

Titre : Quel modèle pour la gouvernance du numérique au sein de l'Union européenne ?

Résumé : En matière de gouvernance du numérique, l'Union européenne (EU) tend à affirmer une voie alternative aux modèles américain et chinois qui constituerait une nouvelle pierre à l'édifice d'une progressive autonomisation numérique de l'Union. La présente tente d'en esquisser les contours au travers de l'analyse du Digital Markets Act, entré en vigueur le 2 mai 2023. Cette réglementation vise à rétablir un juste jeu de la concurrence entre les plateformes afin de permettre la croissance des entreprises européennes pourvoyeuses de services similaires aux Big Tech américains et chinois. Basée sur une revue de littérature ainsi qu'une analyse de documents officiels de l'UE, cette étude démontre que si l'Union accuse un certain retard en matière d'innovation technologique, elle vise à promouvoir un modèle de gouvernance numérique de cette dernière aligné avec ses valeurs et intérêts.

Mots clé : Union européenne, souveraineté numérique, gouvernance du numérique, Big Tech, plateformes, modèle de gouvernance

## Introduction

En 1996, John Perry Barlow, fervent défenseur de la liberté d'expression sur internet, déclarera à propos du cyberspace :

*“I declare the global social space to be naturally independent [...] Governments derive their just power from the consent of the governed. You have neither solicited nor received ours. Cyberspace does not lie within your borders”* (Barlow, 1996).

Le monde numérique ne se situe dans aucune frontière ou repère physique traditionnels, laissant ainsi libre cours au débat concernant les manières de gouverner ce nouvel espace. Cette vision prônée par ce que l'on appellera plus tard les cyberlibertaires se montre particulièrement populaire dans la Silicon Valley et s'inscrit dans un idéal selon lequel Internet constitue un nouveau monde qui se veut libre et égalitaire, bouleversant les rapports sociaux et rendant ainsi obsolètes les régulations existantes. Toute intervention étatique mettrait donc en péril les caractéristiques de ce nouveau monde (Chenou, 2014). Cette vision se voit souvent qualifiée de naïve et idéaliste car elle ne prend pas en compte les dynamiques et jeux de pouvoir autour des

ressources et avantages stratégiques animant les et leurs gouvernements depuis leur création (Mueller, 2010). C'est pourtant cette pensée qui, intégrée dans la pensée libérale américaine, a favorisé le développement des géants du numérique, ou *Big Tech* (Google, Amazon, Facebook, Apple, Microsoft, ou GAFAM), permettant aux États-Unis d'asseoir leur *leadership* en matière de numérique et d'imposer leur modèle, notamment en Europe (d'Agrain, 2022).

Ce leadership se trouve aujourd'hui contrecarré, entre autres par la Chine qui, parallèlement, a vu croître sur son territoire ses propres plateformes et technologies (Baidu, Alibaba, Tencent et Xiaomi, ou BATX, équivalents chinois des GAFAM américains), sous l'impulsion de l'État chinois, profitant du large marché qu'il représente à lui-seul. Plus récemment, c'est le succès de la plateforme TikTok aux États-Unis qui illustre la rivalité entre les deux puissances numériques, les États-Unis ayant même tenté de la faire interdire sur leur territoire (d'Agrain, 2022).

Le monde numérique recouvre désormais un large spectre de domaines. Et le cyberspace est devenu, en quelques décennies, une nouvelle arène au sein de laquelle les ambitions géopolitiques des uns et des autres peuvent se rencontrer ou s'affronter.

L'Union européenne (EU) se situe en marge, tributaire des États-Unis pour ce qui concerne les services offerts par les GAFAM, et dépendante de la Chine sur le marché des micro-puces. Elle cherche désormais à se soustraire à ces deux modèles dominants et à proposer une voie alternative, fondée sur les valeurs européennes (Commission Européenne, 2021a). L'UE met donc un point d'honneur à mettre en place de nouveaux instruments contribuant à asseoir sa souveraineté dans le monde du numérique. Le Digital Markets Act (DMA), en vigueur depuis mai 2023, ambitionne de réguler l'espace numérique intra-européen en actionnant les leviers du droit de la concurrence et de l'obligation d'interopérabilité des plateformes<sup>1 2</sup>.

Dès lors, comment l'UE se positionne-t-elle au sein de cette nouvelle arène de confrontation des intérêts ? Pour répondre à cette question, cet article propose une analyse non exhaustive des instruments politiques permettant à l'UE d'affirmer une nouvelle forme de gouvernance. Il passe ainsi en revue l'instrument clé que constitue le Règlement Général sur la Protection des Données, considéré comme l'une des premières grandes avancées européennes dans cette

---

<sup>1</sup> L'article 7 du DMA impose aux « services de communications interpersonnelles » de rendre les « fonctionnalités de base de leur service interopérables avec tout autre fournisseur qui propose ou à l'intention de proposer de tels services dans l'Union ».

<sup>2</sup> Le terme de plateforme sera utilisé selon la définition de l'académicien Nick Srnicek : « Les plateformes sont des infrastructures numériques qui permettent à deux ou plusieurs groupes d'interagir. Elles se positionnent ainsi comme des intermédiaires rassemblant différents utilisateurs. [...] Elles s'appuient sur l'effet 'réseaux' : plus une plateforme accumule un grand nombre d'utilisateurs, [...] plus elle dispose de données et plus elle gagne en valeur » (Srnicek, 2017, p. 45, [Traduction de l'auteure]).

matière. Il analysera, ensuite, le DMA comme instrument de politique extraterritoriale de l'UE et de potentiel contrebalancement de l'omniprésence des GAFAM sur son territoire. Cette analyse visera à répondre à la question de recherche suivante : « Comment l'UE, au travers de ces instruments, tente-t-elle d'affirmer sa place au sein de la gouvernance du numérique et de proposer une alternative aux modèles existants ? »

## **La souveraineté numérique européenne**

Il est d'abord nécessaire de mettre l'accent sur la définition du concept de souveraineté numérique ainsi que d'en dégager les différents modèles théoriques et leurs applications concrètes, aussi bien en Chine qu'aux États-Unis. Cette mise en perspective permet de dégager les éléments de contexte justifiant la refonte de la politique européenne du numérique et des objectifs stratégiques qu'elle entend servir, notamment à travers la mise en place du DMA.

De prime abord, lorsque l'on tente de définir ce qu'est la souveraineté numérique au sein de l'UE, il s'avère rapidement qu'il s'agit d'un concept recouvrant un large éventail de domaines (Madiega, 2020). Par sa complexité, ce concept laisse place à diverses interprétations quant aux objectifs que les politiques européennes de protection de données recouvrent réellement ainsi qu'aux capacités objectives dont l'UE dispose pour établir un agenda efficient (Roberts et al., 2021). Cependant, la plupart des auteurs s'accordent sur le fait que la souveraineté numérique s'aligne de façon globale sur l'ambition européenne de se positionner en acteur incontournable du numérique, en se dotant de moyens technologiques qui servent des objectifs aussi bien économiques que sécuritaires (Monsees et Lambach, 2022). Elle est présentée dans ce contexte comme « un moyen pour l'UE de développer une société sécurisée et résiliente, d'assumer une position de leader au sein du système international et d'affirmer son autonomie par rapport à certaines parties du monde » (Bellanova et al., 2022, p. 338, [Traduction de l'auteure]). Aujourd'hui inscrite dans un environnement d'interdépendances vis-à-vis d'un large panel d'acteurs (Bellanger, 2012), l'enjeu pour l'UE implique de se positionner comme un acteur incontournable du numérique en imposant son modèle, régi par ses propres normes (Irion, 2022).

Le concept de souveraineté numérique est souvent associé à la « capacité d'agir de façon indépendante dans le monde numérique » (Madiega, 2020, p. 1). Dans ce contexte, elle est perçue comme une forme d'autorité légitime de contrôle (Floridi, 2020) sur les diverses infrastructures numériques, aussi bien matérielles qu'immatérielles, qui transcendent les

frontières territoriales et physiques que nous connaissons (Celeste, 2020). En effet, la souveraineté appliquée au domaine du numérique ne s'entend plus au sens westphalien du terme ; elle ne dépend plus uniquement des prérogatives d'un État en particulier ou d'une entité publique, elle relève désormais partiellement d'organisations privées qui se substituent à l'État, notamment pour ce qui concerne les régulations appliquées aux plateformes (Roberts et al., 2021).

Les acteurs privés détiennent dès lors un rôle prépondérant dans la mise en place des politiques et font partie intégrante du développement technologique de l'UE (Farrand et Carrapico, 2022). En 2021, lors d'une intervention conjointe de la Présidente de la Commission européenne Ursula von Der Leyen et du Premier Ministre néerlandais Mark Rutte, von der Leyen affirme l'importance de l'effort des entreprises du secteur numérique pour rendre l'UE plus compétitive en termes de technologie (von der Leyen, 2021).

