OECD publishing

LES LEVIERS NUMÉRIQUES DE L'ÉCONOMIE MONDIALE

DOCUMENT DE RÉFÉRENCE DESTINÉ À LA RÉUNION MINISTÉRIELLE DU CPEN

OECD DIGITAL ECONOMY PAPERS
Novembre 2022 **No. 337**

OCDE
DES POLITIQUES MEILLEURES POUR UNE VIE MEILLEURE

Avant-propos

Le présent document étudie trois leviers numériques qui sous-tendent l'économie – les plateformes électroniques, les flux transfrontières de données et la sécurité numérique –, ainsi que les défis et les possibilités qu'ils induisent pour les responsables de l'action publique. Ces problématiques ayant par nature une dimension internationale, il met en avant l'importance d'y apporter une réponse politique à l'échelle mondiale.

Ce document fournit des éléments d'information destinés à nourrir les débats qui seront menés au titre du thème 1, « Les leviers numériques de l'économie mondiale », lors de la Réunion ministérielle du Comité de la politique de l'économie numérique qui se tiendra les 14 et 15 décembre 2022 à la Grande Canarie, en Espagne. Il vise à étayer les sessions de la Réunion ministérielle consacrées aux thèmes : « Façonner des politiques adaptées aux plateformes en ligne », « Renforcer la confiance dans les flux transfrontières de données » et « Renforcer les bases de la sécurité numérique de tous les produits et services ».

Le présent document a été rédigé par Angela Attrey, Thyme Burdon, Francesca Casalini, Simon Lange et Peter Stephens, sous la supervision d'Audrey Plonk, Cheffe de la Division de la politique de l'économie numérique de l'OCDE. Il a bénéficié de la contribution de Gallia Daor ; Angela Gosmann, Sebastian Ordelheide et Misha Pinkhasov ont apporté un appui rédactionnel. La Réunion ministérielle et les travaux connexes bénéficient du généreux soutien du gouvernement espagnol.

Le présent rapport a été approuvé et déclassifié selon la procédure écrite par le Comité de la politique de l'économie numérique, le 26 octobre 2022, et préparé en vue de sa publication par le Secrétariat de l'OCDE.

Note aux délégations :

Ce document est également disponible sur O.N.E sous la cote :

DSTI/CDEP(2022)11/FINAL

Table des matières

GRAPHIQUES

Résumé

Les technologies numériques sous-tendent une part croissante de l'activité économique mondiale. Si les technologies et les modèles économiques qu'elles font naître procurent des avantages considérables, ils entraînent également des mutations profondes qui appellent la mise en place de nouveaux cadres d'action à l'échelle internationale. Dans un contexte dense des politique numériques variées, trois leviers se démarquent en tête des priorités des pouvoirs publics :

- Les **plateformes en ligne** abritent les transactions et les interactions entre des groupes d'utilisateurs distincts répartis dans le monde. Elles ouvrent les marchés et offrent de nouvelles opportunités aux consommateurs et aux entreprises, qui peuvent même traiter avec des parties qu'ils ne connaissent pas. Mais elles suscitent également des inquiétudes en termes de concurrence et de protection des consommateurs. Les réponses fragmentaires des pouvoirs publics et des autorités réglementaires sont source de coûts et d'incertitudes pour les entreprises et les consommateurs et exigent une coordination transnationale.
- Les **flux transfrontières de données** ouvrent la voie à la mise en place et la gestion, par les entreprises, de chaînes logistiques mondiales complexes, et facilitent le partage des données de la recherche ainsi que la communication. Pour autant, ils sont également synonymes de préoccupations accrues pour les pouvoirs publics, les poussant à prendre des mesures politiques et réglementaires fixant les conditions et les modalités de la circulation des données à l'échelle internationale. Les responsables de l'action publique doivent évaluer ces évolutions et faire en sorte que la fragmentation et le manque de transparence et de clarté réglementaire n'empêchent pas les opportunités économiques ni la réalisation des objectifs visés.
- La **sécurité numérique** favorise la confiance dans la transformation numérique et la progression de cette dernière. Or le rythme effréné de la révolution numérique ne s'est pas accompagné d'avancées équivalentes de la sécurité des services en ligne et des produits connectés. Les utilisateurs finaux sont rarement à même d'évaluer si les approches de la sécurité sont suffisantes, ce qui entraîne des défaillances du marché qui sapent la confiance des consommateurs et mettent le système en péril. De nombreux défis inhérents à la sécurité numérique ont une dimension internationale dans la mesure où, pour être traitées avec une efficacité optimale, les vulnérabilités et les mauvaises pratiques appellent une action mondiale.

