriser un écosystème numérique compétitif tout en maintenant son modèle d'"économie sociale de marché", ce qui se traduit par des politiques qui cherchent à équilibrer les intérêts des entreprises avec une forte protection des consommateurs et des travailleurs. Sur le plan juridique, l'engagement de l'UE en faveur des droits fondamentaux, tels qu'ils sont inscrits dans la Charte des droits fondamentaux, donne la priorité à la protection de la vie privée et des données, en

²² Angela Huyue Zhang, *Chinese Antitrust Exceptionalism : How the Rise of China Challenges Global Regulation* (New York : Oxford University Press, 2021).

²³ Elaine Fahey, *The EU as a Global Digital Actor : Institutionalising Global Data Protection, Trade, and Cybersecurity*, *Modern Studies in European Law*, volume 111 (Oxford ; New York : Hart, 2022).

²⁴ Frank Schimmelfennig, " L'intégration européenne (théorie) en temps de crise. A Comparison of the Euro and Schengen Crises", *Journal of European Public Policy* 25, no 7 (3 juillet 2018) : 969-89, <https://doi.org/10.1080/13501763.2017.1421252> ; Andreas C. Goldberg, Erika J. Van Elsas, et Claes H. De Vreese, "The Differential Impact of EU Attitudes on Voting Behaviour in the European Parliamentary Elections 2019", *Journal of Contemporary European Studies* 32, no. 4 (octobre 2024) : 1323-42, <https://doi.org/10.1080/14782804.2024.2356643>.

particulier par rapport à d'autres régions.²⁵ Cette combinaison de facteurs se traduit par une approche réglementaire qui doit être prudente dans le traitement du trilemme de la politique numérique, comme nous le montrerons dans la section suivante.

3 Études de cas individuels

La réglementation peut généralement être considérée comme une décision politique visant à équilibrer les compromis. Comme nous l'avons supposé dans la section précédente, l'élaboration de la politique numérique de l'UE comporte de nombreux compromis de ce type qui, s'ils ne sont pas reconnus, peuvent conduire à des politiques qui vont à l'encontre de leurs propres objectifs. Pour illustrer et disséquer ce "trilemme", cette section analyse les compromis et les risques associés pour six études de cas spécifiques : vie privée contre innovation dans la protection des données en Europe, réglementation contre liberté d'expression dans la modération des plateformes, risques de cybersécurité et incitations économiques dans le développement des TIC en Europe, éthique contre compétitivité dans la réglementation de l'IA, autonomie stratégique contre coopération dans le développement de l'infrastructure informatique, et bien-être des consommateurs contre intérêts publics plus larges dans la politique de la concurrence de l'UE.²⁶ L'objectif est de voir s'il existe des parallèles structurels entre ces compromis dans différents sous-domaines de la politique numérique de l'UE, ou si les compromis prennent une forme spécifique (et si c'est le cas, quels en sont les facteurs).

3.1 Protection des données : Vie privée contre innovation

Le règlement général sur la protection des données (RGPD) est un texte historique de la législation de l'UE en matière de protection de la vie privée, qui a des implications considérables pour les entreprises du monde entier.²⁷ Mis en œuvre en mai 2018, le GDPR vise à renforcer les droits individuels en matière de données et à harmoniser les réglementations en matière de protection de la vie privée dans l'ensemble de l'UE. Si le règlement a été salué pour l'amélioration de la protection de la vie privée des consommateurs, il a suscité un débat intense quant à son impact sur l'innovation et la compétitivité des entreprises, en particulier pour les petites entreprises et les start-ups. Le GDPR impose des exigences strictes sur la manière dont les entreprises collectent, traitent et stockent les données personnelles, ce qui nécessite des changements opérationnels et des investissements de mise en conformité pour de nombreuses organisations. En conséquence, plusieurs compromis entre la protection de la vie privée et les processus économiques liés à l'innovation technologique sont devenus visibles.

Tout d'abord, le GDPR fonctionne selon un cadre réglementaire à multiples facettes qui combine des éléments de commandement et de contrôle, de conception et de méta-réglementation, comme le souligne une étude récente de Martínez.²⁸ Cette approche crée un système dynamique dans lequel les responsables du traitement des données doivent non seulement se conformer à des règles spécifiques, mais aussi s'engager dans une évaluation et une gestion continues des risques. En particulier, l'approche fondée sur les risques du règlement exige des organisations qu'elles évaluent la nature, la portée et le contexte du traitement des données, en tenant compte de l'impact potentiel sur les droits fondamentaux au-delà de la vie privée. Cette complexité est aggravée par les principes de protection

²⁵ Torres Pérez, "La force fédéralisante de la Charte des droits fondamentaux de l'UE".

²⁶ Pour une approche similaire de l'étude de cas, voir : Renda et Pelkmans, "EU Regulation".

²⁷ Bradford, *L'effet Bruxelles*.

²⁸ Alba Ribera Martínez, "Ultra Vires Compliance as a GDPR Harm" (novembre 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5008314.

de la vie privée dès la conception et par défaut du GDPR, qui exigent l'intégration de mesures de protection de la vie privée tout au long du cycle de vie des technologies et des applications.

En conséquence, la mise en œuvre de la conformité au GDPR (de la part des entreprises) n'est pas un processus simple, car elle implique de traiter un spectre de modalités réglementaires. Les "responsables du traitement" doivent justifier leurs activités de traitement sur au moins une base juridique, tout en intégrant les principes du GDPR dans leurs processus techniques et organisationnels. Le principe de la protection des données dès la conception, par exemple, exige d'anticiper les risques potentiels en matière de protection des données dès les premières étapes du développement d'un produit. Cette approche proactive vise à intégrer les considérations relatives à la protection de la vie privée au cœur de l'innovation technologique, plutôt que de les traiter après coup. Toutefois, M. Martínez estime que cette complexité peut conduire à des interprétations et à des mises en œuvre différentes des exigences du GDPR, ce qui peut donner lieu à des scénarios de sous-conformité et de surconformité.²⁹ Dans certains cas, il peut y avoir surconformité ou "conformité ultra vires", lorsque les entreprises mettent en œuvre des mesures qui vont au-delà des exigences réelles du GDPR.³⁰ Il est clair que des restrictions inutiles sur les activités de traitement des données limitent le développement de technologies et de services basés sur les données. Plus généralement, l'accent mis par le règlement sur l'évaluation et la gestion globales des risques impose des charges importantes aux organisations. Par conséquent, les compromis réalisés en faveur de l'aversion au risque lors de l'élaboration du GDPR pourraient avoir des conséquences inattendues sur la croissance économique et le progrès technologique dans l'UE.

Après avoir abordé la théorie juridique, quelles sont les preuves que cette complexité juridique et la priorité donnée à l'aversion pour le risque par rapport aux impératifs économiques ont entraîné des désavantages économiques ? En analysant un large échantillon d'entreprises réparties dans 61 pays et 34 secteurs d'activité, Frey et Presidente ont constaté que les entreprises exposées aux marchés de l'UE ont subi une baisse moyenne de 8 % de leurs bénéfices et de 2 % de leurs ventes à la suite de l'application du GDPR.³¹ L'impact négatif a été particulièrement prononcé pour les petites entreprises technologiques, qui ont connu une baisse moyenne de leurs bénéfices presque deux fois plus importante. En revanche, les grandes entreprises technologiques ont semblé relativement épargnées, ce qui laisse à penser que le règlement pourrait, par inadvertance, favoriser les géants technologiques établis au détriment de leurs concurrents plus petits. La recherche menée par Peukert et al. apporte un éclairage supplémentaire sur la manière dont le GDPR a remodelé l'écosystème numérique.³² En suivant plus de 110 000 sites web, l'étude a révélé une réduction significative des connexions aux fournisseurs de technologie web après le GDPR. Parallèlement, ils ont observé une augmentation de la concentration du marché des services de technologie web.

En se concentrant sur les résultats de l'innovation, Blind, Niebel et Rammer ont examiné l'impact du GDPR sur l'innovation de produit parmi les entreprises allemandes.³³ Leur analyse a révélé un passage

²⁹ Ribera Martínez.

³⁰ Ribera Martínez.

³¹ Carl Benedikt Frey et Giorgio Presidente, "Privacy Regulation and Firm Performance : Estimating the GDPR Effect Globally", *Economic Inquiry* 62, no. 3 (juillet 2024) : 1074–89, <https://doi.org/10.1111/ecin.13213>.

³² Christian Peukert et al, "European Privacy Law and Global Markets for Data", CEPR Discussion Paper (Londres : Centre for Economic Policy Research, 2020), <https://cepr.org/publications/dp14475>.

³³ Knut Blind, Crispin Niebel et Christian Rammer, " The Impact of the EU General Data Protection Regulation on Product Innovation ", *Industry and Innovation* 31, no. 3 (15 mars 2024) : 311–51, <https://doi.org/10.1080/13662716.2023.2271858>.

significatif de l'innovation radicale à l'innovation incrémentale à la suite de la mise en œuvre du règlement. L'innovation radicale fait référence au développement de produits entièrement nouveaux qui s'écartent considérablement des offres existantes, créant généralement de nouveaux marchés ou perturbant les marchés existants. En revanche, l'innovation incrémentale implique des améliorations ou des adaptations modestes des produits existants, c'est-à-dire qu'elle se contente d'améliorer leurs caractéristiques ou leurs performances. Les chercheurs notent également que les efforts de mise en conformité avec le GDPR ont incité les entreprises à réorganiser fondamentalement leurs pratiques de gestion des données. Les ressources nécessaires pour se conformer au règlement semblent avoir limité la capacité des entreprises à développer des produits entièrement nouveaux, ce qui pourrait entraver l'innovation perturbatrice dont l'Europe a un besoin urgent au cours de sa double transition.

Une étude récente de Demirer et al. donne un aperçu détaillé de la manière dont le GDPR a modifié les processus de production réels des entreprises.³⁴ En réponse au GDPR, les entreprises de l'UE ont réduit le stockage des données de 26 % et le traitement des données de 15 % par rapport aux entreprises américaines similaires, devenant ainsi moins "intensives en données" et donc moins prêtes à capitaliser sur les innovations en matière d'IA. En estimant une fonction de production avec des données et des calculs comme intrants, l'étude a estimé que le GDPR a effectivement augmenté les coûts des données de 20 % en moyenne pour les entreprises touchées. Toutefois, l'impact variait considérablement d'un secteur à l'autre et d'une entreprise à l'autre, ce qui montre que la forme concrète de l'arbitrage entre la protection des données et l'innovation basée sur les données peut varier en fonction des marchés concernés et des caractéristiques de chaque entreprise.

Quelle est la situation générale ? Après plusieurs années, des preuves empiriques commencent à émerger selon lesquelles le GDPR a eu un impact profond sur les opérations commerciales dans l'UE, les trajectoires d'innovation et la dynamique concurrentielle dans l'économie numérique. Tout en renforçant la protection de la vie privée, le règlement a imposé une incertitude juridique et des coûts de mise en conformité importants, ce qui est particulièrement difficile pour les PME et a accéléré les tendances à la consolidation et à la concentration du marché entre les mains des Big Tech américaines. En particulier, l'évolution observée vers l'innovation incrémentale et la réduction de l'intensité des données dans les entreprises de l'UE soulève des inquiétudes quant aux impacts potentiels à long terme sur le progrès technologique et la compétitivité. Toutefois, le GDPR a également incité les entreprises à réévaluer et à améliorer leurs pratiques de gestion des données, ce qui peut être bénéfique en termes de qualité des données et de confiance des consommateurs.

3.2 Modération des plateformes : Réglementation vs. liberté d'expression, compétitivité et sécurité

Depuis le début de l'année 2024, la loi sur les services numériques (DSA) s'applique pleinement aux services tels que les moteurs de recherche, les places de marché en ligne, les plateformes de médias sociaux et les applications vidéo, que des millions de personnes utilisent quotidiennement dans l'UE. La loi sur les services numériques vise à créer un environnement numérique plus sûr pour les citoyens de l'UE et les autres personnes. Dans le même temps, elle vise à préserver le marché intérieur en évitant la fragmentation qui pourrait résulter de réglementations nationales divergentes couvrant "les exigences de diligence applicables aux prestataires de services intermédiaires en ce qui concerne la

³⁴ Mert Demirer et al, "Data, Privacy Laws and Firm Production : Evidence from the GDPR" (Cambridge, MA : National Bureau of Economic Research, février 2024), <https://doi.org/10.3386/w32146>.

manière dont ils doivent s'attaquer aux contenus illicites, à la désinformation en ligne ou à d'autres risques sociétaux".³⁵ En pratique, l'ASD définit de nouvelles obligations pour les entreprises numériques, y compris les géants des médias sociaux tels que Facebook, Instagram, X et TikTok. Bien qu'elles ne soient pas considérées comme responsables du contenu qu'elles publient, elles doivent désormais supporter les coûts liés à la transparence, à la modération du contenu et au respect d'impératifs clés liés au risque, tels que l'abstention de pratiques trompeuses et la garantie d'un niveau élevé de protection de la vie privée, de la sécurité et de la sûreté des mineurs. Ils s'exposent également à des amendes s'ils ne respectent pas leurs obligations telles qu'elles sont définies dans l'ASD.