Le discours de von der Leyen fait écho aux déclarations de la Commission européenne (CE) de 2020 qui pointaient les entreprises comme leaders de l'innovation et du développement d'outils permettant d'asseoir la compétitivité économique de l'Europe et d'améliorer la qualité de vie de ses citoyens (CE, 2020a). La souveraineté numérique de l'UE est ainsi envisagée comme une étroite collaboration avec les acteurs économiques du secteur privé en tant que socles sur lesquels s'appuyer pour mener à bien les politiques européennes du numérique (Farrand et Carrapico, 2022). Précisons que l'EU opère une distinction entre les entreprises privées, identifiées comme piliers du développement technologique, qui s'alignent avec les valeurs européennes telles que la démocratie et l'état de droit et d'ouverture commerciale, et les entreprises non européennes présentes sur le marché qui répondent aux normes américaines ou chinoises (Farrand et Carrapico, 2022).

Les régulations à destination du monde numérique sont, dans ce contexte, plutôt perçues comme des outils servant l'extra-territorialisation des normes et valeurs européennes en termes de protection des données personnelles, des lois de protection des consommateurs et du droit de la concurrence (CE, 2020b). La souveraineté numérique européenne recouvre ainsi quatre dimensions majeures : la compétitivité économique, l'autonomie stratégique, la sécurité et la cybersécurité, et la diffusion des valeurs européennes (Roberts et al., 2021).

## **La gouvernance du numérique : différents modèles d'application**

L'enjeu du numérique est souvent présenté comme une problématique ancrée dans la rivalité entre la Chine et les États-Unis, notamment caractérisée par deux approches tout à fait distinctes

en termes de gouvernance du numérique. À cet égard, l'UE se revendiquerait comme une voie alternative aux modèles américain et chinois (Schneider, 2020).

Dans son acception générale, le fait de gouverner se définit par la capacité d'un État à émettre et à faire respecter ses normes. Cependant, pour répondre aux besoins actuels, la gouvernance doit désormais s'envisager au-delà d'une vision strictement stato-centrée, afin de prendre en compte la multitude d'acteurs et dynamiques de pouvoirs ou conflits constituant la gouvernance globale du XXI<sup>e</sup> siècle. Gorwa reprend la définition émise par Stoker en 2017 : la gouvernance « *[is about] creating the conditions for ordered rule and collective action* » (Gorwa, 2019a, p. 856) . Elle ne se résume donc plus à la simple capacité de gouverner, mais comprend aujourd'hui un large réseau d'acteurs mus par des comportements différents. En bénéficiant d'un lien direct avec leurs utilisateurs et par l'émission de leurs propres politiques, règlements et nouveaux modes de modération, les plateformes sont désormais considérées comme acteur à part entière de la gouvernance globale. Gorwa établit trois modèles d'application de la gouvernance des plateformes.

### **Self governance**

Relativement dominant, le modèle de l'autorégulation ou de la gouvernance autonome est caractérisé par une intervention minimaliste de la part des institutions de gouvernance dans la régulation des plateformes numériques. Ces dernières agissent en tant qu'intermédiaire entre leurs utilisateurs. Bien que n'étant pas tenues responsables des contenus échangés entre ces derniers, les plateformes numériques sont également investies d'un rôle de modérateur. Pour autant qu'elles répondent aux injonctions de leurs utilisateurs, l'État se tient en retrait (Gorwa, 2019a). C'est ce que Floridi (2020, p. 372) nomme la « digital corporate governance ». Cette approche de la gouvernance des plateformes répond ainsi à la logique libérale américaine selon laquelle l'État n'intervient pas au sein du secteur privé. Les règles établies par les entreprises, si elles ne sont pas acceptées par les consommateurs, se voient sanctionnées par les lois du marché, en d'autres termes, par la concurrence et le libre choix de l'utilisateur (Floridi, 2020).

Globalement ancrée dans la vision libérale, le modèle de gouvernance des plateformes aux États-Unis s'envisage néanmoins différemment de part et d'autre du pays, sur les côtes Est ou Ouest (d'Agrain, 2022).

Héritière du mouvement cyberlibertaire, la gouvernance californienne de la Silicon Valley se base sur un modèle d'ouverture absolue, de liberté, d'accessibilité et de croissance technologique illimitées. Elle est incarnée par l'implantation des GAFAM (O'Hara et Hall,

2018) ou encore par la tenue chaque année du festival Burning Man (Alexandre, 2018). Dans l’imaginaire américain, la Silicon Valley et le festival Burning Man représentent la créativité, les hautes technologies et les expérimentations à haut potentiel d’innovation (Alexandre, 2018) se devant d’être encouragées (Schneider, 2020). Par ailleurs, dans cette approche où la formule « *innovate until it is shown to be harmful* » est d’application (O’Hara et Hall, 2018, p. 6), les problèmes et dangers potentiels émergents trouvent en première instance des solutions technologiques<sup>3</sup>. Dans cette perspective, le « *multistakeholderism* » devient le mode de gouvernance privilégié. Cette approche se présente comme une individualisation de la participation politique ; elle accorde aux individus une forme d’indépendance par rapport aux institutions dans le processus de décision. En effet, les institutions garantissent le bon fonctionnement du marché en éditant des lois qui en assurent la structure, tout en demeurant plus inclusive qu’une approche intergouvernementale. Les lois du marché et de la concurrence restent perçues comme la meilleure forme de régulation (Chenou, 2014).

Même si elle s’aligne sur l’approche libérale prônée par le côté Ouest, la côte Est déploie, en outre, un aspect plus sécuritaire. Du côté de Washington, le cyberspace est perçu comme un nouvel espace d’affrontements géopolitiques mu par des pensées stratégiques et politiques, au sein duquel des forces de nature militaire peuvent être déployées. Cet espace nécessite donc de repenser la stratégie militaire, les attaques de type cyber s’étant multipliées ces dernières années.

Selon Schneider (2020), c’est la première approche, dominante dans la vision américaine, qui a permis à ces plateformes de croître massivement ces deux dernières décennies. En attirant de plus en plus d’utilisateurs, ces plateformes ont pu capitaliser sur les données qu’elles collectent, obtenant ainsi les ressources pour diversifier leur offre et intégrer de nouveaux services, garantissant de la sorte la fidélisation de leurs utilisateurs. Elles se sont donc progressivement attribué le monopole des services numériques, leur permettant de récolter toujours plus de données (de natures personnelle ou industrielle). Contrairement au modèle européen, le modèle américain se montre plus tolérant vis-à-vis des prises de positions monopolistiques.

Le « laissez-faire » qui caractérise l’approche américaine de la gouvernance des plateformes s’ajoute finalement au panel des raisons incitant les autres États, et l’UE, à émettre des régulations contrôlant l’entrée de ces géants américains sur leurs marchés (Schneider, 2020).

---

<sup>3</sup> Par exemple, la plateforme Whats’App a mis en place des outils pour éviter la diffusion de fake news sur son réseau (O’Hara et Hall, 2018).

## **External governance ou state governance**

Ce modèle de gouvernance émerge suite à de nouvelles revendications pour plus de contrôle, de régulation et de fermeté dans les processus de traitement des données par les plateformes. Ces interventions extérieures s'articulent souvent autour de trois leviers d'action : la mise en place de régulations de protection des données et de la vie privée ; le rejet de la non responsabilité des intermédiaires ; et l'utilisation du droit de la concurrence et la limitation des abus de position dominante. Ces régulations obligent les plateformes à appliquer et à respecter un mode opératoire défini pour traiter les données. Elles leur imposent une obligation de transparence et des niveaux adéquats de protection des données au-delà de leur propre mode réglementaire (Gorwa, 2019a, p. 863). En Chine, ce sont les « *Guiding Opinions on Promoting the Regulated and Healthy Development of Platform Economy* », émises en 2019, qui caractérisent les leviers mentionnés par Gorwa. En effet, ce document encourage les entreprises chinoises du numérique à améliorer leur interopérabilité afin de lutter contre les abus de position dominante. Le gouvernement chinois est souvent défini comme un modèle autoritaire (Fei, 2023) et est caractérisé par sa mainmise sur les *Big Tech* chinois, utilisés à des fins d'espionnage et de surveillance de la société chinoise. Ces mécanismes soulèvent d'ailleurs certaines inquiétudes de la part d'États tiers (Farrand et Carrapico, 2022).

Au-delà des leviers mentionnés dans le modèle de Gorwa, l'État Chinois privilégie une forme de gouvernance externe institutionnalisée. Avant de la détailler, il convient de préciser que ces plateformes opèrent quasiment exclusivement au sein du marché chinois et que les données qu'elles récoltent sont stockées par ces opérateurs en Chine, facilitant ainsi leur exploitation par la suite (Liu et Yang, 2022).