Face aux enjeux associés à ces leviers, une coopération internationale s'impose pour concilier au mieux les objectifs stratégiques nationaux et les avantages à attendre d'une économie numérique mondialisée. L'absence de coordination internationale risque de se traduire par une fragmentation du paysage de l'action publique, dans lequel peu d'entreprises pourront naviguer, avec des coûts substantiels pour les consommateurs.

L'OCDE joue de longue date un rôle de premier plan dans le domaine des politiques du numérique, notamment avec ses normes internationales et orientations pratiques. Son expertise de la mesure, du suivi et de l'évaluation des technologies numériques et de leurs incidences sur les sociétés est reconnue à l'échelle planétaire. Elle offre également un modèle de dialogue multipartite inclusif et mondial. Grâce au soutien continu de ses membres et en concertation avec les institutions internationales et parties

prenantes compétentes, l'OCDE peut aider les pays à assouvir leur ambition de tendre vers une économie mondiale fondée sur les technologies numériques.

1 Introduction

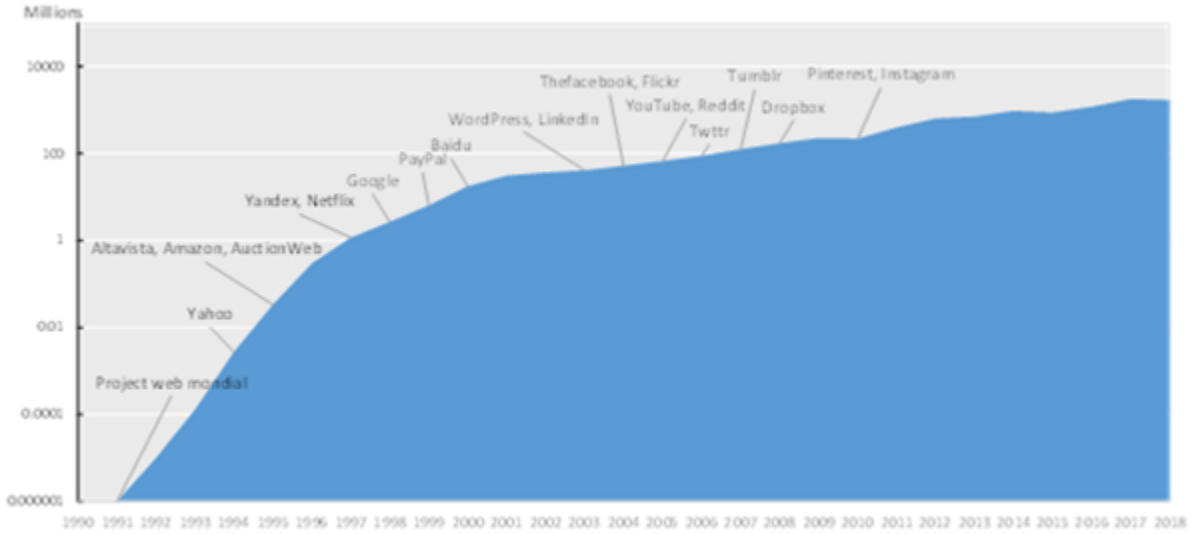
Des débuts modestes au fondement d'une économie mondiale

Pour les utilisateurs de la première heure, le World Wide Web était un espace étrange et prometteur, propice à des expérimentations en apparence sans conséquence. Le premier site internet, qui a vu le jour en 1991, contenait une description de ce qu'était le web et de la façon dont il pouvait être utilisé. Fin 1992, seuls dix sites avaient été publiés en ligne, qui proposaient des logiciels libres, des collections aléatoires d'informations et des contenus à l'humour dépassé. La première webcaméra, qui a commencé à diffuser des images fin 1993, a été mise en place pour surveiller le niveau de café dans une cafetière installée dans un laboratoire informatique de l'université de Cambridge.