En appliquant notre trilemme au cas de l'ASD, il devient clair que, indépendamment de toutes les questions qui entourent inévitablement ce type de réglementation pionnière et son sujet en évolution rapide, au moins trois compromis potentiels sont en effet impliqués, selon le point de vue que l'on adopte : comme expliqué plus en détail ci-dessous, il y a 1) un compromis potentiel entre l'objectif de créer un environnement numérique sûr et sécurisé et les droits individuels et les libertés civiles, en particulier la liberté d'expression ; 2) un compromis potentiel entre la compétitivité des plates-formes en ligne et la protection des droits individuels et des libertés civiles ; et 3) un compromis potentiel entre la compétitivité des plates-formes en ligne et l'objectif de créer un environnement numérique sûr et sécurisé.

La définition du "risque systémique" posé par les "très grandes plateformes en ligne" (VLOP) et les "très grands moteurs de recherche en ligne" (VLOSE) est une question importante. Ce risque est principalement défini par la portée du fournisseur, en particulier lorsqu'il dépasse un seuil opérationnel de 45 millions d'utilisateurs, ce qui équivaut à 10 % de la population de l'UE. L'ASD mentionne ensuite spécifiquement quatre catégories de risques : 1) les risques liés à la diffusion de contenus illicites, tels que des contenus pédopornographiques ou des discours haineux illégaux ; 2) l'impact réel ou prévisible du service sur l'exercice des droits fondamentaux, y compris la liberté d'expression ; 3) les risques liés aux effets négatifs sur les processus démocratiques, les processus électoraux, la sécurité publique ; 4) les risques liés à la conception, au fonctionnement ou à l'utilisation, y compris par la manipulation, de VLOP et VLOSE, qui peuvent avoir un impact négatif sur la protection de la santé publique, des mineurs et des conséquences négatives graves sur le bien-être physique et mental d'une personne, ou sur la violence fondée sur le genre. En résumé, le législateur européen précise clairement la justification, en termes de risques sociétaux, de la réglementation de l'activité du VLOP et du VLOSE.

Un rôle clé dans la mise en œuvre de l'ASN est attribué aux "signaleurs de confiance", des entités non gouvernementales désignées par les coordinateurs nationaux des services numériques et chargées de détecter les contenus potentiellement illicites et d'alerter les plateformes en ligne. Selon l'ASN, les plateformes en ligne doivent traiter en priorité les signalements de contenu suspecté d'être illégal effectués par les signaleurs de confiance. En effet, l'implication des acteurs non gouvernementaux est un exemple de la manière dont l'ASN ne renforce pas seulement les institutions étatiques vis-à-vis des acteurs privés, mais aussi la société civile et les individus vis-à-vis des acteurs privés.³⁶ Deux articles juridiques récents offrent des perspectives contrastées sur le rôle des signaleurs de confiance, soulignant les compromis entre la sécurité, les droits fondamentaux et la compétitivité économique. Ruschmeier adopte un point de vue généralement positif sur le système des signaleurs de confiance, car

³⁵ RÈGLEMENT (UE) 2022/2065 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 19 octobre 2022 sur un marché unique des services numériques et modifiant la directive 2000/31/CE (loi sur les services numériques), <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>.

³⁶ Martin Husovec, *Principes de la loi sur les services numériques*. Oxford : Oxford University Press (2024).

ils contribuent à "l'hygiène de la démocratie" en aidant à identifier et à signaler les contenus illégaux en ligne.³⁷ Elle soutient que l'ASD crée des lignes directrices claires pour les signaleurs de confiance et des procédures transparentes qui peuvent aider à équilibrer le besoin de modération du contenu avec la protection de la liberté d'expression, car les signaleurs de confiance ne prennent pas eux-mêmes les décisions de suppression de contenu. En revanche, M. Lindner estime que le système des signaleurs de confiance présente des risques structurels pour la liberté d'expression.³⁸ Il soutient que les signaleurs de confiance peuvent ne pas avoir l'expertise juridique nécessaire pour déterminer avec précision quel contenu est illégal, ce qui pourrait conduire à la suppression d'un discours légal. Il s'inquiète du manque de transparence du processus de signalement et de l'effet dissuasif qu'il pourrait avoir sur le discours en ligne. Ces deux points de vue juridiques opposés, chacun avec ses propres mérites, illustrent l'équilibre délicat que l'ASD cherche à trouver entre la sécurité et les droits fondamentaux (le premier compromis mentionné ci-dessus) : D'une part, le système de signaleurs de confiance vise à améliorer l'efficacité de la modération des contenus et à protéger les utilisateurs contre les contenus illicites, conformément aux objectifs de l'UE en matière de sécurité et de souveraineté numériques. D'autre part, il existe des inquiétudes légitimes quant aux risques d'ingérence et à l'impact sur la liberté d'expression, qui est un droit fondamental.

Outre les arguments juridiques, il est important de noter qu'en raison de l'absence d'incitations financières à se porter candidat, le nombre de signaleurs de confiance est actuellement très faible.³⁹ Dans ce contexte, il convient également de rappeler que l'ASD prévoit des recours pour les situations qui pourraient être qualifiées de "réaction excessive" ou de "censure excessive", c'est-à-dire les cas dans lesquels un contenu publié est retiré après avoir été considéré à tort comme illégal par un fournisseur. Dans ce qui peut être considéré comme un exercice d'équilibre, l'ASD fait référence à plusieurs reprises à la nécessité de protéger l'exercice des droits fondamentaux consacrés par la Charte des droits fondamentaux de l'Union européenne. En cas de réaction excessive, les utilisateurs disposent de trois options : 1) des systèmes de plainte internes (article 20), que les plateformes doivent fournir et qui doivent être accessibles, équitables et supervisés par du personnel qualifié, et qui permettent aux utilisateurs de contester les décisions de modération du contenu ; 2) la résolution extrajudiciaire des litiges (article 21), c'est-à-dire le recours à des mécanismes de résolution des litiges par l'intermédiaire d'organismes extrajudiciaires certifiés ; ou 3) la réparation judiciaire, c'est-à-dire le recours aux juridictions nationales.⁴⁰

L'aspect compétitivité économique de notre trilemme est également évident dans ce débat. Alors que l'ASD vise à créer un environnement numérique plus sûr susceptible de favoriser l'innovation, l'alourdissement des charges réglementaires pesant sur les plateformes pourrait y faire obstacle, qu'il s'agisse de trouver un équilibre entre la compétitivité et la réglementation des droits individuels, y compris la liberté d'expression, ou de trouver un équilibre entre la compétitivité et la modération des contenus en tant que moyen de créer un environnement numérique plus sûr (les deuxième et troisième compromis mentionnés plus haut).⁴¹ Les coûts associés à la mise en œuvre de systèmes robustes

³⁷ Hannah Ruschemeier, "Flagging Trusted Flaggers", 4 novembre 2024, <https://doi.org/10.59704/6c2c9f4cc624f31a>.

³⁸ Josef Franz Lindner, "Trusted Flagger Als Gefahr Für Die Meinungsfreiheit", 8 novembre 2024, <https://doi.org/10.59704/9460eb2652f47ea8>.

³⁹ Pour une liste des signaleurs de confiance actuellement reconnus, voir

⁴⁰ Voir Aleksandra Kuczerawy, *Remedying Overremoval : L'approche à trois niveaux de l'ASD*,

⁴¹ En effet, les considérations relatives à la sécurité "hors ligne" sont également pertinentes ici. Prenons par exemple le cas des émeutes d'extrême droite qui ont eu lieu au Royaume-Uni en août 2024 et qui ont été alimentées par des fausses nouvelles diffusées sur X (anciennement Twitter) (voir <https://www.politico.eu/article/united-kingdom-riots-elon-musk-x-twitter-fake-news-disinformation/>).

de modération de contenu et au respect de l'ASD peuvent être particulièrement difficiles à supporter pour les petites plateformes ou les nouveaux venus sur le marché. Au fur et à mesure de la mise en œuvre de l'ASN, les décideurs politiques doivent rester vigilants et évaluer si l'approche choisie répond effectivement à ces priorités concurrentes sans compromettre indûment l'un des aspects du trilemme de la politique numérique.

Il est intéressant de noter que les mêmes compromis entre l'atténuation des risques et des dommages, d'une part, et les droits fondamentaux et la liberté d'expression, d'autre part, seront également pertinents dans la loi sur l'IA, en particulier en ce qui concerne la réglementation des modèles d'IA à fort impact et à usage général. La loi sur l'IA, adoptée en juin 2024 et examinée plus en détail ci-dessous (voir section 3.4), exige des fournisseurs de ces modèles qu'ils atténuent les risques systémiques potentiels, ce qui fait écho à des obligations similaires dans l'ASD. La définition du risque systémique dans la loi sur l'IA est vague, englobant "les effets négatifs réels ou raisonnablement prévisibles sur la santé publique, la sécurité publique, les droits fondamentaux ou la société dans son ensemble". Comme l'ont fait valoir des organisations de la société civile, cette définition large pourrait conduire à une approche trop prudente de la part des fournisseurs d'IA, ce qui risquerait d'étouffer l'innovation et de limiter les capacités d'expression des systèmes d'IA.⁴² En outre, à l'instar de l'ASD, les dispositions de la loi sur l'IA relatives au risque systémique pour les modèles d'IA à usage général seront appliquées par la Commission européenne, c'est-à-dire par un organe politique. Cette disposition soulève des inquiétudes quant à la politisation potentielle des décisions d'application, comme on l'a vu lors de la mise en œuvre initiale de l'ASD par le commissaire Breton, qui a utilisé l'application politisée pour brouiller la distinction entre les informations illégales et la désinformation (autorisée).

3.3 Lignes directrices sur la cybersécurité : Sécurité et intérêts économiques

La boîte à outils de sécurité 5G de l'UE et, plus généralement, les plans ambitieux de l'UE sur l'infrastructure informatique et en nuage abordent les risques de cybersécurité. Toutefois, étant donné qu'ils mettent l'accent sur la fabrication nationale et la localisation des données, ils risquent également de peser sur les relations économiques avec les principaux fournisseurs de technologies et partenaires commerciaux tels que les États-Unis (pour le secteur du cloud, pensez à AWS) et la Chine (pour les équipements électroniques, pensez à Huawei), ce qui aurait un impact sur l'adoption rapide et rentable des technologies et, en cas de guerre commerciale, sur les secteurs d'exportation traditionnels du continent.

La boîte à outils de l'UE sur la cybersécurité de la 5G, publiée en janvier 2020, vise à traiter les risques de cybersécurité associés aux réseaux 5G. Il s'agit essentiellement d'un cadre stratégique adopté par l'UE pour faire face aux risques de sécurité lors du déploiement des réseaux 5G. Il a été élaboré par le groupe de coopération sur les réseaux et les systèmes d'information (NIS) sur la base de la directive NIS, qui vise à renforcer la cybersécurité dans l'ensemble de l'UE. La boîte à outils identifie les risques associés aux réseaux 5G, notamment en ce qui concerne la dépendance à l'égard de fournisseurs à haut risque tels que Huawei et ZTE, et propose des mesures pour atténuer ces risques.