Alors que les États-Unis opèrent une division claire entre le marché des plateformes et la gouvernance, la Chine semble promouvoir un modèle beaucoup plus intégré. En effet, la Chine possède ses propres plateformes, capturant la quasi-totalité du marché numérique chinois, de l'e-commerce aux moteurs de recherche en passant par les solutions de paiement. Même si elles sont détenues par des actionnaires privés, ces plateformes et les données qu'elles rassemblent font partie intégrante de la stratégie digitale chinoise (Schneider, 2020).

En ce qui concerne le mode de gouvernance des plateformes en Chine, l'État chinois adopte des régulations qualifiées de « proactives » (Liu et Yang, 2023, p. 308) qui se déclinent en deux volets : le premier concerne la gouvernance du contenu véhiculé par les plateformes ; le second

met l'accent sur la gouvernance des technologies elles-mêmes dans le rapport entre les entreprises concernées et le gouvernement chinois (Liu et Yang, 2023).

Dans le premier cas, compte tenu de la culture collectiviste de la société chinoise, la gouvernance des contenus s'inscrit dans un mécanisme de filtrage strict des discours diffusés sur les plateformes, aussi bien de la part des utilisateurs que des créateurs. Le gouvernement joue ainsi un rôle central dans la modération du contenu en privilégiant une approche top-down<sup>4</sup>. Par ailleurs, ce mode de régulation se fonde sur une importante base sociale. En effet, les individus y jouent un rôle capital car c'est sur base de leurs rapports et dénonciations que les contenus jugés illégaux sont signalés au gouvernement. En 2020, 15 millions de signalements par mois étaient enregistrés (Liu et Yang, 2023).

Pour ce qui est du second volet, les plateformes n'agissent pas en électrons libres au sein du marché chinois. Elles sont soumises à de fermes régulations et sont chargées de maîtriser la modération et la diffusion des contenus. Elles sont placées sous la stricte surveillance des agences du gouvernement et doivent d'ailleurs rendre des comptes sur leurs opérations (Liu et Yang, 2023).

Enfin, l'essor du modèle chinois repose sur deux axes : le développement et la digitalisation. En refusant systématiquement les services proposés par les États-Unis, il a développé, sur son territoire, ses propres technologies tout en conservant une faible pénétration étrangère sur son marché (Nouveau, 2022).

## **Co governance**

Ce dernier modèle est celui que l'on qualifie de moyen terme ou d'équilibre entre les deux modèles précédents. Il inclut la possibilité d'y intégrer une certaine responsabilité démocratique des plateformes, sans pour autant en modifier complètement leur fonctionnement. En créant un organe chargé de traiter les revendications des utilisateurs et d'édicter un cadre éthique, les États pourraient faire appliquer par les plateformes un code de conduite, dans un processus de concertation et de coopération (Gorwa, 2019a). Cette autre voie esquissée par Gorwa inclut la participation de groupes extérieurs à l'élaboration des standards de communauté des plateformes. Cette option leur permettrait de gagner la confiance de leurs utilisateurs tout en légitimant leurs décisions (Gorwa, 2019a).

---

<sup>4</sup> La « Chinese Cyberspace Administration » (CAC) envoie ses directives aux CAC régionales qui les appliquent ensuite au sein des petites divisions locales (Liu et Yang, 2023).



Dans ce modèle, chaque acteur ou groupe d'acteurs disposerait d'une certaine latitude à mettre en place des régulations et aurait la capacité d'intervenir différemment à chacune des nombreuses étapes de l'implémentation d'une politique ou d'une régulation. Gorwa cite l'exemple des ONG. Selon l'auteur, bien qu'elles jouissent parfois d'une grande représentativité et d'un poids significatif au sein de certaines institutions multilatérales, elles ne disposeront jamais des capacités de mise en œuvre d'une grande plateforme, alors que cette dernière agira toujours selon ses propres intérêts. Les États, quant à eux, disposent d'un rayon d'action et d'exécution importants mais dépendent des plateformes pour l'approbation de leurs opérations. Tous les éléments précités constitueraient les éléments nécessaires à la mise en place d'une collaboration entre les différents acteurs pour l'implémentation d'une régulation légitime et efficace (Gorwa, 2019b).

## Quel modèle pour l'UE ?

A l'origine, l'UE doit son existence à une volonté commune de coopération économique entre les États. La majorité de ses prérogatives étant d'ordre économique et normatif, elle s'est rarement positionnée sur la scène internationale comme un acteur à part entière de la géopolitique (Broeders et Kaminska, 2022). Cependant, depuis l'avènement du système international multipolaire et d'une rivalité croissante entre la Chine et les États-Unis, l'UE tend à s'affirmer sur la scène internationale, notamment à travers son discours de souveraineté numérique et d'autonomie stratégique (Broeders et Kaminska, 2022). A cet égard, la Présidente de la CE déclare en 2019 : « *the geopolitical Commission [...] that Europe urgently needs* » (von der Leyen, 2019). Étant donné l'importance des flux transfrontaliers de données, tant au sein de l'UE que sur le marché international, l'UE se donne comme objectif d'imposer de nouveaux standards de protection des données (Bradford, 2020a).

La vulnérabilité et la dépendance technologique des États européens se sont particulièrement révélées au cours de ces dix dernières années à travers les affaires Snowden<sup>5</sup> et Cambridge Analytica<sup>6</sup>. Elles ont d'ailleurs engendré un nouveau débat au sein des sphères politiques

---

<sup>5</sup> En 2013, le lanceur d'alerte et ancien membre de la « Central Intelligence Agency et de la National Security Agency », Edward Snowden, met à jour le plus grand scandale lié à de la surveillance de masse opérée par les services secrets américains. Dans ses révélations, Edward Snowden explique les méthodes d'infiltration des algorithmes par les services américains et britanniques à des fins de collectes de données et d'affaiblissement de standards technologiques (Utersinger, 2019).

<sup>6</sup> Le scandale lié à l'entreprise « Cambridge Analytica » est mis au jour par les journaux *The Guardian*, *The Observer* et *The New York Times*. Cette affaire, suite à l'élection de Donald Trump en tant que Président des États-Unis, révèle l'exploitation massive de données utilisées afin d'influencer le résultat des élections. « Cambridge Analytica » est accusée d'avoir utilisé les données de 30 à 70 millions de personnes, notamment via le réseau

européennes et incité à établir de nouvelles législations qui permettraient de garantir la souveraineté technologique de l'Europe et l'application de ses standards à des firmes non européennes (Danet et Desforges, 2020), avant de se voir elle-même soumise à des réglementations susceptibles de porter atteinte aux intérêts européens (Bradford, 2020a). C'est notamment à la suite de ces débats que le « Privacy Shield » et le Règlement Général pour la Protection des Données (RGPD) sont adoptés en 2016 (Nocetti, 2018).

Le « Privacy Shield » vise à mettre en place un cadre de régulation pour le transfert des données de l'UE vers les États-Unis. Selon cet accord, le « Department of Commerce » s'engage à mettre en place un cadre jugé conforme aux principes de respect de la vie privée (Commission Implementing Decision (EU) 2016/1250, 2016, point 14) garanti par l'UE, repris à l'article 8 de la Convention Européenne des Droits de l'Homme et mis en application par le RGPD. Ces principes, énumérés au point 2.1. de la décision, garantissent un niveau adéquat de sécurisation des données ainsi qu'une obligation de notification, auprès des usagers, des informations potentiellement utilisées dans le cadre d'objectifs identifiés et limités lors de la passation d'un contrat (Commission Implementing Decision (EU) 2016/1250, 2016).

Placée au rang de droit fondamental dans le traité de Lisbonne, la volonté européenne de protéger les données personnelles de ses citoyens s'illustre, entre autres, dans le RGPD en étendant son champ d'application aux entreprises non européennes, dès lors qu'elles proposent leurs services à des résidents européens ou qu'elles sont présentes sur le territoire européen (Règlement (UE) 2016/679, 2016, art. 3).

Ce dernier instaure ainsi les bases sur lesquelles les transferts de données peuvent être effectués. Ils doivent faire l'objet d'une approbation de la CE, après évaluation du caractère adéquat du niveau de protection garanti par le pays tiers concerné par ces transferts (RGPD, art. 45), ainsi que des voies de recours possibles offertes par ce même pays tiers en cas de non-respect des standards imposés (RGPD, art. 47).

Par ailleurs, le RGPD se répercute également dans la doctrine et les pratiques juridiques européennes, notamment au travers de l'arrêt du 6 octobre 2015, opposant le Data Protection Commissioner à Maximilian Schrems, et de celui du 16 juillet 2020, opposant le Data Protection Commissioner à Facebook Ireland Ltd. et Maximilian Schrems (ci-après respectivement dénommés Schrems I et Schrems II). Ces arrêts constituent des interprétations importantes de la Charte ainsi que du RGPD, en invalidant par deux fois des accords

---

social Facebook, afin d'en effectuer des profilages et de leur proposer des contenus pouvant orienter leur vote final (Audureau, 2018).

commerciaux liés à des transferts de données entre les États-Unis et l'UE, alors même qu'ils avaient été préalablement signés par la CE<sup>7</sup>.