Depuis ces débuts modestes, le nombre de sites web a explosé. En 1994 a été lancé le *Jerry and David's Guide to the World Wide Web*, qui deviendra plus tard Yahoo. Outre les navigateurs web Mosaic et Netscape, qui ont vu le jour respectivement en 1993 et 1994, des moteurs de recherche ont permis à un public de plus en plus large d'accéder à différentes parties du web. La population d'internautes n'a cessé de progresser grâce aux innovations complémentaires telles que le haut débit et les technologies mobiles. C'est ainsi que le web est passé d'un site unique en 1991 à plus d'un million de sites en 1997. Dix ans plus tard, on en dénombrait plus de 100 millions (Graphique 1).

Graphique 1. Évolution du nombre de sites web, de 1991 à 2018

Millions, échelle logarithmique



Note : On entend par « sites web » des noms d'hôtes uniques. Le nombre de sites web actifs (par opposition aux domaines enregistrés non utilisés, ou équivalents) pourrait être sensiblement inférieur.
Source : Netcraft (2022[1]), *Web Server Survey*, https://news.netcraft.com/archives/category/web-server-survey/ ; Gray (1996[2]), *Web Growth Summary*, https://www.mit.edu/people/mkgray/net/web-growth-summary.html.

L'internet – soit le système mondial de réseaux informatiques interconnectés – stimule l'innovation (OCDE, 2016[3]). Derrière des sites web nés entre 1995 et 2005 se trouvaient de jeunes entreprises à l'origine d'applications et de services nouveaux. Certaines d'entre elles – d'Amazon à Baidu, en passant par Facebook, Google, Netflix et PayPal – sont aujourd'hui connues de tous. La concurrence était acharnée, comme en témoignent les « guerres de navigateurs » (la bataille continue que se livraient les acteurs pour s'imposer sur le marché des navigateurs internet). Les plateformes en ligne, à l'image d'Amazon, Airbnb ou Uber, ont bouleversé des secteurs entiers, tandis que les entreprises traditionnelles se sont peu à peu tournées vers les technologies numériques pour optimiser leurs processus et bâtir des chaînes logistiques mondiales complexes.

Les leviers numériques de l'économie mondiale et les défis qu'elles représentent pour les pouvoirs publics

Les technologies et les services numériques fondés sur l'internet sous-tendent désormais l'économie mondiale, favorisant l'émergence de modèles économiques, de connexions et de transactions nouveaux, et offrant un accès sans précédent à l'information, indépendamment de la localisation géographique. Si de nombreux facteurs jouent un rôle important – de la connectivité aux compétences –, le présent document examine trois leviers numériques essentiels de l'économie mondiale qui figurent aujourd'hui en tête des priorités d'action des pouvoirs publics :

- **Plateformes en ligne.** La mise en relation d'utilisateurs partout sur la planète est propice à l'activité économique mondiale en ce qu'elle permet aux entreprises d'accéder à de nouveaux marchés, et aux consommateurs, à davantage de contenus et de produits. Pour autant, si à l'origine l'écosystème numérique bouillonnait d'énergie entrepreneuriale, on craint aujourd'hui que ce dynamisme ne se soit tari et que les plateformes en place ne soient devenues ancrées. Juristes et économistes observent que les entreprises du numérique semblent voir leur pouvoir de marché augmenter, tandis que la protection des cyberconsommateurs suscite des inquiétudes croissantes.
- **Flux transfrontières de données.** L'architecture de l'internet permet une circulation fluide des données entre les appareils connectés partout dans le monde, ce qui facilite la coordination des chaînes de valeur mondiales et la prestation de services par-delà les frontières. Néanmoins, les pouvoirs publics tendent à adopter des politiques et des mesures visant à réglementer les transferts de données entre pays et territoires. Les internautes ont de plus en plus l'impression que la surveillance en ligne, loin de se limiter aux cafetières, les concernent désormais également. La protection de la vie privée devient dès lors une préoccupation phare, au même titre que celle des droits de propriété intellectuelle et d'autres objectifs de l'action des pouvoirs publics.
- **Sécurité numérique.** Sans la sécurité numérique, particuliers et organisations ne pourraient adopter en toute confiance les produits et services numériques qui sous-tendent progressivement la production et les échanges internationaux. Alors que des pans entiers de l'économie reposent désormais sur les technologies numériques, les enjeux de la cybersécurité vont croissant, et pour cause : une sécurité lacunaire peut occasionner des préjudices émotionnels, financiers et physiques d'une ampleur sans précédent. Or jusqu'à présent, le rythme effréné de la transformation numérique ne s'est pas accompagné d'un renforcement adapté des normes de sécurité.