La boîte à outils de l'UE n'est pas juridiquement contraignante pour les États membres, mais elle constitue un ensemble de lignes directrices que les États sont encouragés à mettre en œuvre volontairement. Les mesures s'appuient sur une approche fondée sur les risques, ce qui permet à chaque État

⁴² Calvet-Bademunt (2024), [Safeguarding Freedom of Expression in the AI Era | TechPolicy.Press](#).

membre de décider comment les intégrer dans son cadre national de cybersécurité. L'absence de force contraignante signifie que la mise en œuvre varie considérablement d'un État membre à l'autre, ce qui contribue à des progrès inégaux. Bien que la capacité de l'UE à faire appliquer les mesures de cybersécurité soit limitée par le principe de la souveraineté nationale en matière de sécurité, la Commission a activement poussé les États membres à adopter ses recommandations afin de garantir une approche coordonnée, en utilisant des incitations politiques et financières pour encourager l'alignement sur les lignes directrices de la boîte à outils. Faisant le point sur la situation trois ans après l'introduction de la boîte à outils,⁴³ la Commission a exprimé en 2023 une forte inquiétude concernant "les risques que certains fournisseurs d'équipements de communication pour réseaux mobiles font peser sur la sécurité de l'Union, comme en témoignent également les décisions prises par certains États membres".⁴⁴

En août 2024, seuls onze États membres de l'UE avaient exercé (bien qu'à des degrés divers) des pouvoirs légaux pour restreindre la participation de fournisseurs de télécommunications à haut risque tels que Huawei et ZTE à l'infrastructure du réseau 5G.⁴⁵ Il convient de noter que cela ne se traduit pas nécessairement par des interdictions totales - qui, dans de nombreux cas, seraient techniquement et financièrement irréalisables. Le gouvernement allemand, par exemple, a négocié avec les opérateurs de réseaux mobiles un accord visant à garantir le retrait des composants Huawei et ZTE des réseaux centraux 5G d'ici à la fin de 2026. En outre, les systèmes de gestion critiques fournis par ces deux fabricants dans les réseaux d'accès et de transport 5G doivent être remplacés par des technologies alternatives d'ici à la fin de 2029.⁴⁶ Depuis 2019,⁴⁷ les autorités françaises ont le pouvoir d'imposer des restrictions, des interdictions ou des exigences spécifiques sur la fourniture, le déploiement et l'exploitation des équipements 5G. Elles peuvent notamment rendre obligatoire l'obtention d'une autorisation préalable du Premier ministre pour le déploiement et l'exploitation d'équipements sensibles au sein des réseaux 5G, ainsi que des futures technologies de télécommunications (telles que la 6G).⁴⁸ De même, en Italie, conformément à la nouvelle législation introduite en 2022,⁴⁹ les entreprises qui ont l'intention d'acquérir des biens ou des services liés à la conception, à la mise en œuvre, à la maintenance et à la gestion de services de communication électronique à large bande basés sur la technologie 5G doivent notifier des informations détaillées au bureau du Premier ministre. Cette notification est nécessaire pour que le gouvernement puisse déterminer s'il doit exercer son droit de veto.

Il convient de noter que, faisant écho aux préoccupations exprimées par la Commission en 2023, Henna Virkkunen, commissaire désignée à la souveraineté technologique, à la sécurité et à la démocratie, a exprimé son mécontentement quant à l'état actuel de la mise en œuvre de boîte à outils de

⁴³ Voir : <https://digital-strategy.ec.europa.eu/en/library/second-report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity>

⁴⁴ Voir : Communication de la Commission : "Mise en œuvre de la boîte à outils pour la cybersécurité de la 5G", <https://digital-strategy.ec.europa.eu/en/library/communication-commission-implementation-5g-cybersecurity-toolbox>

⁴⁵ Voir : "Onze pays de l'UE ont pris des mesures de sécurité pour la 5G afin d'interdire Huawei et ZTE", <https://www.euro-news.com/next/2024/08/12/eleven-eu-countries-took-5g-security-measures-to-ban-huawei-zte>

⁴⁶ Voir : "Plus de sécurité et de souveraineté technologique pour le réseau mobile 5G allemand : Le gouvernement fédéral conclut des contrats avec des entreprises de télécommunications", <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2024/07/5g-en.html>

⁴⁷ Loi 810/2019 du 1er août 2019 <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038864094>

⁴⁸ Rapport sur les progrès réalisés par les États membres dans la mise en œuvre de la boîte à outils de l'UE sur la cybersécurité de la 5G. <https://digital-strategy.ec.europa.eu/en/library/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity>

⁴⁹ Loi 108/2022 <https://www.normattiva.it/atto/caricaDettaglioAtto?atto.dataPubblicazioneGazzetta=2022-08-05&atto.codiceRedazionale=22G00120&atto.articolo.numero=1&atto.articolo.sottoArticolo=1&atto.articolo.tipoArticolo=0>

cybersécurité 5G, annonçant une révision de la loi sur la cybersécurité de l'UE en 2025 et proposant une loi sur les réseaux numériques.⁵⁰

Le projet de système de certification de l'UE pour les services en nuage (CSCS) est un autre exemple illustrant les compromis possibles. Le SCCS et la boîte à outils de l'UE sur la cybersécurité de la 5G sont des éléments complémentaires de la stratégie plus large de l'UE en matière de cybersécurité, mais alors que la boîte à outils se concentre sur la sécurisation des réseaux 5G par des mesures d'atténuation des risques, le SCCS de l'UE devrait garantir que les services en nuage, qui soutiennent souvent des infrastructures critiques comme la 5G, répondent à des normes de cybersécurité robustes. Ensemble, ils abordent les risques interconnectés dans des domaines technologiques clés, conformément à l'idée selon laquelle l'UE "devrait s'assurer qu'elle dispose d'une industrie nationale compétitive capable de répondre à la demande de solutions de "cloud souverain"" contenue dans le "rapport Draghi" sur l'avenir de la compétitivité européenne.⁵¹

Récemment, le projet de CSCS de l'UE a été au centre d'une bataille politique sur les exigences de souveraineté.⁵² La France, mais aussi les représentants des PME numériques de l'UE, sont favorables à une approche plus stricte qui exclurait à terme les fournisseurs de services en nuage non européens des niveaux de sécurité les plus élevés.⁵³ D'autres États membres et acteurs de l'industrie se sont farouchement opposés à cette idée, la considérant comme une mesure protectionniste. Plus généralement, les détracteurs des projets de l'UE soutiennent qu'une approche qui donne la priorité à la "souveraineté numérique" - qui vise à maintenir le contrôle européen sur les infrastructures et les données critiques, mais favorise également les politiques de localisation, y compris dans l'IA et l'informatique quantique - nécessiterait des ressources excessives pour rester au niveau des concurrents mondiaux, ce qui pourrait détourner l'investissement et le capital humain d'autres secteurs.⁵⁴

Le débat autour du projet de CSCS de l'UE a mis en évidence les préférences divergentes des États membres de l'UE en ce qui concerne l'introduction d'exigences de souveraineté pour les prestataires de services. En effet, les organisations professionnelles de pays tels que l'Allemagne ont clairement exprimé leur inquiétude quant à la possibilité que l'introduction de telles exigences entrave la croissance des entreprises européennes opérant à l'échelle mondiale.⁵⁵ Il s'agit clairement d'un compromis entre la compétitivité économique et la poursuite de la sécurité et de la souveraineté de l'UE. Le nouveau commissaire chargé de la souveraineté technologique, de la sécurité et de la démocratie devra

⁵⁰ Voir : "Le nouveau chef de la technologie de l'UE discutera des mesures de sécurité de la 5G avec les gouvernements nationaux", <https://www.euronews.com/my-europe/2024/11/13/new-eu-tech-chief-to-discuss-5g-security-measures-with-national-governments>.

⁵¹ Voir : https://commission.europa.eu/document/download/97e481fd-2dc3-412d-be4c-f152a8232961_en?file-name=The%20future%20of%20European%20competitiveness%20-%20A%20competitiveness%20strategy%20for%20Europe.pdf.

⁵² Voir : <https://www.euronews.com/next/2024/06/18/decision-on-cloud-certification-scheme-delayed-to-mid-july>.

⁵³ Voir : <https://www.digitalsme.eu/changes-to-the-eu-cloud-services-cybersecurity-certification-scheme-put-eu-citizens-data-at-risk-a-call-for-digital-sovereignty/>.

⁵⁴ Voir, par exemple, Matthias Bauer, Fredrik Erixon et Dyuti Pandya : Matthias Bauer, Fredrik Erixon et Dyuti Pandya, "The EU's Trillion Dollar Gap in ICT and Cloud Computing Capacities : The Case for a New Approach to Cloud Policy", ECIPE Occasional Paper (Bruxelles : Centre européen d'économie politique internationale (ECIPE), 2024), <https://hdl.handle.net/10419/299187>.

⁵⁵ Voir : Julia Rone, "The Sovereign Cloud" in Europe : Diverging Nation State Preferences and Disputed Institutional Competences in the Context of Limited Technological Capabilities', *Journal of European Public Policy* 31, no 8 (2 août 2024) : 2343-69, <https://doi.org/10.1080/13501763.2024.2348618>.

examiner attentivement ce compromis lors de l'élaboration des innovations réglementaires en matière d'infrastructures TIC mentionnées ci-dessus.

3.4 Réglementation de l'IA : Normes éthiques et compétitivité

La loi sur l'IA de l'UE, qui est entrée en vigueur le 1er août 2024, est une étape audacieuse vers l'établissement de normes éthiques pour le développement et l'utilisation de l'IA, y compris dans le domaine des grands modèles de langage (LLM). Si cette législation vise à positionner l'UE en tant que leader mondial en matière d'IA responsable, elle soulève également des inquiétudes quant à l'impact potentiel sur l'innovation et la compétitivité. Ce compromis entre les considérations éthiques et la compétitivité économique n'est pas propre à la réglementation de l'IA, mais il est particulièrement pertinent compte tenu du potentiel de transformation des technologies de l'IA. Selon les chercheurs de Bruegel, "on ne sait pas si la loi stimulera l'utilisation responsable de l'IA ou si elle étouffera l'innovation".⁵⁶

Les LLM, tels que BERT, LLaMA et la série GPT d'OpenAI, ont le potentiel de révolutionner la façon dont nous interagissons avec l'information et communiquons à l'ère numérique. Ces modèles peuvent améliorer considérablement notre capacité à récupérer et à traiter l'information, en augmentant potentiellement l'intelligence collective (IC) à une échelle inimaginable jusqu'à présent. Toutefois, comme l'a récemment souligné un grand groupe de chercheurs dans la revue *Nature*, ce pouvoir s'accompagne de risques et de compromis inhérents.⁵⁷ La diversité et la compétence individuelle qui contribuent à l'IC dans les systèmes humains peuvent être compromises si les LLM homogénéisent les sources d'information ou réduisent la nécessité d'une réflexion critique individuelle. En outre, les mécanismes d'agrégation qui sont essentiels à l'IC doivent être soigneusement pris en compte lors de l'intégration des MAE dans les processus décisionnels collectifs. Le fait que les MAV puissent à la fois soutenir et éventuellement compromettre l'IC met en évidence l'équilibre délicat qui doit être trouvé dans leur développement et leur réglementation.

L'impact potentiel de la réglementation de l'IA sur l'innovation et la compétitivité a fait l'objet de nombreux débats et recherches.⁵⁸ Une étude approfondie menée par le Centre for European Policy Studies (CEPS) en 2020 a estimé que les coûts de mise en conformité pour les entreprises soumises à la loi sur l'IA pourraient se situer entre 1 % et 4 % des revenus liés à l'IA. Il est toutefois important de noter que ces coûts s'appliqueraient principalement aux systèmes d'IA à haut risque, qui ne représenteraient que 5 à 15 % de l'ensemble des systèmes d'IA. L'étude note que de nombreuses entreprises se conforment déjà à certaines des exigences proposées dans le cadre de leurs pratiques commerciales habituelles, ce qui pourrait réduire la charge supplémentaire liée à la conformité. Néanmoins, les coûts associés à la mise en œuvre de systèmes de gestion de la qualité pour les produits d'IA à haut risque pourraient être importants pour les PME, allant potentiellement de 193 000 à 330 000 euros pour la mise en place initiale, auxquels s'ajouteraient 71 400 euros pour la maintenance annuelle. Il est important d'aborder les estimations de coûts avec prudence et de tenir compte du contexte général. Les chercheurs du CEPS ont eux-mêmes souligné que les résultats de leur étude ont été mal interprétés par certains, ce qui a conduit à des projections de coûts exagérées.

⁵⁶ Voir : [L'Acte sur l'IA de l'Union européenne : réglementation prématurée ou précoce ?](#).

⁵⁷ Jason W. Burton et al, 'How Large Language Models Can Reshape Collective Intelligence', *Nature Human Behaviour* 8, no. 9 (20 septembre 2024) : 1643–55, <https://doi.org/10.1038/s41562-024-01959-9>.

⁵⁸ Pour ce résumé, voir : [Clarifier les coûts de la loi européenne sur l'IA - CEPS](#).

Étant donné que l'approche de la loi sur l'IA de l'UE vise des applications spécifiques à haut risque plutôt que des secteurs entiers, il est également probable que le compromis entre la réglementation et l'innovation puisse varier d'une industrie à l'autre.⁵⁹ Dans le secteur des soins de santé, l'interaction entre la loi sur l'IA et les réglementations existantes telles que le règlement sur les dispositifs médicaux (MDR) et le règlement sur les dispositifs médicaux de diagnostic in vitro (IVDR) peut accroître la charge de conformité pour les fabricants. Toutefois, elle pourrait également accroître la sécurité des patients et la confiance dans les solutions médicales basées sur l'IA. De même, dans les services financiers, l'accent mis par la loi sur l'IA sur les applications à haut risque pourrait conduire à une surveillance accrue de l'évaluation du crédit, des modèles de tarification et des évaluations des risques alimentés par l'IA. Cette surveillance accrue vise à protéger les consommateurs et à maintenir la stabilité du marché, mais elle pourrait également ralentir l'adoption de produits financiers innovants alimentés par l'IA. Enfin, dans l'industrie automobile, la loi sur l'IA pourrait apporter une clarté indispensable au cadre réglementaire des véhicules autonomes. Si elle pourrait simplifier certains aspects du développement et du déploiement, elle introduit également de nouvelles exigences en matière de normes de sécurité.