Consciente de l'importance du marché qu'elle représente, l'UE devient pionnière dans le domaine de la protection des données et étend son influence à l'international (O'Hara et Hall, 2018). C'est ce que l'académicien Bradford nomme le « Brussels effect ». *De facto*, le marché européen est un client d'importance considérable pour ces entreprises. Les plateformes telles que Facebook et Google comptabilisent plus de 250 millions d'utilisateurs en Europe, représentant ainsi 25 % des parts de marché de Facebook et contribuant à faire de Google une plateforme utilisée par 90 % de la population des États membres (chiffre supérieur à celui des États-Unis où se situe la maison mère). Il devient ainsi de plus en plus difficile pour ces entreprises de contourner les lois émises par l'UE en matière de protection des données si elles souhaitent conserver leurs parts de marché. *De jure*, le RGPD s'est avéré suffisamment influent pour que certaines parties du monde s'en emparent comme modèle. En devenant l'une des conditions pour passer des accords de marché avec l'UE, les standards européens se sont ainsi progressivement imposés dans près de 120 pays à travers le monde (Bradford, 2020b). À cet égard, John Bowman, ancien membre des négociations sur le RGPD pour le Royaume-Uni déclarait : « *Europe wanted to be seen selling a global standard [...] That's crystallized through its adequacy decisions* » (Cerulus et Scott, 2018).

## **Principes pour un nouveau cadre de gouvernance pour la souveraineté numérique européenne**

Au vu de notre analyse, la stratégie européenne semble s'articuler selon deux axes principaux : le développement de ses industries et le maintien du contrôle de leur transition numérique (Broeders et al., 2023). Depuis quelques années, l'UE a développé nombre important d'initiatives ayant pour objectif de mettre en place de nouveaux instruments politiques en ligne avec les objectifs susmentionnés. Premièrement, les politiques visent d'abord les concurrents

---

<sup>7</sup> Par deux fois, Maximilian Schrems fait valoir dans ses plaintes qu'il souhaite faire interdire à Facebook Ireland Ltd. de transférer ses données vers Facebook Inc. (basée aux États-Unis), argumentant que le droit américain ne permet pas de garantir un niveau adéquat de protection des données à caractère personnel. Dans l'arrêt Schrems I, c'est le EU-US Safe Harbour qui est remis en question et finalement invalidé par la Cour de Justice de l'Union Européenne (C.J.U.E.), faute de garantie suffisante de la protection des droits des résidents européens (*Shrems I*, points 98, 106 et 107). Dans le deuxième cas, la C.J.U.E. argumente que la décision du BPD (Bouclier de Protection des Données, ou *Privacy Shield*) ne permet pas non plus un recours devant des organes offrant des « garanties substantiellement équivalentes » à celles requises par l'article 47 de la Charte. Le *Privacy Shield* est déclaré incompatible avec l'article 45 du RGPD, les articles 7, 8 et 47 de la Charte et est ainsi invalidé dans sa totalité (*Shrems II*, point 56 et points 197 à 202).

externes et les pays tiers (comme les États-Unis ou la Chine). Ensuite, au niveau interne, ces mesures visent à promouvoir une coopération intra-européenne afin d'unir les capacités et les ressources favorisant la réussite de ces projets (Broeders et al., 2023). En effet, l'UE a pour objectif de se soustraire à l'influence des États-Unis et la Chine dont les biens et services inondent le marché européen, laissant ainsi ses propres entreprises et citoyens à la merci de technologies dont ils n'ont pas le contrôle (Celeste, 2020).

Il s'agit là des objectifs clés qui devront, par la suite, faire l'objet de régulations pour les mener à bien et assurer de la sorte un positionnement de « *trendsetter* » (CE, 2020c, p. 2) dans le domaine du numérique sur la scène internationale. Le premier principe s'articule autour du développement de technologies amenées à intégrer, de plus en plus, le quotidien des citoyens européens (CE, 2020c). Le deuxième objectif concerne le marché qu'elle souhaite, autant que possible, équitable et compétitif. Au sein du marché unique, les entreprises, indépendamment de leur taille, seraient ainsi assurées d'un juste jeu de la concurrence et du respect des droits du consommateur (CE, 2020c). Le troisième principe de la gouvernance s'oriente vers les valeurs démocratiques de l'UE visant à rassurer les citoyens européens quant à l'usage des données qu'ils fournissent, aussi bien en ligne qu'hors ligne. Enfin, l'UE mise sur un partenariat multi-niveaux et transnational entre la CE, les États membres et les industries de premier plan dans le domaine du numérique (Nouveau, 2022).

En énonçant ces nouvelles orientations politiques, le défi auquel s'attelle désormais l'UE consiste à s'affirmer comme nouveau pouvoir géostratégique. Compte tenu de ses prérogatives limitées en tant qu'acteur international dans les affaires étrangères, elle fonde cette nouvelle position sur son important pouvoir normatif et politique en se basant sur ses piliers que sont le libre marché et la protection des droits humains. Elle y adjoint une dimension géopolitique et économique en promouvant une voie alternative à celles actuellement partagées par le duopole sino-américain (Broeders et al., 2023).

### **Nécessité d'implémentation d'une nouvelle norme**

En 2020, la CE déclare que les données représentent désormais un pilier du développement économique. La mise en place d'une « économie fondée sur les données » (CE, 2020c, p. 3) serait donc essentielle pour booster l'innovation et la compétitivité en facilitant un échange sécurisé au sein de l'UE. Cependant, comme explicité précédemment, la plupart des données sont pour le moment détenues par un petit nombre de firmes américaines, rendant ainsi l'accès à ce marché très difficile pour des entreprises européennes (CE, 2020c). En effet, la position

monopolistique des plateformes sur les marchés numériques leur octroie, par défaut, un rôle de « point d'accès ou de contrôleur d'accès » (Proposition de règlement du Parlement européen et du Conseil 2020/0374, 2020, p. 1)<sup>8</sup>, notamment grâce à la solidité et la durabilité de l'écosystème qui s'articule autour de leurs services. Leur puissant ancrage sur les marchés rend les entreprises utilisatrices dépendantes de ces contrôleurs d'accès, occasionnant nombre de comportements déloyaux et une difficile contestabilité de leur position. La CE estime donc qu'il est important d'harmoniser, au sein de tous les États membres, les régulations touchant au droit de la concurrence dans le secteur numérique (Proposition de règlement du Parlement européen et du Conseil 2020/0374, 2020).

Les Petites et Moyennes Entreprises (PME) souhaitant se développer sur les marchés numériques doivent pouvoir compter sur des régulations appliquées de façon uniforme, transparente et efficiente sur le territoire de l'UE, ainsi que sur un marché à domicile équitable pour leur permettre de se lancer à l'international (CE, 2020c). A cette fin, l'UE émet donc des politiques ambitieuses afin d'extra-territorialiser ses valeurs et standards tels que le marché libre en étendant prioritairement à des entreprises étrangères le champ d'application de certaines de ses régulations sur le numérique (Bendiek et Stürzer, 2022).

## **Digital Markets Act : nouvel outil au service des ambitions stratégiques de l'Union européenne**

« L'adjectif stratégique qualifie [...] tout ce qui représente une valeur fondamentale pour un acteur » (Rosière, 2001, p. 41) et la stratégie définit « le mode opératoire pour atteindre [ses] objectifs » (Rosière, 2001, p. 38). Si l'on considère traditionnellement la géopolitique comme l'étude des dynamiques politiques s'exerçant au sein d'un État ou entre États, elle concerne désormais toutes les échelles de territoires (Rosière, 2001). Et comme nous l'avons déjà établi précédemment, l'espace numérique est devenu, depuis plusieurs décennies, un nouveau théâtre où se rencontrent de nouvelles ambitions stratégiques.

### **Objectifs et principes d'application**

La tendance monopolistique des grandes entreprises américaines sur le territoire européen est basée, notamment, sur la puissance de leurs algorithmes, affaiblissant dès lors les nouveaux

---

<sup>8</sup> La notion de « contrôleur d'accès » ou de *gatekeeper* est définie plus en détails dans la section suivante.

arrivants sur un marché déjà barricadé. L'incapacité de l'UE à traiter ces situations via les outils traditionnels du droit de la concurrence ont incité les États membres à envisager l'implémentation de mesures plus fermes (Timmers, 2022).