Un appel en faveur d'une gouvernance numérique mondiale

Le World Wide Web était à l'origine accessible et intelligible à très peu de personnes. Désormais, plus de la moitié de la population mondiale accède à l'internet d'une façon ou d'une autre. À mesure que progressait la transformation numérique, la plupart des pays de l'OCDE ont défini des stratégies

numériques nationales (Gierten et Lesher, 2022[4]) et adopté des lois, réglementations et normes pour protéger les consommateurs tout en favorisant la transformation numérique et en veillant à ce qu'elle profite au plus grand nombre.

Pour autant, de nombreux défis auxquels les pouvoirs publics sont confrontés dans ce domaine ont une portée internationale et la transformation numérique appelle une gouvernance plus solide au plan mondial, afin que les particuliers et les entreprises puissent tirer le meilleur parti des opportunités qu'elle offre. Les décideurs doivent dès lors travailler de concert pour définir des approches cohérentes de la gouvernance des leviers numériques de l'économie mondiale.

Encadré 1. Principaux travaux de recherche et instruments juridiques de l'OCDE sur les leviers numériques de l'économie mondiale

Plateformes en ligne

- OCDE (à paraître[5]), « Data shaping firms and markets », *Documents de travail de l'OCDE sur l'économie numérique*, Éditions OCDE, Paris.
- OCDE (2022[6]), « The role of online marketplaces in protecting and empowering consumers: Country and business survey findings », *Documents de travail de l'OCDE sur l'économie numérique*, n° 329, Éditions OCDE, Paris, https://doi.org/10.1787/9d8cc586-en.
- OCDE (2019[7]), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, Éditions OCDE, Paris, https://doi.org/10.1787/53e5f593-en.
- OCDE (2019[8]), *Unpacking E-commerce: Business Models, Trends and Policies*, Éditions OCDE, Paris, https://doi.org/10.1787/23561431-en.
- OCDE (2016[9]), Recommandation du Conseil sur la protection du consommateur dans le contexte du commerce électronique.

Flux transfrontières de données

- OCDE (à paraître[10]), « Fostering cross-border data flows with trust », *Documents de travail de l'OCDE sur l'économie numérique*, Éditions OCDE, Paris.
- OCDE (2021[11]), Recommandation du Conseil sur l'amélioration de l'accès aux données et de leur partage.
- OCDE (2013[12]), Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel (les « Lignes directrices de l'OCDE sur la protection de la vie privée »).

Sécurité numérique

- OCDE (à paraître[13]), Recommandation du Conseil sur la gestion du risque de sécurité numérique.
- OCDE (à paraître[14]), Recommandation du Conseil sur les stratégies nationales en matière de sécurité numérique.
- OCDE (à paraître[15]), Recommandation du Conseil sur la sécurité numérique des produits et des services.
- OCDE (à paraître[16]), Recommandation du Conseil sur la gestion des vulnérabilités de sécurité numérique.
- OCDE (à paraître[17]), Cadre d'action sur la sécurité numérique.
- OCDE (2021[18]), « Understanding the digital security of products: An in-depth analysis », *Documents de travail de l'OCDE sur l'économie numérique*, n° 305, Éditions OCDE, Paris, https://doi.org/10.1787/abea0b69-en.
- OCDE (2021[19]), « Encouraging vulnerability treatment: Overview for policy makers », *Documents de travail de l'OCDE sur l'économie numérique*, n° 307, Éditions OCDE, Paris, https://doi.org/10.1787/0e2615ba-en.

2 Plateformes en ligne : facteur de facilitation des transactions et des interactions mondiales, mais aussi de remise en cause des cadres d'action

Les plateformes en ligne sont probablement l'archétype même du modèle économique numérique : un service qui facilite les interactions entre des groupes distincts d'utilisateurs, par l'intermédiaire de l'internet (OCDE, 2019[7]). Elles offrent aux consommateurs comme aux entreprises l'accès à de nouveaux marchés et de nouvelles opportunités, et permettent des transactions et des interactions mondiales qui, sans elles, seraient impossibles, notamment en fournissant des outils qui garantissent des échanges sûrs, dans des conditions de confiance, entre des parties qui ne se connaissent pas (Burdon, 2021[20]). On y trouve souvent des produits et services nouveaux de qualité, à des prix abordables voire sans contrepartie financière (mais parfois en échange du collecte de données). Elles ont été source de bouleversements pour les entreprises historiques du monde analogique et ont permis la diffusion d'informations pour aider les consommateurs faire des choix plus éclairés concernant les produits, les services ou les fournisseurs (OCDE, 2022[21]).