À la lumière de ces compromis, l'examen des leçons tirées des efforts réglementaires antérieurs pourrait fournir des indications pour la mise en œuvre de la loi sur l'IA. Aghion, Bergeaud et Van Reenen ont examiné l'impact des réglementations (du travail) sur l'innovation en France.⁶⁰ Ils ont constaté que les entreprises situées juste en dessous du seuil réglementaire de 50 employés présentaient une forte réduction de l'innovation, en particulier en réponse aux opportunités du marché. Dans l'ensemble, les chercheurs estiment que la réglementation a réduit l'innovation globale d'environ 5,4 %, ce qui équivaut à une perte de 2,2 % du bien-être équivalent à la consommation. Fait important, l'étude a révélé que la majeure partie de cette perte d'innovation était due à une réduction de l'intensité de l'innovation par entreprise, plutôt qu'à une simple mauvaise répartition des ressources au profit des petites entreprises ou à une réduction de l'entrée sur le marché. Cela suggère que l'impact de la réglementation sur l'innovation est plus complexe qu'une simple modification de la structure du marché. Cependant, la recherche a également mis en évidence une nuance intéressante : alors que la réglementation semble réduire l'innovation incrémentale, elle semble encourager des percées plus radicales, qui permettent d'économiser de la main-d'œuvre. Les entreprises soumises à une réglementation plus stricte ont tendance à mettre en œuvre des projets d'innovation plus ambitieux lorsqu'elles innovent.

Ces résultats pourraient donner des indications sur la mise en œuvre de la loi sur l'IA. Les décideurs politiques devraient concevoir avec soin et réévaluer régulièrement les seuils réglementaires afin d'éviter d'étouffer les incitations à l'innovation, en particulier pour les entreprises proches de ces limites. La mise en place de mécanismes d'évaluation continue de l'impact de la loi sur l'IA sur l'intensité et l'orientation de l'innovation sera cruciale pour affiner le cadre réglementaire au fil du temps. Compte tenu de l'impact disproportionné sur les petites entreprises, un soutien ciblé ou des exemptions pour les PME dans le secteur de l'IA pourraient contribuer à maintenir un écosystème diversifié et innovant. Enfin, la réglementation pouvant avoir une incidence sur la compétitivité mondiale, la promotion de la coopération internationale en matière de gouvernance de l'IA pourrait créer des conditions de concurrence plus équitables tout en promouvant des normes d'IA responsables à l'échelle mondiale, un point sur lequel nous reviendrons plus loin (section 4).

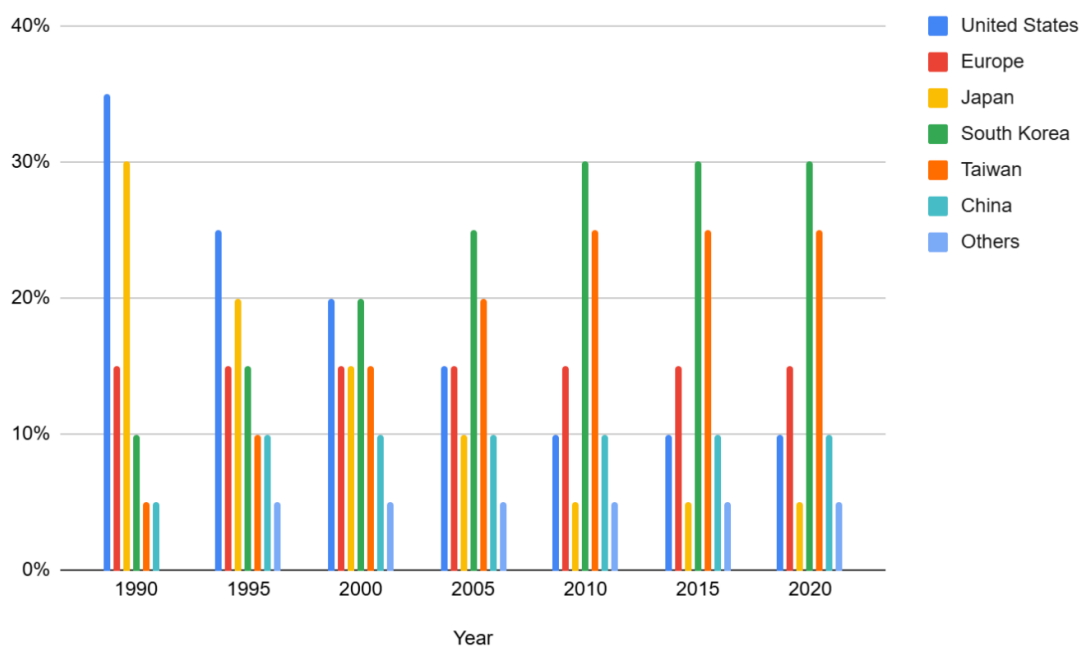
⁵⁹ Voir : [Loi européenne sur l'IA : Opportunités et défis | Roland Berger](#).

⁶⁰ Voir : Blind, Niebel et Rammer, "The Impact of the EU General Data Protection Regulation on Product Innovation".

3.5 Infrastructure informatique : Autonomie stratégique ou coopération mondiale

La lutte mondiale pour le contrôle de la technologie des microprocesseurs est devenue un champ de bataille géopolitique crucial qui a des répercussions considérables sur le pouvoir économique, les capacités militaires et le progrès technologique.⁶¹ Cette compétition, qui opposait autrefois principalement les États-Unis et la Chine, s'est désormais étendue à l'Europe en tant qu'acteur majeur. La réponse de l'UE à ce défi est double et porte à la fois sur les aspects matériels et logiciels de l'infrastructure informatique. D'une part, la loi européenne sur les puces vise à renforcer l'industrie européenne des semi-conducteurs et à réduire la dépendance à l'égard des fournisseurs étrangers. D'autre part, la récente initiative "AI Factories" de l'UE vise à exploiter les atouts de l'Europe en matière de calcul à haute performance afin d'accélérer le développement de l'IA. Nous examinerons ces deux aspects tour à tour.

Fig.2 : Capacité de production de semi-conducteurs par région, 1990-2020



Source : BofA Global Research : BofA Global Research. Extrait de : Artisan Partners Growth Team, The Semiconductor Decade.

Au cours des deux dernières décennies, l'industrie mondiale des semi-conducteurs est devenue de plus en plus dépendante d'une poignée de fabricants d'Asie de l'Est, en particulier pour les puces de pointe (figure 2). Les processus de production de puces "frontales" les plus sophistiqués sont concentrés aux États-Unis, à Taïwan et en Corée du Sud, de plus en plus en Chine, et dans une moindre mesure (et de moins en moins) en Europe, tandis que l'Asie du Sud-Est se spécialise dans la fabrication de semi-conducteurs "dorsaux".⁶² Taiwan Semiconductor Manufacturing Company (TSMC) et Samsung Electronics en Corée du Sud sont devenus les acteurs dominants de la production des puces les plus avancées,

⁶¹ Chris Miller, *Chip War : The Fight for the World's Most Critical Technology* (Londres : Simon & Schuster Ltd, 2023).

⁶² Par opposition à la fabrication de semi-conducteurs "front-end", qui consiste à créer les structures semi-conductrices aboutissant à la production d'une plaquette de silicium, la phase "back-end" consiste à découper la plaquette, à l'assembler, à la conditionner et à tester le produit final. Voir : <https://www.rabobank.com/knowledge/d011371771-mapping-global-supply-chains-the-case-of-semiconductors>.

TSMC représentant à lui seul plus de 90 % de la production mondiale de puces au nœud de 5 nanomètres et moins. Cette concentration a été motivée par les énormes investissements en capital nécessaires pour maintenir le leadership technologique et les avantages des économies d'échelle.

Alors que d'autres pays et régions investissent depuis longtemps dans le développement de l'industrie des semi-conducteurs, l'introduction de la loi sur les puces européennes marque une nouvelle tendance, l'UE cherchant à atteindre une autonomie stratégique dans cette industrie. Les raisons de cette évolution sont multiples. La pandémie a mis en évidence la dépendance de la chaîne d'approvisionnement de l'UE et sa vulnérabilité face à des événements géopolitiques imprévus. La sécurité de l'approvisionnement en semi-conducteurs est soudain apparue comme une priorité essentielle pour l'UE, notamment en raison des pénuries rencontrées dans l'industrie automobile. D'une manière générale, les puces sont essentielles au développement des technologies vertes, la décarbonisation de l'économie étant devenue une priorité politique. Cela souligne la nécessité d'une "géographie diversifiée de la production".⁶³ En d'autres termes, la loi européenne sur les puces signale le passage du modèle "juste à temps", typique d'une vision optimiste de la mondialisation économique, à une approche plus prudente de la gestion de la chaîne d'approvisionnement, "juste au cas où", qui a émergé en réponse à la pandémie et aux récentes crises géopolitiques.

Fig.3 : Investissement dans les puces, 2021-2023

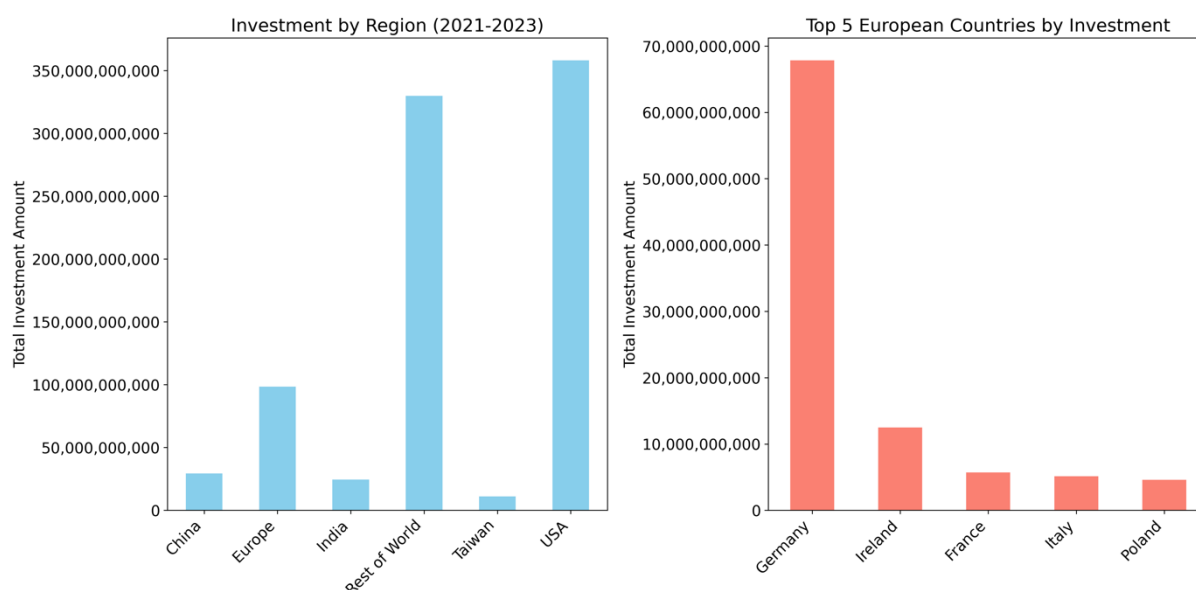


Illustration personnelle et analyse des données. Données extraites du site web SemiconductorEngineering.

Pour évaluer l'ampleur et l'efficacité de la réorientation de l'Europe, nous avons examiné des données compilées à partir de deux rapports en ligne complets publiés par Semiconductor Engineering, détaillant les nouveaux investissements dans les usines et les "fabs" annoncés entre 2021 et 2023.⁶⁴ Les données ont été agrégées manuellement à partir des annonces et des communiqués de presse des entreprises, ce qui donne un aperçu des plans d'expansion de l'industrie au cours de cette période. Pour assurer la cohérence de notre analyse, tous les investissements ont été convertis en dollars

⁶³ Voir : Lindsay Whitfield et al, "European Chips Act and the Global Race in Semiconductor Industrial Policy" : Business in Development ; E7 (Danemark : Centre for Business and Development Studies, 24 juin 2024).