En effet, les articles 101 et 102 du Traité sur le Fonctionnement de l'UE (TFEU) ne permettent des interventions qu'*ex-post* de la part de la CE, et ces interventions ne sont possibles qu'après enquête ayant fait la preuve de comportements anticoncurrentiels ou abusifs (TFUE, article 105, §1, 2 et 3). Ces enquêtes impliquent de longs délais, parfois de plusieurs années. En conséquence, des résultats économiques équitables ne sont que très peu garantis en ce qui concerne les services de plateforme dits « essentiels » (Règlement (UE) 2022/1925, 2022).

Le DMA s'attache ainsi à poser les bases d'une régulation *ex-ante*, encadrant les comportements interdits pour les plateformes dites « contrôleurs d'accès ». En leur imposant une certaine ligne de conduite, la CE espère pouvoir rendre ses interventions plus efficaces. En effet, ce type de régulation *ex-ante* n'exige pas l'établissement de preuve, la simple non-conformité au règlement devant suffire à éviter certains abus et comportements anticoncurrentiels par l'application de sanctions (Van Cleynenbreugel, 2021).

Dans son considérant (7), la loi sur les services numériques stipule deux objectifs, le premier s'articulant autour de règles visant à garantir la contestabilité et l'équité des marchés, et le deuxième autour de garanties réglementaires contre les pratiques déloyales uniformisées afin d'éliminer la fragmentation existante ou d'éviter qu'elle apparaisse. À cet égard, le DMA, dans ses considérants (91) et (94), accorde à la CE toutes prérogatives de désignation des contrôleurs d'accès définis selon les critères objectifs stipulés dans l'article 3 du DMA<sup>9</sup>. Lorsque ces seuils sont atteints, il incombe aux entreprises de transmettre ces informations à la CE. Elle se réserve le droit de désigner un contrôleur d'accès sur base des informations dont elle dispose si l'entreprise n'a pas fait part, volontairement, des bilans de ses derniers exercices. Si une entreprise est désignée comme « gatekeeper », elle disposera de six mois à compter du moment de sa nomination pour se conformer aux obligations qui lui incombent (DMA, art. 3, §10).

Le DMA étant applicable depuis le 2 mai 2023, sept entreprises ont déclaré rencontrer les critères mentionnés ci-dessus : Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft et Samsung. Après examen des informations transmises, les six entreprises américaines de la liste

---

<sup>9</sup> Article 3 : i) L'entreprise a réalisé un chiffre d'affaires annuel dans l'Union équivalent ou supérieur à 7,5 milliards d'euros ou sa capitalisation boursière atteint un minimum de 75 milliards d'euros au cours du dernier exercice et elle fournit le même service à au moins trois pays au sein de l'Union, ii) Ce service a bénéficié, mensuellement, à au moins 45 millions d'utilisateurs et annuellement, à au moins 10 000 entreprises établies dans l'Union Européenne, iii) On considère que l'entreprise bénéficie d'une position « solide et durable » ou jouira probablement de cette position dans un avenir proche si les précédents seuils (cités en ii) ont été atteints au cours des trois derniers exercices.

se sont vues accorder ou non le statut de contrôleurs depuis le 6 septembre 2023 (CE, 2023a). Ces dernières se trouvent donc désormais sous le coup d'obligations bien précises visant à atteindre les deux objectifs susmentionnés. Les « gatekeepers » doivent permettre aux entreprises utilisatrices de proposer des produits similaires sur leurs plateformes et de se rendre interopérables avec les services offerts par des concurrents. Par ailleurs, l'utilisation des données récoltées sur leurs utilisateurs finaux se trouve désormais strictement régulée par l'article 5 du DMA. Enfin, pour s'assurer du respect de la règle, le contrôleur d'accès ne peut pas restreindre « directement ou indirectement la possibilité pour les entreprises utilisatrices ou les utilisateurs finaux de faire part à toute autorité publique compétente, y compris les juridictions nationales, de tout problème de non-respect, par le contrôleur d'accès, du droit de l'Union ou national pertinent dans le cadre des pratiques de ce dernier » (DMA, art. 5, §6).

En régulant le jeu de la concurrence, l'UE espère permettre à ses PME, également fournisseurs de services essentiels, de prospérer. Sur le long terme, l'affaiblissement des barrières bloquant l'accès au marché devrait permettre de le rééquilibrer et d'ouvrir ainsi une place aux entreprises européennes sur les marchés numériques, du moins en Europe.

Le DMA sert ainsi l'objectif de la CE, énoncé dans la *European Strategy for Data*, de faire prospérer les entreprises européennes fournissant des services similaires. Elle espère ainsi que les données européennes seront stockées de plus en plus massivement au sein de l'espace européen. Ce faisant, la CE pourrait en garantir la sécurité. En sécurisant ses données dans des « clouds » adéquats (« European health data space », « European financial data space », « European energy data space », etc.), l'UE pourrait potentiellement atteindre son objectif de « data space » européen<sup>10</sup> et favoriser un échange transfrontalier européen de données, les données étant devenues moteur de l'innovation. Cette innovation, favorisée par la mobilisation des données, devrait pouvoir soustraire l'UE à ses dépendances technologiques (CE, 2020b). En créant les conditions d'émergence d'une infrastructure fédérée permettant de « connecter les différents hubs nationaux de données [...] conçue en *open source* » (Nocetti, 2022, p. 58), l'UE bénéficierait ainsi d'un cercle vertueux, initié par cet « effet boule de neige ».

### **Le Digital Markets Act : l'affirmation de la souveraineté numérique européenne ?**

En théorie, le DMA ne trouve pas d'application sur le plan externe. Son champ d'application est circonscrit aux frontières des États membres de l'UE. Cependant, au vu de ce qui a été

---

<sup>10</sup> Entendu comme un large espace de stockage de données européen au sein duquel les échanges de données pourraient s'opérer en toute sécurité, (CE, 2020b, p. 22)

développé dans la section précédente, il pourrait être avancé que le DMA a été articulé autour des deux sources reconnues de pouvoir de l'UE, à savoir : la protection des droits fondamentaux en axant sa politique sur la protection des données, de la vie privée de ses citoyens, la protection des droits fondamentaux constituant la source de la légitimité de l'action de l'UE aussi bien au sein de ses frontières que dans son action extérieure ; et la promotion du libre marché et de l'innovation technologique en axant la stratégie du DMA sur une coopération multilatérale au sein d'un marché intégré et libre. Ce sont également ces principes qui lui donnent sa légitimité d'action sur la scène internationale et lui permettent, en partie, d'externaliser ses politiques. Bien que n'ayant que peu de prérogatives en termes de politique internationale, l'externalisation de ses principes et de ses politiques renforcent sa position de pouvoir normatif ou de puissance réglementaire (Broeders et al., 2023).

On assisterait alors, selon Broeders et al. (2023, p. 9), à une forme de « geopoliticisation » des politiques numériques de l'UE. Ils notent ainsi deux tendances dans le développement des politiques numériques européennes. Premièrement, ces dernières visent prioritairement des entreprises étrangères, plus particulièrement américaines ou chinoises (Broeders et al., 2023). En effet, les critères établis dans l'article 3 du DMA concernant la désignation des « gatekeepers », laissent à penser qu'aucune entreprise européenne du numérique n'aurait pu rencontrer les critères énoncés dans le règlement. De cette façon, la CE élèverait une forme de barrière visant à protéger le marché européen. Deuxièmement, on note également une tendance à la géopolitisation d'instruments de politique préexistants. Parmi ceux-ci se retrouvent notamment : les instruments dits « classiques » de régulation interne inhérents à la régulation de la concurrence et du marché intérieur ; les politiques visant à imposer des conditions à l'entrée du marché intérieur, telles que le RGPD ; et de nouvelles politiques numériques de type hybride rassemblant les deux premiers instruments, telles que le DMA (Broeders et al., 2023).

Le *de facto* « Brussels effect », décrit par Anu Bradford, s'en trouve assez bien illustré. Exploitant l'importance du marché qu'elle représente, l'UE peut se permettre d'émettre des lois restrictives visant des cibles dites « inélastiques », telles que le marché ou ses parties prenantes clés. La CE tant à la fois régulatrice et sanctionnatrice, ces dernières trouvent, en général, plus avantageux de se soumettre à ce type de régulation stricte que de quitter le marché européen. Des régulations émises de manière unilatérale telles que le DMA ou le RGPD pourraient donc progressivement s'imposer comme des standards globaux, devenus inséparables du marché qu'ils investissent et donc du bénéfice que les entreprises en retirent (Bradford, 2020a). Ce « Brussels effect » est mesurable par la force d'exécution avec laquelle est implémentée une loi et permet ainsi son externalisation. En ce qui concerne le DMA, il sera potentiellement



possible d'en mesurer les effets durant l'année suivant la désignation des « gatekeepers », à savoir à partir du 6 septembre 2023 (Bradford, 2020b).