Aux prémices du World Wide Web, des modèles économiques expérimentaux ont vu le jour, pour disparaître rapidement (Furman et al., 2019[22]). Depuis le milieu des années 1990, une poignée de plateformes électroniques se sont toutefois imposées, attirant l'attention, les compétences, les données et les revenus. Même si les plateformes en ligne affichent une taille, des utilisateurs et des fonctionnalités variables (OCDE, 2019[7]), ces géants braquent l'attention des décideurs et du public sur des questions telles que la protection de la vie privée, la modération de contenu et l'intermédiation sur le marché du travail. Tandis qu'ils se taillent la part du lion sur les principaux marchés en ligne – du commerce électronique, aux recherches, en passant par la publicité en ligne et les médias sociaux (OCDE, 2022[21]) – leurs effets sur la concurrence font l'objet d'une attention particulière.

Les données économiques plus larges suggere que la concurrence sur les marchés du numérique tend à perdre en ampleur. Dans les pays de l'OCDE, les entreprises sont moins nombreuses à entrer sur les marchés et à en sortir (OCDE, 2021[23] ; Bajgar et al., 2019[24]) – un phénomène plus marqué encore dans les secteurs à forte intensité de numérique (Calvino et Criscuolo, 2019[25]). Si les start-ups spécialisées dans le numérique attirent d'importants investissements en fonds propres et en capital-risque, elles sont de plus en plus souvent rachetées par des acteurs de plus grande taille, avant d'avoir pu croître et prospérer (Bajgar, Criscuolo et Timmis, 2021[26]). Dans les pays de l'OCDE, on observe certes des phénomènes de concentration (Bajgar et al., 2019[24]), mais ils touchent tout particulièrement les secteurs qui reposent sur les logiciels et les données (Bajgar, Criscuolo et Timmis, 2021[26]). Ces tendances sont

d'autant plus préoccupantes que la concurrence est essentielle au maintien de prix bas, à l'innovation, à la croissance et au bien-être à long terme (OCDE, 2022[21]).

Dans ce contexte, les experts font valoir que certaines plateformes numériques jouissent d'un pouvoir de marché durable (OCDE, 2022[27] ; OCDE, 2022[21] ; OCDE, 2021[28]), en mettant l'accent sur les facteurs suivants :

- **Importants effets de réseau.** À mesure que le nombre d'utilisateurs augmente, la valeur qu'ils attribuent aux produits croît, ce qui a pour effet d'en attirer de nouveaux. Les marchés peuvent alors basculer vers une situation de monopole (où le « gagnant remporte tout ») (OCDE, 2022[21]).
- **Économies d'échelle.** Le coût de l'ajout d'un utilisateur supplémentaire étant généralement peu élevé, les plateformes peuvent facilement changer d'échelle et étendre leur couverture géographique sans devoir réaliser des investissements additionnels conséquents.
- **Collecte de données.** Les plateformes en ligne peuvent recueillir des données détaillées auprès des utilisateurs de toutes les faces d'un marché – consommateurs, annonceurs publicitaires et autres entreprises. Ces données peuvent aider à améliorer la qualité des produits, renforcer les effets de réseau, viser de nouvelles cibles et orienter la prise de décision des consommateurs (OCDE, 2022[29]). Allié à l'échelle, l'avantage que les données confèrent aux plateformes électroniques peut empêcher l'entrée d'autres acteurs (OCDE, 2022[27]).
- **Intégration verticale, conglomérats et liens entre les marchés.** Il n'est pas rare que les plateformes en ligne proposent plusieurs produits numériques (systèmes d'exploitation et appareils, par exemple) dans le cadre d'offres groupées axées sur les données, de sorte que les consommateurs ont parfois plus de difficultés à changer de prestataire (OCDE, 2022[27]). Elles peuvent également profiter de leur position dominante sur un marché (en utilisant par exemple leurs données ou en proposant des offres groupées) pour en pénétrer un autre. Les modèles économiques de certaines plateformes électroniques se caractérisent par une intégration verticale, qui peut obliger les concurrents en aval à dépendre d'elles pour accéder aux clients et ainsi provoquer des plaintes pour comportement anticoncurrentiel (lorsqu'une plateforme livre concurrence en aval sur la place de marché qu'elle exploite, par exemple) (OCDE, 2021[28]).