⁶⁴ Voir : <https://semiengineering.com/money-pours-into-new-fabs-and-facilities/> (investissements annoncés en 2023 et fin 2022) et <https://semiengineering.com/where-all-the-semiconductor-investments-are-going/> (investissements annoncés en 2021 et 2022).

américains en utilisant les taux de change approximatifs au moment de l'annonce. Lorsqu'une fourchette d'investissements a été fournie, nous avons utilisé l'estimation la plus élevée afin de saisir tout le potentiel du projet. Pour certains investissements, les détails financiers spécifiques n'ont pas été divulgués. Notre ensemble de données couvre une période de trois ans, de 2021 à 2023, ce qui permet de saisir la vague initiale d'annonces d'investissements à la suite de la pénurie mondiale de puces et des réponses politiques qui en ont découlé. Cependant, l'industrie des semi-conducteurs est cyclique et certains investissements annoncés peuvent avoir été modifiés ou annulés depuis leur annonce initiale.⁶⁵ Les types d'investissement ont été ventilés pour refléter les catégories nuancées (par exemple, "emballage avancé") qui se retrouvent souvent dans les mêmes entrées, et des distinctions régionales ont été appliquées pour comparer les dépenses entre les États-Unis, l'Europe, la Chine, l'Inde, Taïwan et d'autres régions.

Le panneau de gauche (bleu) de la figure 3 montre la répartition des investissements dans l'industrie des semi-conducteurs entre les principales régions du monde. Les États-Unis sont clairement la première région, avec des investissements totaux dépassant 350 milliards de dollars, conformément à la loi américaine CHIPS. La catégorie "Reste du monde", qui comprend divers marchés tels que le Japon, la Corée du Sud, le Viêt Nam, la Malaisie et Singapour, affiche également un niveau d'investissement notable, de l'ordre de 300 milliards de dollars. À la suite de sa propre loi sur les puces électroniques, l'Europe vise à rattraper son retard, avec des investissements cumulés d'environ \$ 100 milliards. Dans le même temps, les niveaux d'investissement dans des régions telles que Taïwan, l'Inde et la Chine sont comparativement modestes. Cette répartition reflète essentiellement les efforts déployés récemment par les principales économies pour renforcer leurs secteurs des semi-conducteurs dans le contexte des préoccupations relatives à la chaîne d'approvisionnement mondiale, ce qui fait des États-Unis une plaque tournante dominante.

Le panneau de droite (rouge) de la figure 3 illustre une disparité significative dans la répartition des investissements dans les semi-conducteurs en Europe, l'Allemagne attirant à elle seule l'écrasante majorité des financements, pour un total d'environ 70 milliards de dollars. En revanche, d'autres pays de l'UE tels que l'Irlande, la France, l'Italie et la Pologne reçoivent des parts beaucoup plus faibles. Cette répartition met en évidence une certaine distorsion dans le marché unique de l'UE. Un tel déséquilibre peut, par la suite, exacerber les dépendances technologiques au sein de l'UE et réduire la résilience de la chaîne d'approvisionnement en semi-conducteurs dans l'ensemble de la région. En d'autres termes, ce type de politique industrielle pourrait avoir des effets néfastes sur la convergence économique au sein de l'UE.⁶⁶

Nous analysons également les données de manière qualitative afin de mieux comprendre les domaines spécifiques de la technologie des semi-conducteurs dans lesquels des investissements importants ont été concentrés. Des investissements importants ont été consacrés à la fabrication de puces de fonderie, avec 228 milliards de dollars alloués à cette catégorie, ce qui souligne l'importance accordée par l'industrie à l'expansion des capacités de fabrication de base. En outre, 100 milliards de dollars ont été investis dans la mise à niveau des outils de lithographie EUV à haute résolution sur le campus Gordon Moore Park d'Intel aux États-Unis, une technologie de lithographie de nouvelle génération essentielle à la réduction de la taille des puces. En ce qui concerne la fabrication de pointe, des investissements

⁶⁵ Un exemple notable est le projet d'investissement d'Intel en Allemagne, qui a été révisé depuis sa première annonce.

⁶⁶ Sur ce point, voir : Angela Wigger, "The New EU Industrial Policy and Deepening Structural Asymmetries : Smart Specialisation Not So Smart", *JCMS : Journal of Common Market Studies* 61, no. 1 (janvier 2023) : 20–37, <https://doi.org/10.1111/jcms.13366>.

importants ont été réalisés dans la technologie du processus 3nm, en particulier dans des régions telles que les États-Unis () et Taïwan, qui chercheront probablement à maintenir leur leadership technologique grâce à la fabrication de semi-conducteurs de pointe. En revanche, nous observons une concentration plus large sur divers domaines de l'infrastructure des semi-conducteurs et de l'expansion des capacités dans d'autres régions du monde, y compris en Europe. Les investissements dans les plaques de 300 mm, les nouvelles fabs et l'infrastructure générale de fabrication de semi-conducteurs suggèrent une volonté de renforcer les capacités de base plutôt que de se concentrer exclusivement sur les nœuds technologiques de pointe. La présence de 20 milliards de dollars d'investissements dans des domaines tels que l'informatique quantique, l'IA et le cloud hybride indique également une stratégie d'investissement diversifiée. En outre, les investissements importants dans les unités d'assemblage et de test et dans une unité de fabrication d'écrans suggèrent une concentration sur les capacités de production en aval qui soutiennent la chaîne d'approvisionnement des semi-conducteurs au sens large. Dans l'ensemble, les États-Unis et Taïwan semblent se concentrer fortement sur l'innovation de haute technologie et les processus de fabrication de pointe, tandis que l'Europe et d'autres régions donnent la priorité à l'expansion des capacités de production et des infrastructures.

En complément du Chips Act axé sur la fabrication, la nouvelle initiative "AI Factories" de l'UE vise à accroître les investissements dans l'infrastructure matérielle et logicielle essentielle au développement de l'IA générative. Lancé début 2024, ce programme de 2 milliards d'euros vise à créer un réseau de superordinateurs optimisés pour l'IA et accessibles aux chercheurs, aux startups et à l'industrie dans toute l'Europe.⁶⁷ En s'appuyant sur les capacités existantes de l'entreprise commune européenne pour le calcul à haute performance (EuroHPC JU), l'initiative vise à démocratiser l'accès aux ressources informatiques nécessaires au développement d'applications d'IA à grande échelle.

Cependant, l'initiative, bien qu'ambitieuse, semble souffrir des mêmes problèmes conceptuels que les subventions européennes aux puces décrites ci-dessus. Les deux initiatives manquent d'une politique industrielle véritablement centralisée, qui est essentielle pour éviter les distorsions du marché et garantir une allocation efficace des ressources. Le plan pour les usines d'IA, comme son équivalent pour les semi-conducteurs, risque de se fragmenter en tentant de répartir les ressources entre plusieurs États membres pour satisfaire des demandes politiques plutôt que de se concentrer sur les solutions les plus efficaces. Cette approche pourrait conduire à une dilution des financements et à l'absence de la masse critique nécessaire pour être compétitif à l'échelle mondiale. Comme le M. Hoos, l'investissement prévu par l'UE dans chaque usine d'IA se situe dans le "mauvais ordre de grandeur", avec seulement quelques dizaines de millions d'euros alloués par installation.⁶⁸ Cette approche fragmentaire contraste fortement avec les investissements massifs réalisés par des entreprises américaines comme OpenAI et Microsoft, qui prévoient un centre de données de 100 milliards de dollars d'ici à 2028.

3.6 Politique de concurrence : Bien-être des consommateurs et intérêts publics plus larges

Dans toute l'Europe, le droit de la concurrence a récemment été considéré comme une discipline très technique, axée principalement sur l'analyse économique et la prévention de la fixation de prix non

⁶⁷ Voir : <https://digital-strategy.ec.europa.eu/en/policies/ai-factories>.

⁶⁸ Voir : <https://www.euractiv.de/section/innovation/news/ki-computing-eu-kaempft-mit-rueckstand-und-investitionslucke/>.

optimaux par les grandes entreprises.⁶⁹ Au cours des dernières décennies, en particulier à l'époque de l'"approche plus économique", la politique de concurrence s'est caractérisée par sa dépendance à l'égard de modèles économétriques complexes et d'évaluations quantitatives.⁷⁰ Bien que rigoureuse, cette approche a souvent négligé les implications sociétales plus larges et les valeurs normatives au-delà de l'efficacité économique pure. L'accent mis sur l'analyse technique a servi à isoler le droit de la concurrence des considérations externes, créant un champ d'expertise quelque peu insulaire qui ignore les compromis potentiels. Cette approche diffère de celle de rivaux stratégiques tels que la Chine, qui utilise la législation antitrust pour promouvoir les entreprises nationales et comme instrument de politique commerciale et étrangère.⁷¹

Toutefois, ces dernières années ont été marquées par un changement prudent du paradigme de la politique de concurrence de l'UE. L'ampleur et la portée sans précédent des plateformes numériques ont forcé les décideurs politiques et les universitaires à reconnaître que le pouvoir exercé par les géants de la technologie n'affecte pas seulement la concurrence sur le marché, mais a également de profondes implications pour la vie privée, la démocratie et la cohésion sociale.⁷² Par conséquent, il est de plus en plus admis que la politique de concurrence ne peut pas fonctionner indépendamment de ces préoccupations sociétales plus larges. La pandémie a encore souligné la nécessité d'une approche plus holistique de la politique de concurrence. La crise Covid ayant révélé les vulnérabilités des chaînes d'approvisionnement mondiales et mis en évidence les risques associés aux monopoles et aux points de défaillance uniques dans les secteurs critiques, un débat s'est engagé sur le rôle du droit de la concurrence dans la promotion de la résilience économique et la sauvegarde des services essentiels en temps de crise. Un autre nouveau domaine de débat est le concept d'"antitrust vert", qui cherche à intégrer des considérations de durabilité dans l'analyse de la concurrence de l'UE.⁷³ Ses partisans soutiennent que la politique de concurrence devrait évoluer pour soutenir les pratiques commerciales durables et les efforts de coopération visant à réduire les dommages environnementaux, même si de telles actions peuvent sembler restreindre la concurrence à court terme.

La possibilité d'une présidence Trump 2.0 - qui s'est maintenant matérialisée - a encore intensifié ces débats. La menace précoce de J.D. Vance de retirer le soutien des États-Unis à l'OTAN si l'UE continue d'enquêter sur la plateforme X d'Elon Musk est un exemple de l'intersection croissante entre la réglementation des plateformes et les considérations géopolitiques.⁷⁴ L'UE doit-elle maintenir l'intégrité et l'indépendance de l'application des règles de concurrence face aux pressions politiques extérieures et aux préoccupations de sécurité nationale ? Lors de son audition parlementaire, la nouvelle commissaire européenne chargée de la technologie, Henna Virkkunen, a évité d'aborder le rôle de Musk dans la diffusion de fausses informations sur X - marquant un contraste frappant avec son prédécesseur,

⁶⁹ Oles Andriychuk, *Les fondements normatifs du droit européen de la concurrence : Assessing the Goals of Antitrust through the Lens of Legal Philosophy* (Cheltenham, UK : Edward Elgar Publishing, 2017).

⁷⁰ André Schmidt et Michael Wohlgemuth, "Das Wettbewerbskonzept der EU aus Sicht der Wirtschaftswissenschaften : Wie ökonomisch ist der "more economic approach"", in *Dimensionen des Wettbewerbs : europäische Integration zwischen Eigendynamik und politischer Gestaltung*, ed. Hermann-Josef Blanke, Arno Scherzberg, and Gerhard Wegner, Neue Staatswissenschaften 11 (Tübingen : Mohr Siebeck, 2010), 51-80.

⁷¹ Zhang, *Chinese Antitrust Exceptionalism*.

⁷² Patrick Barwise et Leo Watkins, "The Evolution of Digital Dominance : How and Why We Got to GAFA", dans *Digital Dominance : The Power of Google, Amazon, Facebook, and Apple*, ed. Martin Moore et Damian Tambini (Oxford : Oxford University Press, 2018), 21-49, <https://doi.org/10.35065/PUB.00000914>.

⁷³ Maarten Pieter Schinkel et Leonard Treuren, "Green Antitrust : Friendly Fire in the Fight against Climate Change", *SSRN Electronic Journal*, 2020, <https://doi.org/10.2139/ssrn.3749147>.

⁷⁴ Voir : <https://www.independent.co.uk/news/world/americas/us-politics/jd-vance-elon-musk-x-twitter-donald-trump-b2614525.html>.

Věra Jourová, qui avait qualifié Musk de " promoteur du mal ".⁷⁵ Au lieu de cela, Mme Virkkunen a souligné le double défi auquel elle est confrontée : assurer la sécurité européenne, qui repose fortement sur la coopération américaine, tout en faisant progresser la souveraineté technologique européenne, souvent en désaccord avec les géants américains de la technologie.