Selon Broeders et al. (2022) également, nous assisterions actuellement à une forme de glissement dans la politique européenne, axée désormais sur l'affirmation d'une position géopolitique ancrée dans la défense des intérêts de l'UE, partant du postulat que celle-ci perd de son importance sur la scène internationale dans les domaines technologiques, du marché et de l'investissement. Cependant, ces affirmations constitueraient une forme de paradoxe et les incitations européennes à encourager l'innovation et la fluidification des échanges de données sembleraient incompatibles avec l'émission d'une telle loi dite discriminatoire et « quasi-frauduleuse » par les États-Unis, qualifiant d'« injustifiées » les barrières élevées contre les technologies étrangères (Broeders et al., 2022, p. 8).

A travers l'extension du « Brussels effect », l'UE s'est vue accusée par les États-Unis d'impérialisme et de protectionnisme. Ces derniers ont souligné que, s'il était effectivement important pour l'UE de vouloir préserver ce qui constitue son ADN (à savoir la protection des droits de ses citoyens et un marché libre et équitable au sein de ses frontières), les revendications souveraines sur le monde du numérique ne devraient pas faire l'objet d'une forme d'« insularisation » (Celeste, 2020, p. 16) (autrement dit d'isolement) ni dépasser les champs d'application définis de la loi européenne, au risque de voir s'élever de nouvelles tensions géopolitiques et économiques, ou d'inciter d'autres pays à user de leurs prérogatives pour mettre en place ce même type de régulation, détériorant *de facto*, la souveraineté numérique de chaque partie (Celeste, 2020).

En contrepartie, le 10 juillet 2023, la CE et les États-Unis ont signé un « Nouveau cadre pour la protection des données UE-États-Unis ». Il a pour vocation de renforcer le partenariat transatlantique et se présente comme une amélioration du « Privacy Shield », précédemment déclaré non conforme au RGPD par l'arrêt Schrems II. Par ailleurs, il garantira une circulation sécurisée des données, avec comme nouveauté une possibilité pour la Cour de Justice de l'Union européenne (CJUE) de faire supprimer des données collectées en violation de cet accord (CE, 2023b). L'UE devra donc désormais composer avec le DMA et ce nouvel accord. Ce dernier encadre les échanges de données collectées par les entreprises visées par le DMA qui, lui, tend à sécuriser un échange de données intra-européen.

## L'UE : un modèle « hybride » de gouvernance numérique ?

### Considérations géopolitiques

Le DMA, conjointement aux autres politiques numériques, pourrait être l'une des premières clés vers l'affirmation de la souveraineté numérique européenne, et donc d'un modèle de gouvernance propre à l'UE sur son territoire. Cependant, ces politiques s'appliquent à l'instant « T », dans un monde numérique mouvant et en perpétuelle croissance exponentielle. Même si ces politiques ont été conçues pour permettre leur développement et leur adaptation au contexte, nous ne disposons pas de garantie absolue sur la capacité d'adaptation des processus légaux européens, souvent chronophage, et rythmés par les développements technologiques chinois et américains.

Par ailleurs, bien que l'UE mette en place nombre d'instruments ayant des objectifs communs (dont la souveraineté numérique), elle a pris un retard conséquent dans les domaines du numérique et se trouve désormais prise « entre deux feux », deux modèles radicalement opposés en termes d'idéologie(s) dont elle dépend. Les récentes rivalités sino-américaines sont considérées comme des freins à l'innovation en Europe. Elle s'est d'ailleurs vu retirer son autonomie de décision dans le cadre de politiques commerciales ou de sécurité (notamment en ce qui concerne l'implémentation de la 5G chinoise, dont l'exemple a été décrit plus haut). L'UE, alliée de longue date des États-Unis, ne peut plus se contenter d'assurer la légitimation ou la cohérence de ses lois, mais doit aussi se concentrer sur sa capacité à les émettre de façon autonome vis-à-vis des États-Unis, notamment afin de préserver ses parts de marché en Chine. De plus, l'UE n'émet pas le souhait d'une indépendance totale de sa chaîne de production dans le secteur numérique. L'indépendance réside dans le fait de pouvoir prendre seule des décisions de gouvernance numérique à des fins de protection des droits de ses citoyens, de leur vie privée, de ses industries et du respect des règles du marché jugées justes et équitables. Patricia Nouveau (2022, p. 362) déclare d'ailleurs à cet égard : « *behind the question of the consumer protection stands the question of the protection of Europe* ».

Nous ne pouvons pas manquer d'évoquer la nomination de Fiona Scott Morton au poste de chef économiste à la Direction Générale concurrence le 11 juillet 2023. Bien que la CE ait ouvert ce poste à l'étranger dans le but de recruter les meilleurs experts, c'est donc une Américaine, anciennement lobbyiste auprès de plusieurs GAFAM, qui a été nommée par la CE pour endosser le rôle. Celle-ci devait prendre ses fonctions le 1<sup>er</sup> septembre 2023. Cependant,

dès la médiatisation de cette nomination et l'indignation qu'elle a causée, Fiona Scott Morton a renoncé à ce poste. Pour rappel, la désignation des « gatekeepers » devait normalement être finalisée le 6 septembre 2023 (CE, 2023c).

En l'état actuel de ses capacités de production technologique, l'Europe ne peut prétendre à une pleine souveraineté numérique. Un partenariat transatlantique s'avère indispensable pour établir cette souveraineté et assurer la position géopolitique de l'UE, une juste concurrence des marchés et le respect des droits et libertés. Mais ce postulat s'applique de même aux Etats-Unis. En effet, à titre d'exemple, l'UE et les Etats-Unis représentent 21 % de la production mondiale de semi-conducteurs et 43 % de la consommation globale de services numériques, et courent donc un risque potentiel important de dépendance aux producteurs chinois. Si l'Europe dépend des entreprises américaines en termes d'offre numérique, les entreprises américaines peuvent poursuivre leur croissance grâce à leur accès au marché européen. En plus de constituer des marchés colossaux, les États-Unis et l'UE partagent les mêmes valeurs inhérentes aux démocraties libérales telles que le droit à la vie privée, la liberté d'expression et la promotion d'un marché juste et équitable (Bendiek et Stürzer, 2022).

Depuis 2021, l'UE et les États-Unis s'attellent également à renforcer leurs liens à travers une coopération encadrée par le « Trade and Technology Council » (TTC). A l'issue de la réunion des représentants du TTC, rassemblant plusieurs représentants américains au commerce et aux échanges ainsi que les Commissaires Margarethe Vestager, Thierry Breton et Valdis Dombrovskis, les déclarations conjointes s'articulent autour de la défense des valeurs démocratiques, de la protection des libertés individuelles et d'un marché libre et équitable. L'accent est mis également sur une gouvernance commune des technologies et la promotion d'un internet sécurisé, équitable et ouvert (U.S. Department of Commerce, 2022). Ces déclarations rejoignent d'ailleurs celles énoncées dans le paquet législatif proposé par la CE dans les matières numériques : « une technologie au service des personnes », « une économie juste et compétitive », « une société ouverte, démocratique et durable », et « une dimension internationale » (Ponce del Castillo, 2022, pp. 91-96). Seul l'avenir pourra préciser quelle forme d'équilibre atteindront ensemble, dans leurs articulations respectives, les accords transatlantiques et les lois du marché intérieur visant les grosses entreprises américaines.

### **La gouvernance du numérique pour l'UE : un modèle hybride ?**

Pour rappel, Gorwa (2019a) identifie trois modèles de gouvernance des plateformes : « self governance », « external governance », et « co governance ».

Suite à l'analyse développée, il apparaît que l'UE privilégie des instruments de la gouvernance externe ainsi que de la co-gouvernance, sans s'inscrire de façon définie dans l'une ou l'autre. En effet, la CE utilise les leviers énoncés par Gorwa dans sa modélisation de la gouvernance externe, à savoir les lois régulant les marchés et la concurrence, ainsi que les instruments de sécurisation des échanges de données et de protection de la vie privée, notamment avec la mise en application du RGPD. Cependant, elle met également l'accent sur le besoin de responsabilisation des plateformes dans le but de protéger les valeurs démocratiques et les droits fondamentaux de ses citoyens, fondations de la légitimité d'action de l'UE (Broeders et al., 2023). De plus, elle s'essaye à inclure les parties prenantes comme acteurs à part entière de l'application de ses politiques. Avec l'émission d'une loi comme le DMA, elle s'appuie sur les plateformes en affichant sa volonté de coopération avec le secteur privé, en leur faisant mener leurs propres audits, collectant ainsi des informations qu'elle espère fiables et servant les ambitions de bonne gouvernance de l'UE dans le secteur du numérique. Nous pourrions ainsi voir dans le modèle proposé par l'UE, d'après le précédent développement, une forme de gouvernance à mi-chemin entre la gouvernance externe comme outil de régulation de la concurrence et protection des données pour un espace numérique sécurisé et équitable, et une co-gouvernance fondée sur un partenariat public-privé.