Comment gérer ces nouveaux types de compromis non économiques du point de vue de la politique de la concurrence ? Martijn Snoep, président de l'Autorité néerlandaise pour les consommateurs et les marchés, a récemment fait remarquer que si les autorités de la concurrence sont bien équipées pour analyser la dynamique du marché et proposer des mesures visant à renforcer la concurrence, elles ne sont pas toujours les mieux placées pour prendre les décisions finales lorsque d'autres intérêts publics essentiels sont en jeu.⁷⁶ Comme le souligne M. Snoep, "ce qui peut être bon pour la concurrence peut être mauvais, par exemple, pour la sécurité nationale ou la vie privée". Il a donc proposé un garde-fou supplémentaire qui donnerait à un ministre le pouvoir d'annuler, en tout ou en partie, toute mesure qu'une autorité de la concurrence propose d'imposer si elle entre en conflit avec des intérêts publics plus larges. En introduisant un contrôle ministériel, ce système permettrait à de procéder à une évaluation plus complète des mesures de concurrence proposées au regard d'un éventail plus large de préoccupations sociétales. Ce pouvoir ministériel d'annulation serait similaire aux mécanismes existants en Allemagne, où les ministres des affaires économiques peuvent annuler les décisions de l'autorité de la concurrence dans les affaires de fusion pour des raisons d'intérêt public général. D'un point de vue ordolibéral, cependant, la mise en œuvre de cette approche nécessiterait une conception minutieuse afin de garantir la transparence et d'éviter toute ingérence politique indue dans les questions de concurrence. Des critères clairs pour l'intervention ministérielle et une justification publique de toute dérogation seraient essentiels pour maintenir l'intégrité du processus d'application des règles de concurrence.

4 Dimension externe : Aborder les compromis par le biais de partenariats

Bien qu'elle soit parfois sous-estimée, la dimension extérieure de la politique numérique de l'UE offre plusieurs possibilités de répondre à certains des compromis identifiés dans les sections précédentes. Alors que l'engagement international est souvent perçu comme une source de risques potentiels, une approche stratégique des partenariats et de la coopération pourrait en fait servir de solution à de nombreux défis numériques de l'UE. Cette perspective peut sembler contre-intuitive étant donné le récit dominant des luttes géopolitiques, des chocs culturels, de la souveraineté numérique et de l'auto-suffisance, mais elle offre un moyen prometteur de résoudre des dilemmes politiques complexes. En encourageant la coopération avec des partenaires internationaux, l'UE peut en fait améliorer ses capacités technologiques et renforcer ses mesures de sécurité, tout en atténuant certains des compromis internes qui sont apparus dans le paysage de sa politique numérique. Ces arguments rejoignent ceux de Renda, qui a récemment affirmé que "ce n'est qu'en intégrant des règles et des valeurs dans le "code" et en préservant l'ouverture au reste du monde que l'UE parviendra à atteindre les objectifs qu'elle s'est fixés".⁷⁷

⁷⁵ Politico (2024), [5 things to know about EU tech security chief Henna Virkkunen's hearing - POLITICO.](#)

⁷⁶ Voir : <https://www.acm.nl/en/publications/blog-martijn-snoep-updating-competition-enforcement>.

⁷⁷ Andrea Renda, "Making the Digital Economy 'Fit for Europe'", *European Law Journal* 26, no. 5-6 (novembre 2020) : 202, <https://doi.org/10.1111/eulj.12388>.

L'Union européenne (UE) a fait des progrès considérables pour s'imposer comme un leader mondial de la diplomatie numérique.⁷⁸ Cette transformation a d'abord été marquée par l'initiative du marché unique numérique lancée en 2015, qui est passée d'un projet largement axé sur le marché intérieur à un projet aux ambitions internationales étendues, comme le montre la "Boussole numérique 2030" lancée en 2021.⁷⁹ L'approche de l'UE en matière de diplomatie numérique a intégré un cadre à plusieurs niveaux qui comprend des réglementations numériques, des collaborations internationales, une coopération au développement et un alignement politique avec les États membres. Dans le contexte du cadre institutionnel de l'UE, plusieurs directions générales (DG) clés au sein de la Commission européenne contribuent à façonner la diplomatie numérique de l'UE. La DG Connect (Réseaux de communication, contenu et technologie) est passée d'une branche axée sur la recherche à une entité axée sur les politiques, travaillant sur la réglementation numérique, les partenariats numériques internationaux et les grandes initiatives de recherche telles que le PPP 5G. La DG Grow (marché intérieur, industrie, entrepreneuriat et PME) mène des initiatives en faveur de la transformation numérique et de la décarbonisation de l'industrie et des PME européennes, soutenant l'objectif de faire de l'UE une économie plus verte, plus numérique et plus résiliente. La DG Intpa (Partenariats internationaux) met l'accent sur l'intégration des initiatives numériques dans la politique de développement, en raison de l'importance croissante de la technologie numérique dans des domaines tels que l'agriculture, les ressources en eau et les droits de l'homme dans les pays partenaires. La DG Commerce a intensifié son attention sur le commerce numérique, en particulier dans les négociations sur les flux de données, tandis que la DG Justice (Justice et consommateurs) veille à ce que la confidentialité des données et les droits soient respectés dans le cadre de ces échanges. La DG Recherche et innovation finance des projets d'infrastructure numérique essentiels qui soutiennent les efforts de diplomatie numérique de l'UE, tels que le câble Bella, d'une importance géostratégique, qui relie l'Europe et l'Amérique latine, et Medusa, qui traverse la Méditerranée. Enfin, le Service européen pour l'action extérieure (SEAE) joue un rôle clé dans la coordination des efforts de l'UE en matière de diplomatie numérique. À la suite des conclusions du Conseil sur la diplomatie numérique de l'UE en 2022 et 2023, l'UE a défini des actions prioritaires pour une politique numérique plus stratégique et plus cohérente, en mettant l'accent sur une approche "Team Europe" pour un engagement mondial coordonné sur les questions numériques.⁸⁰ Ces actions sont axées sur le renforcement des partenariats multilatéraux, la lutte contre la fracture numérique et la promotion du leadership en matière de normes numériques mondiales, en particulier dans le domaine des technologies émergentes. Plus récemment, l'examen du Conseil des affaires étrangères de juillet 2024 a mis en évidence l'importance stratégique des questions numériques dans la politique étrangère de l'UE et la nécessité d'une action unifiée pour soutenir la démocratie, l'économie et la société.

⁷⁸ Ici, la *diplomatie numérique* fait référence à un concept plus large, mettant en évidence les efforts diplomatiques concentrés sur des domaines politiques stratégiquement critiques tels que la cybersécurité, la protection des données, le commerce électronique, la gouvernance de l'internet et la gouvernance de l'IA. Ces sujets influencent presque tous les domaines politiques pertinents pour l'UE, de la géopolitique et du développement aux droits de l'homme et à la sécurité. Voir : Cecilia Emma Sottolotta, "A "Battle for Hearts and Minds" ? EU Digital Diplomacy toward the Global South", *Global Policy*, 22 août 2024, 1758-5899.13423, <https://doi.org/10.1111/1758-5899.13423>.

⁷⁹ Voir : COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS Boussole numérique 2030 : la voie européenne pour la décennie numérique, COM/2021/118 final.

⁸⁰ Voir : [Diplomatie numérique de l'UE : Le Conseil convient d'une approche européenne plus concertée face aux défis posés par les nouvelles technologies numériques - Consilium](#) ; et [Digital diplomacy : Le Conseil définit des actions prioritaires pour renforcer l'action de l'UE dans les affaires numériques mondiales - Consilium](#).

Comment la coopération et les partenariats pourraient-ils contribuer à résoudre les problèmes spécifiques identifiés ci-dessus ?

1. Pour commencer, l'UE peut recourir à des partenariats internationaux pour trouver un équilibre entre ses normes élevées en matière de protection des données et la nécessité de favoriser un environnement commercial compétitif. Les décisions d'adéquation mutuelle de l'UE pour le transfert de données à caractère personnel avec le Japon (2019) et la Corée du Sud (2021), respectivement, sont des exemples de coopération réussie, facilitant la libre circulation des données à caractère personnel tout en maintenant de solides protections de la vie privée. Rétrospectivement, les pays qui ont bénéficié de l'adéquation de l'UE ont vu leur commerce numérique augmenter de 6 à 14 %, ce qui représente une réduction des coûts commerciaux pouvant aller jusqu'à 9 %.⁸¹ Toutefois, les organisations de défense des libertés civiles ont fait valoir que l'évaluation positive par la Commission du cadre de protection des données UE-États-Unis (DPF) minimise les préoccupations importantes concernant la surveillance étatique et commerciale, perpétuant en fait les pratiques de surveillance de masse révélées par Edward Snowden il y a plus d'une décennie.⁸² En outre, la seconde présidence Trump complique encore la situation. Au cours de son premier mandat, l'administration du président Trump a adopté une position de confrontation à l'égard des cadres de protection de la vie privée de l'UE, arguant qu'ils entravaient les entreprises américaines et posaient des risques pour la sécurité nationale.⁸³ Les efforts de son administration pour priver les citoyens non américains des protections de la vie privée en vertu de la loi sur la protection de la vie privée ont illustré cette approche, ce qui a suscité des inquiétudes quant au fait que le DPF pourrait être sapé ou rendu inefficace si des mesures similaires étaient rétablies. Alors que l'UE cherche à redéfinir ses relations avec les États-Unis, la question est de savoir si les Européens sont prêts et capables de faire des compromis sur la protection des données face aux pressions géopolitiques.

Au-delà des FDP, l'UE a lancé en décembre 2020 le D4D Hub (Digital for Development Hub), une initiative visant à promouvoir une transformation numérique inclusive et durable à l'échelle mondiale. Elle s'inscrit dans le cadre de la stratégie "Global Gateway" de l'UE et vise à encourager les partenariats numériques avec des pays d'Afrique, d'Amérique latine, d'Asie et du Pacifique.⁸⁴ Le hub D4D vise à exploiter l'expertise et les valeurs technologiques de l'UE, en mettant l'accent sur la connectivité, la cybersécurité et le renforcement des capacités, tout en encourageant les investissements du secteur privé. Parmi ses activités, on peut citer l'initiative UE-UA sur la gouvernance des données, qui aide les États membres de l'Union africaine (UA) à élaborer des lois sur la protection des données et des cadres de gouvernance numérique alignés sur les normes internationales, l'Alliance numérique UE-ALC, qui promeut l'échange de politiques et la coopération sur des questions telles que la gouvernance numérique, les technologies émergentes et la cybersécurité, ou encore le partenariat Inde-UE sur les normes TIC, qui encourage l'adoption de normes alignées sur celles de l'UE pour la 5G, l'Internet des Objets

⁸¹ Martina Francesca Ferracane et al, "Digital Trade, Data Protection and EU Adequacy Decisions", document de travail, EUI RSC (Florence : European University Institute, 2023), <https://hdl.handle.net/1814/75629>.

⁸² Krempel (2024), [Vorwürfe zum EU-US-Datenaustausch : Kommission spielt Massenüberwachung herunter | heise online](#).

⁸³ Vinocur (2020), [Pourquoi l'administration Trump s'en prend aux règles européennes en matière de protection de la vie privée - POLITICO](#).

⁸⁴ L'initiative "Global Gateway" de l'UE, lancée en décembre 2021, est la stratégie phare de l'Union européenne pour mobiliser les investissements en faveur du développement des infrastructures mondiales. Elle vise à renforcer la résilience économique, sociale et environnementale dans le monde entier en promouvant des projets durables, de haute qualité et axés sur les valeurs dans des domaines tels que la connectivité numérique, l'énergie, les transports, la santé et l'éducation. L'initiative est largement considérée comme la réponse de l'UE à l'initiative chinoise Belt and Road Initiative (BRI) et au Partenariat pour l'infrastructure et l'investissement mondiaux (PGII) dirigé par les États-Unis.

(IdO) et l'IA en Inde, en garantissant l'interopérabilité et la sécurisation des réseaux. En s'appuyant sur ces partenariats, l'UE pourrait affiner le GDPR en y intégrant des mécanismes plus flexibles qui soutiennent l'innovation axée sur les données. Par exemple, l'introduction de bacs à sable réglementaires ou de processus rationalisés pour les transferts internationaux de données pourrait répondre aux préoccupations des entreprises concernant l'impact du GDPR sur la compétitivité sans compromettre les droits à la vie privée des individus.

2. Lorsqu'il s'agit de réglementer le contenu en ligne et la liberté d'expression, la coopération internationale offre des perspectives précieuses sur les approches alternatives, notamment dans le contexte de groupes multipartites tels que le Forum des Nations unies sur la gouvernance de l'internet. Comme décrit ci-dessus, l'ASD de l'UE vise à créer un espace numérique plus sûr en tenant les plateformes en ligne responsables du contenu qu'elles hébergent. L'engagement avec des partenaires démocratiques tels que la Nouvelle-Zélande, qui a lancé l'"appel de Christchurch" pour éliminer les contenus terroristes et extrémistes violents en ligne, ou la Corée du Sud, connue pour ses mesures proactives contre les discours haineux et la désinformation en ligne, pourrait éclairer la mise en œuvre à grande échelle de l'AVD au cours des prochaines années, en veillant à ce qu'elle concilie efficacement la protection des utilisateurs et la préservation de la liberté d'expression. Un domaine clé dont l'UE pourrait s'inspirer est celui de l'Australie, qui préconise la vérification technologique de l'âge sur les plateformes de médias sociaux. L'ASD a été confrontée à des difficultés dans la mise en œuvre effective des mesures de vérification de l'âge, et l'approche australienne pourrait offrir des solutions.⁸⁵

3. Dans le domaine de la cybersécurité et des incitations économiques, des partenariats avec d'autres nations technologiquement avancées pourraient renforcer les capacités de l'UE tout en partageant la charge économique. La stratégie de cybersécurité de l'UE pour la décennie numérique souligne l'importance de la coopération internationale pour améliorer la cyber-résilience. Des initiatives conjointes de recherche et de développement avec des pays tels qu'Israël, connu pour son solide secteur de la cybersécurité, ou Singapour, leader en matière d'innovation dans le domaine de la cybersécurité, ainsi qu'avec le Japon et la Corée du Sud, pourraient renforcer la résilience technologique de l'UE. Des recherches récentes menées par M. Wolf soutiennent cette approche, en soulignant le rôle crucial du partage transfrontalier des connaissances dans la promotion de l'innovation, en particulier dans les domaines technologiques critiques.⁸⁶ Son analyse des données mondiales sur les brevets montre que l'UE ne dispose pas d'avantages technologiques comparatifs dans plusieurs domaines essentiels, notamment l'intelligence artificielle et la connectivité. Cela souligne la nécessité d'établir des partenariats internationaux pour renforcer les capacités technologiques de l'UE. Fait important, M. Wolf constate que les brevets de l'UE issus de collaborations de recherche avec des pays tiers ont reçu beaucoup plus de citations que ceux dont les inventeurs sont purement nationaux, et il recommande donc que l'UE élabore une stratégie de coopération technologique spécifique. De tels partenariats faciliteraient le transfert de connaissances, encourageraient l'innovation et pourraient déboucher sur de nouvelles opportunités économiques dans l'économie numérique de l'UE. Comme indiqué précédemment, l'UE a récemment commencé à expérimenter certains mécanismes réglementaires qui pourraient être utiles à cet égard : Les bacs à sable réglementaires, comme le souligne le nouvel agenda européen de l'innovation, fournissent un environnement réel contrôlé pour tester les innovations avec des

⁸⁵ Voir : <https://www.rte.ie/news/business/2024/1126/1483039-meta-regulation-on-age-verification/>.

⁸⁶ André Wolf, "Forschungskooperationen Bei Kritischen Technologien : Europas Strategischer Balanceakt", *Zeitschrift Für Wirtschaftspolitik*, 13 novembre 2024, <https://doi.org/10.1515/zfw-2024-2021>.

ajustements temporaires des réglementations.⁸⁷ Ils pourraient faciliter l'expérimentation collaborative entre l'UE () et ses partenaires internationaux, en garantissant le développement de technologies de cybersécurité sûres, évolutives et efficaces. De même, les bancs d'essai axés sur les avancées technologiques pourraient offrir un espace permettant d'évaluer, sans contraintes réglementaires, des outils et des systèmes de cybersécurité novateurs mis au point en partenariat avec des leaders mondiaux. Enfin, les laboratoires vivants, qui mettent l'accent sur la cocréation et la participation des utilisateurs, pourraient permettre aux entreprises des États membres de l'UE et des pays partenaires de concevoir, de tester et d'affiner, en collaboration, des mesures de cybersécurité répondant aux besoins de la société.

4. L'élaboration de normes éthiques pour l'IA est un autre domaine dans lequel la coopération internationale devrait être poursuivie, afin d'éviter les lacunes caractérisant l'approche actuelle de la "souveraineté en matière d'IA" qui, selon Mugge, oppose l'UE au "reste".⁸⁸ Plutôt que de chercher à réduire les risques liés à l'IA de manière isolée, l'UE devrait se concentrer sur les efforts multilatéraux tels que le Partenariat mondial sur l'intelligence artificielle (GPAI), qui comprend des membres importants tels que le Canada, le Japon, l'Australie et les États-Unis. Dans cette optique, le ministre fédéral allemand des affaires numériques et des transports, Volker Wissing, a récemment souligné l'importance des alliances mondiales en matière de politique numérique. Dans un monde interconnecté où les conditions d'un internet libre ne peuvent être fixées unilatéralement, il appelle à un plus grand engagement dans les forums internationaux tels que le G7, l'OCDE et le Forum sur la gouvernance de l'internet (FGI) pour aider à façonner des normes mondiales conformes à des valeurs partagées.⁸⁹ En s'engageant auprès de diverses parties prenantes, notamment les professionnels des STIM, les décideurs politiques et les communautés sous-représentées, des initiatives telles que celles menées par l'IEEE et l'UNESCO ont permis de réaliser des progrès significatifs dans l'établissement de cadres éthiques pour l'IA.⁹⁰ Pour relever les défis de la mise en œuvre et de l'adoption, une intégration plus structurée des connaissances techniques dans les programmes globaux de gouvernance de l'IA est nécessaire.

5. En ce qui concerne le compromis entre l'autonomie stratégique et la coopération mondiale en matière d'infrastructure informatique à grande échelle, l'UE peut bénéficier de partenariats ciblés, mais doit également développer ses capacités nationales pour atténuer les risques associés à une dépendance excessive à l'égard de systèmes externes tels que Starlink de SpaceX. Comme nous l'avons souligné dans la section précédente, le secteur européen des semi-conducteurs est confronté à un risque de fragmentation en raison d'une course aux subventions internes due à des politiques d'aides d'État disparates entre les États membres. Pour relever ce défi, l'UE doit d'abord supprimer progressivement les cadres temporaires tels que ceux introduits pour la pandémie et la crise énergétique d'ici à la fin de 2025, en se concentrant plutôt sur des instruments permanents tels que le RGEC et les IPCEI afin d'aligner les initiatives nationales sur une stratégie paneuropéenne.⁹¹ Il est essentiel de renforcer

⁸⁷ Commission européenne, "L'apprentissage réglementaire dans l'UE : Guidance on Regulatory Sandboxes, Testbeds, and Living Labs in the EU, with a Focus Section on Energy", document de travail des services de la Commission (Bruxelles : Commission européenne, août 2023), https://research-and-innovation.ec.europa.eu/document/download/fc6f35cd-a8d6-4770-aeef-c09ca85cff8c_en?filename=swd_2023_277_f1.pdf.

⁸⁸ Daniel Mùgge, "EU AI Sovereignty : For Whom, to What End, and to Whose Benefit ?", *Journal of European Public Policy*, 28 février 2024, 1-26, <https://doi.org/10.1080/13501763.2024.2318475>.

⁸⁹ Wissing (2024), [Wir brauchen mehr global Allianzen - Tagesspiegel Background](#).

⁹⁰ Voir : Mariazel Maqueda López et al, "Science and Technology : A Framework for Peace", *Communications Engineering* 3, no. 1 (5 novembre 2024) : 4, <https://doi.org/10.1038/s44172-024-00310-4>.

⁹¹ Donato Di Carlo, Andreas Eisl et Diane Zurstrassen, "Together We Trade, Divided We Aid : Mapping the Flexibilization of the EU State Aid Regime across GBER, IPCEIs and Temporary Frameworks", Policy Paper (Jacques Delors Institute, November 2024), <https://institutdelors.eu/en/publications/together-we-trade-divided-we-aid/>.

l'instrument IPCEI, la Commission devant jouer un rôle plus important pour veiller à ce que les projets soient sélectionnés en fonction de leur mérite stratégique plutôt que de la capacité fiscale de chaque État membre. Une fois ces règles du jeu internes établies, l'UE pourrait travailler avec des partenaires de confiance pour compléter ses ressources, comme le Japon, qui développe des superordinateurs de nouvelle génération. Cependant, il n'est pas possible de faire l'économie du développement de ses propres capacités grâce à des initiatives telles que le programme IRIS² (Infrastructure for Resilience, Interconnectivity and Security by Satellite) et l'EuroHPC JU. Dans le cadre des subventions et des rivalités géopolitiques évoquées ci-dessus, le paysage mondial des semi-conducteurs est en pleine mutation, les États-Unis, l'UE et d'autres régions ayant adopté une législation ambitieuse pour renforcer la production nationale de puces et réduire la dépendance à l'égard des fournisseurs étrangers. L'expansion apparemment réussie de TSMC en Arizona,⁹², soutenue par un financement du gouvernement américain à hauteur de 6,6 milliards de dollars, est un exemple de la manière dont les partenariats internationaux peuvent contribuer à résoudre les problèmes de souveraineté technologique. En amenant la production de puces 3 nm et 2 nm de pointe sur le sol américain, cette collaboration renforce la compétitivité économique et la sécurité nationale des États-Unis tout en offrant à TSMC une base de production stable moins exposée à un conflit potentiel dans le détroit de Taïwan. Contrairement aux États-Unis, l'Union européenne ne dispose pas d'un fabricant de puces dominant comme Intel et dépend donc encore plus de l'attraction des investissements étrangers. Toutefois, la réalisation des objectifs de l'EU Chips Act nécessitera non seulement un financement substantiel, mais aussi une coopération étroite avec les leaders mondiaux de l'industrie. En encourageant les partenariats avec des entreprises comme TSMC et Intel, tout en renforçant les liens avec des alliés démocratiques comme le Japon et la Corée du Sud, l'UE peut tirer parti de l'expertise extérieure pour construire un écosystème de semi-conducteurs plus résistant et plus compétitif.

Le compromis entre l'autonomie stratégique et la coopération mondiale en matière d'infrastructures informatiques à grande échelle est un défi essentiel pour l'UE dans le contexte d'initiatives mondiales concurrentes telles que l'initiative chinoise Belt and Road Initiative (BRI). La BRI est une stratégie de développement mondial lancée par la Chine pour améliorer le commerce international et la connectivité des infrastructures en investissant dans un réseau mondial de routes commerciales, de ports et d'infrastructures numériques à travers l'Asie, l'Afrique, l'Europe et au-delà. Pour analyser l'ampleur du défi, nous avons regroupé les pays en trois coalitions : la coalition de l'UE, la coalition occidentale et la coalition démocratique. La coalition de l'UE comprend tous les États membres de l'UE et les pays européens étroitement associés. La coalition occidentale élargit ce groupe pour inclure les alliés occidentaux traditionnels tels que les États-Unis, le Canada, l'Australie, le Japon, la Corée du Sud et Israël, c'est-à-dire une alliance plus large de démocraties libérales. Enfin, la Coalition pour la démocratie formelle comprend non seulement les nations occidentales, mais aussi des démocraties d'autres régions, comme l'Inde, le Brésil et l'Afrique du Sud. La figure 4 compare ces coalitions avec l'Initiative de Bretton Woods et une catégorie résiduelle d'"autres" pays en dehors de ces groupes définis.

⁹² Voir : <https://www.bloomberg.com/news/articles/2024-10-24/tsmc-s-arizona-chip-production-yields-surpass-taiwan-s-a-win-for-us-push>.

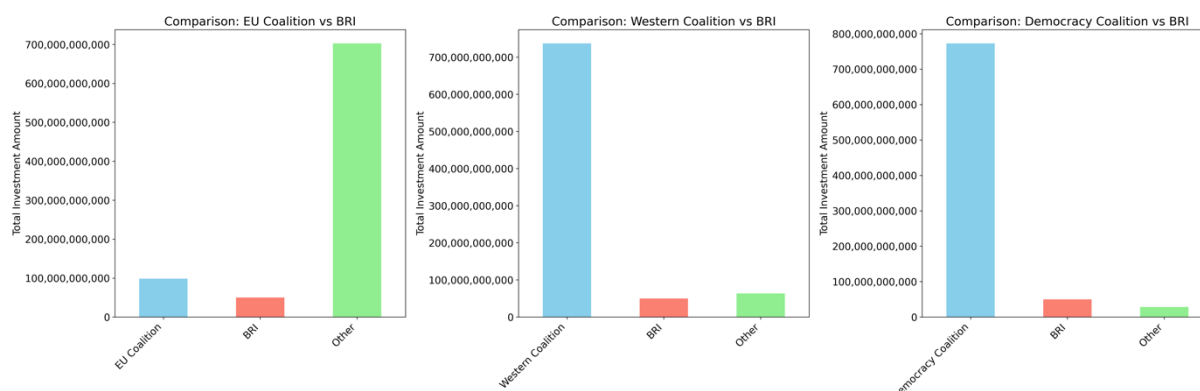
Fig.4 : Modélisation de scénarios : coalitions d'investissement possibles

Illustration personnelle et analyse des données. Données extraites du site web SemiconductorEngineering.