Par ailleurs, comme le rappelle le Conseil de l'Europe (2023), il nous paraît également important de mentionner que l'UE est caractérisée par une gouvernance multiniveaux. Bien que la CE détienne le quasi-monopole de la mise à exécution des lois du numérique au sein de la Direction Générale de la Concurrence et de la Direction Générale des Réseaux de Communication, du Contenu et des Technologies, la gouvernance du numérique au sein des frontières de l'UE repose sur une institutionnalisation croissante de cette gouvernance en coopération avec les autorités nationales de ses États membres (notamment via les Autorités chargées de la Protection des Données et du « European Competition Network »). En effet, ceux-ci sont les canaux de transmission de l'information sur lesquels la CE doit également se baser pour une mise en place efficace de sa politique.

Enfin, abstraction ne peut être faite de la dimension humaine qui sous-tend toute réflexion ou action. La loi qui est édictée dépend, dans son exécution, du ou des individu(s) endossant la responsabilité des décisions prises et des actions menées. Margarethe Vestager, considérée comme très atlantiste, devrait bientôt céder sa place à la tête de la Direction Générale de la Concurrence (L'Écho, 2023). Le profil de son ou sa successeur influencera inévitablement l'implémentation de ces lois.

Les contours du modèle européen de gouvernance du numérique restent encore peu définis. Les dynamiques d'extra-territorialisation des politiques de l'UE ainsi que la gouvernance multiniveaux, unique en son genre, incluant secteur privé, États membres et institutions européennes semblent encore difficiles à modéliser ou à contenir dans une seule théorie.

## **Conclusion**

Le but de cet article était de comprendre comment l'UE tend à affirmer une voie alternative aux modèles américains et chinois en approfondissant l'étude de certains outils de régulation des plateformes sur le territoire européen lui permettant de se situer dans le spectre des différents types de gouvernance du numérique.

A cette fin, nous avons tenté de définir les contours du concept clé du discours européen, à savoir la souveraineté numérique. Cette notion peut se résumer au contrôle des secteurs indispensables à l'exercice de la souveraineté, en disposant des ressources nécessaires pour asseoir son autonomie (Timmers, 2022). Elle se définit comme la capacité « d'agir de façon autonome dans le domaine du numérique » (Madiaga, 2022 p. 1). Elle émerge suite aux préoccupations qu'engendre l'entrée des Big Tech américains sur le marché européen et la dépendance européenne aux technologies chinoises, et aux modèles de gouvernance qui les régulent tels que définis par Gorwa. Le détail de ces deux modèles nous a permis de comprendre l'enjeu que représente la gouvernance des plateformes et, plus largement, du numérique, en marge de ces deux géants.

Pour en saisir les subtilités, nous avons également considéré l'importance d'établir le contexte dans lequel se développent les revendications de souveraineté numérique. Dans un premier temps, nous avons identifié ce qui semble être devenu le cheval de bataille de l'UE : la protection des données personnelles et industrielles de ses citoyens et de ses entreprises (CE, 2020b), et le droit à la vie privée consacré dans la Charte européenne des Droits de l'Homme. La première pierre, capitale en termes de protection des données et de sauvegarde des droits, est posée par la mise en application du RGPD, symbole de la puissance normative de l'UE et du rayonnement des standards qu'elle impose sur son territoire.

Cependant, au cours des dernières années, les entreprises américaines du numérique ont renforcé leur position sur le marché européen de façon exponentielle, impliquant la multiplication des comportements anticoncurrentiels nuisant à l'équité du marché et à la croissance des entreprises européennes du numérique. La stratégie de l'UE consiste à rééquilibrer le marché en limitant les comportements anticoncurrentiels afin de permettre la

croissance des entreprises européennes du numérique et, sur le long terme, de diminuer ses dépendances stratégiques vis-à-vis des États-Unis et de la Chine (CE, 2020c).

A cette fin, le DMA est entré en vigueur depuis le 2 mai 2023. Cette nouvelle loi a pour but d'éviter les comportements nuisant à l'équité du marché et favoriser ainsi une concurrence juste. Le DMA s'attelle donc à définir ce qu'il nomme des « gatekeepers » ou des « contrôleurs d'accès ». Ces derniers sont désignés sur base de critères économiques tels que le chiffre d'affaires ou le nombre d'utilisateurs et se voient imposer plusieurs obligations visant à éviter les comportements cités précédemment (DMA, art. 5 à 7). Ce faisant, le DMA pose le cadre d'une régulation *ex-ante* de la concurrence et actionne ainsi l'un des leviers présentés par Gorwa dans son modèle de la gouvernance externe des plateformes. De plus, en axant sa stratégie sur le développement industriel et la transition numérique contrôlée de ses entreprises, le DMA permet à l'UE de se positionner en tant qu'acteur géopolitique d'importance dans la gouvernance globale du numérique et sur la scène internationale, en tendant à atteindre une certaine autonomie stratégique (Borrell, 2020).

En quoi le modèle européen de gouvernance du numérique pourrait-il se présenter comme une voie alternative aux deux premières tracées respectivement par les États-Unis et la Chine ? Le modèle européen est fondé sur la défense et la protection des droits fondamentaux, alors que les deux premiers oscillent entre « une vision dérégulée du numérique conduisant au dévoiement du capitalisme et une approche basée sur un techno-étatisme décomplexé en matière de surveillance de masse » (Nocetti, 2021, p. 60). Par ailleurs, l'UE étend le champ d'application de ses lois aux entreprises étrangères, en utilisant son pouvoir normatif et le caractère incontournable de son marché pour faire appliquer ses standards.

Ce nouveau modèle européen se caractérise également, à terme, par un cloisonnement du marché du numérique afin de favoriser un transfert intra-européen des données, tout en maintenant un marché ouvert, juste et équitable. D'un point de vue strictement binaire, les deux objectifs peuvent paraître paradoxaux. La voie esquissée par l'UE s'orientera entre les deux tendances et devra y trouver l'équilibre le plus profitable et le plus porteur.

## **Bibliographie**

AUDUREAU, William. « Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook ». *Le Monde.fr*, 2018, disponible à l'adresse suivante : <https://www.lemonde.fr/>

AFP, « La commissaire européenne Margarethe Vestager candidate pour devenir présidente de la BEI », *L’Echo*, 2023, disponible à l’adresse suivante : <https://www.lecho.be/economie-politique/>

D’AGRAIN, Henri. « Géopolitique de l’espace numérique. Quelles stratégies de sécurité ? » *Futuribles*, 2022, vol. 45. n° 6 pp. 21-37.

ALEXANDRE, Olivier. « Burning Man : l’esprit de la Silicon Valley. Un festival libertaire devenu liberal ». *Revue du Crieur*, 2018, vol. 11. n° 3, pp. 86-107.

BELLANGER, Pierre. « De la souveraineté numérique ». *Le Débat*, 2012, vol. 170. n° 3, pp. 149-59.

BELLANOVA, Rocco, CARRAPICO, Helena et DUEZ, Denis. « Digital/sovereignty and European security integration: an introduction ». *European Security*, 2022, vol. 31. n° 3, pp. 337-55.

BENDIEK, Annegret, et STÜRZER, Isabella. *Advancing European Internal and External Digital Sovereignty: The Brussels Effect and the EU-US Trade and Technology Council*. SWP Comment. Berlin: Stiftung Wissenschaft und Politik -SWP- Deutsches Institut für Internationale Politik und Sicherheit, 2022, vol. 20.

BRADFORD, Anu. « The Brussels Effect ». In BRADFORD, Anu (Ed.), *The Brussels Effect: How the European Union Rules the World*, New York, Oxford University Press, 2020, pp. 25-66.

BRADFORD, Anu. « Digital Economy ». In BRADFORD, Anu (Ed.), *The Brussels Effect: How the European Union Rules the World*, New York, Oxford University Press, 2020, pp. 131-170.

BROEDERS, Dennis and KAMINSKA, Monica. « EU digital sovereignty: When top-down meets bottom-up. » In BROEDERS Dennis, (ed.) *Digital Sovereignty: From Narrative to Policy?* EU Cyber Direct, 2022, pp. 9-17.

BROEDERS, Dennis, CRISTINAO, Fabio et KAMINSKA, Monica. « In Search of Digital Sovereignty and Strategic Autonomy: Normative Power Europe to the Test of Its Geopolitical Ambitions ». *JCMS: Journal of Common Market Studies*, 2023, vol. 61. n°5, pp. 1261-1280.

CELESTE, Edoardo. « Digital Sovereignty in the EU: Challenges and Future Perspectives », in FABBRINI, Federico, CELESTE, Edoardo and QUINN, John, *Data Protection Beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty*. Oxford, Hart Publishing (Bloomsbury), 2020, pp. 211-228.

CERULUS, Laurens et SCOTT, Mark, « Europe's new data protection rules export new privacy standards worldwide », *Politico*, 2018, disponible à l'adresse suivante : <https://www.politico.eu>

CHEN, Shaowei, JIA, Kai. « Global Digital Governance: Paradigm Shift and an Analytical Framework ». *Global Public Policy and Governance*, 2022, vol. 2. n° 3, pp. 283-305.

CHENOU, Jean-Marie. « From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s ». *Globalizations*, 2014, vol. 11, n° 2, pp. 205-23.

C.J.E.U (gde ch.) Arrêt *Schrems c. Data Protection Commissioner* du 6 octobre 2015, C-362/14, EU:C:2015:650

C.J.E.U (gde ch.) Arrêt *Schrems et Facebook Ireland Ltd c. Data Protection Commissioner* du 16 juillet 2020, C-311/18, EU:C:2020:559

COMMISSION EUROPÉENNE, « On Artificial Intelligence: A European Approach to Excellence and Trust », *White Paper*, Brussels, 19.2.2020, COM(2020) 65 final, 2020a.

COMMISSION EUROPÉENNE, « A European strategy for data », *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, Brussels, 19.2.2020, COM(2020) 66 final, 2020b.

COMMISSION EUROPÉENNE, « Shaping Europe's digital future », *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, 19.2.2020, COM(2020) 67 final, 2020c.



COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, *O.J.E.U.* L207/1, 1.8.2016.

COMMISSION EUROPÉENNE, « Remarks by Commissioner Breton: Here are the first seven potential ‘Gatekeepers’ under the EU Digital Markets Act », 2023a, disponible à l’adresse suivante: [https://ec.europa.eu/commission/presscorner/detail/en/statement\\_23\\_3674](https://ec.europa.eu/commission/presscorner/detail/en/statement_23_3674)

COMMISSION EUROPEENNE, « Protection des données : la Commission européenne adopte une nouvelle décision d’adéquation concernant la circulation sécurisée et fiable des données entre l’UE et les États-Unis », 2023b, disponible à l’adresse suivante : <https://www.cnil.fr/fr/transferts-de-donnees-vers-les-etats-unis-la-commission-europeenne-adopte-une-nouvelle-decision>

COMMISSION EUROPEENNE, « Daily News 11/07/2023 », 2023c, disponible à l’adresse suivante : [https://ec.europa.eu/commission/presscorner/detail/en/mex\\_23\\_3805](https://ec.europa.eu/commission/presscorner/detail/en/mex_23_3805)

Conseil de l’Europe, « Document d’informations sur le concept de gouvernance multiniveaux et question générales / préliminaires à examiner », *Comité européen sur la démocratie et la gouvernance (CDDG), Groupe de Travail sur la Gouvernance (GT-G)*, Strasbourg, 25 janvier 2023, GT-G(2023)4

DANET, Didier, et DESFORGES, Alix. « Souveraineté numérique et autonomie stratégique en Europe : du concept aux réalités géopolitiques », *Hérodote*, 2020, vol. 2. n°177-178, pp. 179-95.

FARRAND, Benjamin, et CARRAPICO, Helena. « Digital sovereignty and taking back control: from regulatory capitalism to regulatory mercantilism in EU cybersecurity ». *European Security*, 2022, vol. 31. n° 3, pp. 435-53.

FEI, Lanfang. « Regulation under Administrative Guidance: The Case of China’s Forcing Interoperability on Digital Platforms ». *Computer Law & Security Review*, 2023, vol. 48. 105786.

FLORIDI, Luciano. « The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU ». *Philosophy & Technology*, 2020, vol. 33. n° 3, pp. 369-78.

GORWA, Robert. « What is platform governance? » *Information, Communication & Society*, 2019a, vol. 22. n° 6, pp. 854-71.

GORWA, Robert. « The Platform Governance Triangle: Conceptualizing the Informal Regulation of Online Content », *Internet Policy Review*, 2019b, vol. 8. n° 2, pp. 1-22.

IRION, Kristina. « The General Data Protection Regulation through the lens of digital sovereignty ». In BROEDERS Dennis, (ed.) *Digital Sovereignty: From Narrative to Policy?* EU Cyber Direct, 2022, pp. 53-56.

Joint Conclusions of the European Parliament, the Council of the European Union and the European Commission on Policy Objectives and Priorities for 2020-2024 2021/C 451 I/02, *J.O.U.E.*, CI451/4, 29 décembre 2020.

LIU, Jinhe, et YANG, Le. « ‘Dual-Track’ Platform Governance on Content: A Comparative Study between China and United States ». *Policy & Internet*, 2022, vol. 14. n° 2, pp. 304-23.

MADIEGA, Tambiana. “Digital sovereignty for Europe” (No. PE 651.992). European Parliamentary Research Service, European Parliament, 2020.

MONSEES, Linda, et LAMBACH, Daniel. « Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. » *European Security* 2022, vol. 31. n° 3, pp. 377-94.

MUELLER, Milton L. *Networks and States: The Global Politics of Internet Governance*, Cambridge, MIT Press, 2010.

NOCETTI, Julien. « L’Europe reste-t-elle une ‘colonie numérique’ des États-Unis ? » *Politique étrangère*, 2021, vol.86. n° 3, pp. 51-63.

NOUVEAU, Patricia, « Falling behind and in between the United States and China: can the European Union drive its digital transformation away from industrial path dependency? », in DEFRAIGNE, Jean-Christophe, WOUTERS, Jan, TRAVERSA, Edoardo & ZURSTRASSEN, Dimitri

(eds.), *EU Industrial Policy in the Multipolar Economy*, Edward Elgar Publishing, 2022, pp. 332-381.

O'HARA, Kieron, et HALL, Wendy. « Four internets: the geopolitics of digital governance », *CIGI Papers*, 2028, n°206.

PONCE DEL CASTILLO, Aída. « Chapitre 4 : La stratégie numérique de l'Europe : centrée sur les personnes, sur les données ou sur les deux ? » In VANHERCKE, Bart, SPASOVA, Slavina (Eds.), *Bilan social de l'Union européenne 2021 Les ambitions sociales renaissantes par temps de redressement de l'Union*, European Trade Union Institute (ETUI) et Observatoire Social Européen (OSE), 2022, pp. 89-107.

Proposition de règlement du Parlement Européen et du Conseil du 15 décembre 2020 relatif aux marchés contestables et équitables dans le secteur numérique (législation sur les marchés numériques), *J.O.U.E.*, 2020/0374 (COD).

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L119/1, 4 mai 2016

Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques), *J.O.U.E.*, L265/1, 12 octobre 2022.

ROSIERE, Stéphane. « Géographie politique, géopolitique et géostratégie: distinctions opératoires ». *L'Information Géographique*, 2001, vol. 65. n° 1, pp. 33-42.

ROBERTS, Huw, COWL, Josh, CASOLARI, Federico, MORLEY, Jessica, TADDEO Mariarosaria, et FLORIDI Luciano. « Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies ». Rochester, NY, SSRN Scholarly Paper, 2021.

SRNICEK, Nick. *Platform Capitalism*, Cambridge, John Wiley & Sons, 2017

SCHNEIDER, Ingrid. « Democratic Governance of Digital Platforms and Artificial Intelligence?: Exploring Governance Models of China, the US, the EU and Mexico ». *JeDEM - EJournal of EDemocracy and Open Government*, 2020, vol. 12. n° 1, pp. 1-24.

TIMMERS, Paul. « Investment policy for digital sovereignty: From policy to action ». In BROEDERS Dennis, (ed.) *Digital Sovereignty: From Narrative to Policy?* EU Cyber Direct, 2022, pp. 25-33.

« Treaty on the Functioning of the European Union », 2016, *Official Journal of the European Union*, C 202, 7.6.2016, disponible à l'adresse suivante, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:C:2016:202:TOC> (accessed 6 January 2023).

U.S DEPARTMENT OF COMMERCE, « U.S.-EU Joint Statement of Trade and Technology Council », *Department of Commerce of the United States of America*, May 16, 2022.

UTERSINGER, Martin. « Ce que les 'révélations Snowden' ont changé depuis 2013 ». *Le Monde.fr*, 2019, disponible à l'adresse suivante <https://www.lemonde.fr/>

VAN CLEYENBREUGEL, Pieter. « The Commission's Digital Services and Markets Act Proposals: First Step towards Tougher and More Directly Enforced EU Rules? » *Maastricht Journal of European and Comparative Law*, 2021, vol. 28, n° 5, pp. 668-685.

VON DER LEYEN, Ursula, « Speech by President-elected in the European Parliament plenary session on the occasion of the presentation of her College of Commissioners and their program », *European commission*, 2019, disponible à l'adresse suivante: [https://ec.europa.eu/commission/presscorner/detail/en/SPEECH\\_19\\_6408](https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_19_6408)