Les résultats de la figure 4 révèlent des différences significatives dans la capacité d'investissement en fonction de la manière dont les coalitions sont formées. Seule, une coalition étroite de l'UE accuse un retard important par rapport au reste du monde, ce qui met en évidence l'impact de la fragmentation au sein de l'UE, où les politiques divergentes en matière d'aides d'État et les initiatives nationales non coordonnées diluent la force financière collective. Dans un tel environnement, la BRI apparaît comme un concurrent de poids, tirant parti des capacités centrales de coordination et de financement de la Chine. Toutefois, si l'UE étend ses partenariats à une coalition occidentale, celle-ci domine clairement l'investissement mondial, reflétant les ressources économiques et stratégiques combinées de ses États membres. Une coalition démocratique plus large aurait une avance encore plus nette. Cette analyse souligne la nécessité pour l'UE de renforcer sa cohésion interne par le biais de mécanismes tels que les IPCEI et de cadres permanents tels que le RGEC. Elle souligne également l'importance de tirer parti de partenariats avec des alliés mondiaux de confiance. Ce n'est que grâce à cette approche équilibrée que l'UE pourra réduire sa dépendance à l'égard des systèmes extérieurs et s'imposer comme un acteur de premier plan.

6. Alors que l'UE s'est traditionnellement concentrée sur le bien-être des consommateurs en tant qu'objectif principal de sa politique de concurrence, l'ère numérique a apporté de nouveaux défis liés à la concurrence qui nécessitent une approche plus nuancée. L'approche "New Brandeisian" aux États-Unis, défendue par des universitaires tels que Lina Khan et peut-être également adoptée par l'administration Trump 2.0, représente un changement significatif par rapport à la norme traditionnelle du bien-être du consommateur.⁹³ Ce mouvement plaide en faveur d'une vision plus large de l'antitrust qui prend en compte des facteurs tels que la structure du marché, la protection des travailleurs et la préservation des petites entreprises. Par exemple, l'UE pourrait envisager d'intégrer des éléments de la nouvelle pensée brandeisienne dans son cadre de concurrence, notamment en accordant plus d'importance aux effets à long terme des fusions sur l'innovation et la structure du marché.⁹⁴ Toutefois, il est essentiel que l'UE parvienne à un équilibre qui préserve la sécurité juridique et ne décourage pas les activités commerciales légitimes. Les réseaux de coopération internationale jouent un rôle important pour relever ces défis. Le réseau européen de la concurrence (REC), qui facilite la coopération entre la Commission et les autorités nationales de la concurrence, constitue un modèle d'application transfrontalière efficace. Pour trouver un compromis entre le bien-être des consommateurs et les

⁹³ Lina Khan, 'The New Brandeis Movement : America's Antimonopoly Debate', *Journal of European Competition Law & Practice* 9, no. 3 (1er mars 2018) : 131–32, <https://doi.org/10.1093/jeclap/lpy020>.

⁹⁴ Florian Krafft, 'Should EU Competition Law Move towards a Neo-Brandeis Approach ?', *European Competition Journal* 16, no. 1 (2 janvier 2020) : 55-96.

intérêts publics plus larges, l'UE pourrait proposer la création d'un groupe de travail spécialisé au sein du Réseau international de la concurrence (RIC).

5 Conclusion : La hiérarchie des compromis

L'analyse de la politique numérique s'enlise souvent dans des détails complexes, ce qui conduit à une compréhension fragmentée qui ne tient pas compte des implications plus larges et de l'interconnexion des différents objectifs politiques. Cette approche compartimentée peut occulter les compromis inhérents, mais aussi les synergies potentielles entre les différents domaines politiques. En raison des pressions géopolitiques actuelles - exacerbées par des développements récents tels que la présidence Trump 2.0 - il est de plus en plus nécessaire d'adopter une perspective holistique qui tienne compte de l'interaction complexe entre la compétitivité, la sécurité et les droits fondamentaux. Dans ce document, nous avons fourni un cadre conceptuel pour ce faire en conceptualisant un trilemme dans l'élaboration de la politique numérique de l'UE. Ce trilemme indique que, contrairement à la rhétorique courante, l'UE ne peut pas simultanément maximiser la compétitivité économique et l'innovation, garantir la sécurité et la souveraineté et respecter pleinement les droits fondamentaux et la cohésion sociale sans faire de compromis.

Chaque étude de cas que nous avons examinée illustre les manifestations concrètes de ce trilemme :

1. Le GDPR renforce la protection de la vie privée mais impose des coûts de mise en conformité susceptibles d'entraver l'innovation et la compétitivité, en particulier pour les PME.
2. L'ASN vise à créer un environnement numérique plus sûr, mais soulève des inquiétudes quant à la liberté d'expression et impose des charges réglementaires susceptibles d'affecter la compétitivité des plateformes.
3. Des initiatives telles que la boîte à outils de sécurité 5G et les systèmes de certification du cloud donnent la priorité à la sécurité et à la souveraineté, mais risquent de peser sur les relations économiques avec les principaux fournisseurs de technologie, ce qui affecterait la compétitivité à court terme.
4. La loi sur l'IA cherche à établir des normes éthiques pour le développement de l'IA, ce qui pourrait augmenter les coûts de mise en conformité et avoir un impact sur l'innovation, en conciliant les droits fondamentaux et la compétitivité économique.
5. Des initiatives telles que la loi sur les puces électroniques et les usines d'IA visent l'autonomie stratégique mais peuvent conduire à une allocation inefficace des ressources et à des distorsions du marché intérieur, reflétant un compromis entre la souveraineté et l'efficacité économique.
6. L'évolution du rôle de la politique de concurrence de l'UE pourrait prendre en compte des préoccupations sociétales plus larges que le bien-être des consommateurs, telles que le changement climatique ou la sécurité, mais pourrait perdre de vue son objectif initial tel qu'il est formulé dans les traités et devenir trop discrétionnaire.

En regroupant nos résultats et en les reliant à notre cadre original (figure 5), ces études de cas montrent que toutes les politiques numériques et technologiques sont unies par la présence de compromis importants qui ne sont pas toujours explicitement reconnus. Le cadre du trilemme nous permet de cartographier ces compromis selon les trois axes de la compétitivité, de la souveraineté et des droits fondamentaux. Il apparaît clairement que certaines politiques impliquent plus de compromis que d'autres. Par exemple, la protection des données implique deux côtés du trilemme, tandis que la modération des plateformes touche aux trois dimensions, ce qui suggère une hiérarchie de complexité dans l'élaboration des politiques. Cette compréhension hiérarchique peut avoir des implications pour les projets actuels d'harmonisation et de rationalisation de la politique numérique de l'UE. Reconnaître les différents degrés de compromis permettent aux décideurs politiques de donner la priorité aux

questions qui nécessitent un équilibre plus nuancé et de concevoir des politiques plus cohérentes. La reconnaissance du trilemme encourage également le dialogue entre les différentes DG et les parties prenantes. Plus généralement, le nouveau commissaire européen chargé de la souveraineté technologique, de la sécurité et de la démocratie devrait être conscient du fait qu'aucune approche politique unique ne peut répondre à toutes les préoccupations sans compromettre potentiellement d'autres objectifs. Pour favoriser un écosystème numérique résilient, l'UE doit reconnaître explicitement et rapidement ces compromis et permettre un apprentissage politique au fil du temps.

Fig.5 : Résumé des résultats

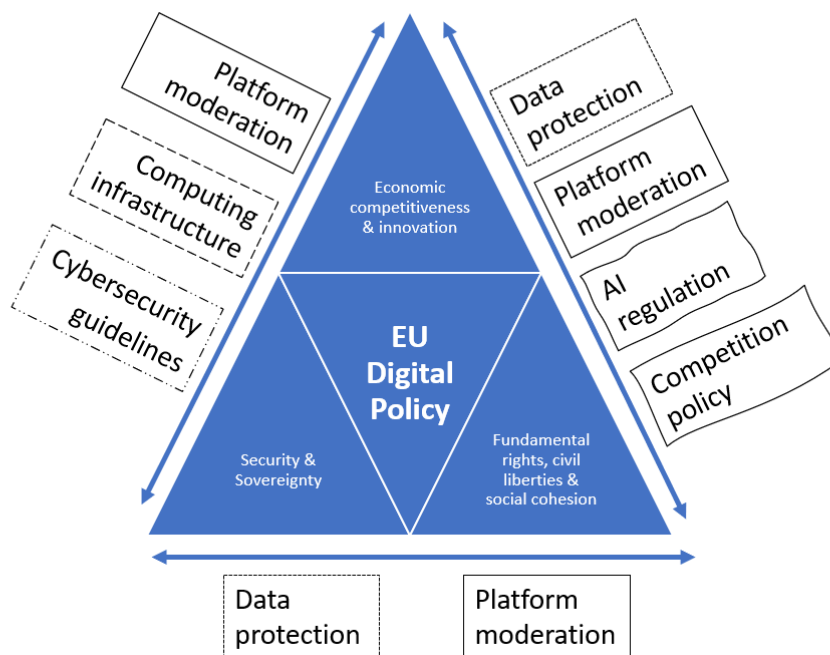


Illustration personnelle.

Dans la dernière partie de ce document, nous avons suggéré un moyen d'aborder certains des compromis par une voie qui est devenue moins populaire ces dernières années - la coopération internationale. Alors que la poursuite de l'autonomie stratégique est devenue un thème dominant de la récente politique numérique de l'UE, notre analyse suggère que la coopération internationale reste une voie importante pour atténuer les compromis inhérents identifiés dans le trilemme de la politique technologique. Par exemple, la coopération internationale offre des possibilités d'équilibrer la protection de la vie privée et l'innovation en harmonisant les normes de protection des données, comme le montrent les différents accords d'adéquation. En ce qui concerne la modération des plateformes, la collaboration avec des alliés démocratiques peut contribuer à l'élaboration de bonnes pratiques qui protègent la liberté d'expression tout en renforçant la sécurité. En matière de cybersécurité, les partenariats avec des nations technologiquement avancées peuvent renforcer les défenses de l'UE sans nuire aux intérêts économiques, par exemple grâce à des projets de R&D conjoints avec Israël. En ce qui concerne la réglementation de l'IA, la participation à des forums mondiaux tels que le Partenariat mondial sur l'intelligence artificielle permet à l'UE de promouvoir des normes éthiques sans s'isoler des réseaux d'innovation internationaux. Dans le domaine de l'infrastructure informatique, les alliances stratégiques peuvent aider l'UE à atteindre ses objectifs sans allocation inefficace des ressources, comme le montre la collaboration de TSMC avec les États-Unis. Enfin, dans le domaine de la politique de la

concurrence, les réseaux internationaux peuvent contribuer à équilibrer le bien-être des consommateurs et les intérêts publics plus larges en garantissant que l'application du droit de la concurrence de l'UE tienne compte de la dynamique mondiale sans devenir trop discrétionnaire ou isolée. Par conséquent, si l'autonomie stratégique reste importante, une stratégie équilibrée impliquant des partenariats mondiaux est essentielle pour harmoniser et rationaliser les politiques numériques de l'UE et atténuer certains des compromis inhérents au trilemme technologique.

**Auteurs :**

Anselm Küsters, LL.M.

Chef de la division Numérisation et nouvelles

kuesters@cep.eu

Dr. Cecilia Emma Sottilotta

Professeur adjoint de sciences politiques, Université pour étrangers de Pérouse (Unistrapg)

cecilia.sottilotta@unistrapg.it

Traductrice:

Emma Drouet,

Chargée de relations presses et publiques

Drouet@cep.eu

Centrum für Europäische Politik FREIBURG |

Kaiser-Joseph-Straße 266 | D-79098 Freiburg

Schiffbauerdamm 40 Räume 4205/06 | D-10117 Berlin

Tél. + 49 761 38693-0

Le **Centrum für Europäische Politik** FREIBURG | BERLIN, le **Centre de Politique Européenne** PARIS, et le **Centro Politiche Europee** ROMA forment le **réseau des Centres de Politique Européenne** FREIBURG | BERLIN | PARIS | ROMA.

Exempt d'intérêts particuliers et neutre sur le plan politique, le réseau des Centres for European Policy Network fournit une analyse et une évaluation de la politique de l'Union européenne, dans le but de soutenir l'intégration européenne et de défendre les principes d'un système économique de libre marché.