En conséquence, de nombreux pays ont adapté les outils de contrôle traditionnels, renforcé les capacités techniques des autorités et donné la priorité aux mesures d'application des lois relatives à la concurrence et la protection des consommateurs sur les marchés numériques. Par ailleurs, observant les caractéristiques structurelles des marchés numériques propices aux phénomènes de concentration, de nombreux pays et territoires ont proposé ou mis en œuvre des initiatives réglementaires supplémentaires ciblant un ensemble limité d'entreprises, en y incluant généralement les grandes plateformes en lignes (OCDE, 2021[28]). Si ces réglementations varient, elles tendent à couvrir les aspects suivants (OCDE, 2021[28]) :

- Les **préoccupations liées aux données**, notamment l'obligation d'autoriser les concurrents à accéder aux ensembles de données importants et de mettre en œuvre des mesures garantissant l'interopérabilité et la portabilité des données.
- La **perception du statut de « contrôleurs d'accès » des plateformes en ligne**, avec des mesures visant à limiter l'« autopréférence », qui consiste à mettre en avant leurs propres produits et services, ainsi que les offres groupées.
- Les **obligations en termes de transparence et de pratiques commerciales équitables**, avec des codes de conduite obligatoires et des exigences liées à la transparence des algorithmes, aux pratiques commerciales et publicitaires et à la collecte des données. Certaines règles proposées imposent des contraintes concernant les modalités de conservation, de traitement ou de transfert des données (observées ou déduites) des utilisateurs.

- Des **exigences supplémentaires liées aux fusions**, dont l'obligation d'informer les autorités de réglementation de toutes les opérations de fusion et d'acquisition pertinentes.

Bien que les réglementations proposées présentent certaines caractéristiques communes et visent toutes à promouvoir la concurrence en ligne, les mesures varient sensiblement d'un pays ou territoire à un autre. Or la fragmentation de l'environnement politique et réglementaire dans lequel évoluent les plateformes induit des coûts pour les entreprises comme les consommateurs, renforce l'incertitude et peut faire obstacle à l'innovation et le bien-être (OCDE, 2021[28]). De plus, compte tenu de l'envergure mondiale des plateformes en ligne, les effets des réglementations dans un pays ou territoire peuvent avoir des répercussions dans d'autres. Une approche mondiale cohérente aiderait à renforcer l'efficacité des règlementations et garantir que les marchés numériques restent concurrentiels et contestables, et contribuent au bien-être économique.

Partout dans le monde, les décideurs s'intéressent également de près aux questions liées à la protection des consommateurs. La responsabilité des plateformes en ligne à l'égard des comportements illégaux de leurs utilisateurs est souvent limitée du fait de leur position d'intermédiaires entre commerçants et consommateurs (Burdon, 2021[20]). En revanche, l'une de leurs caractéristiques tient à leur capacité de contrôler leur propre écosystème, car les expériences positives favorisant la fidélisation des utilisateurs sont essentielles à leur réussite (OCDE, 2019[7]). Cela passe généralement par la mise en place de règles sur les utilisateurs habilités à utiliser les plateformes et la façon dont ils s'y conduisent. Elles peuvent surveiller leurs comportements pour s'assurer qu'ils respectent les règles et encourager la conformité en prenant des mesures contre les éventuels contrevenants (par exemple des mesures d'exclusion).

Dans la pratique, malgré les investissements réalisés dans les outils de surveillance et la mise en place de processus de détection des cas de non-respect des règles, les plateformes peinent à réglementer le comportement des utilisateurs. Certaines entreprises prennent des mesures pour protéger les consommateurs, mais les escroqueries, la vente de produits dangereux ou contrefaits, et les faux avis et évaluations perdurent sur de nombreuses places de marché (OCDE, 2022[6]). En conséquence, les décideurs et les autorités chargées de la concurrence et de la protection des consommateurs poussent les plateformes vers davantage d'autorégulation et vers des modèles alternatifs de réglementation pilotée par les pouvoirs publics, à l'instar des engagements en matière de sécurité des produits (OCDE, 2021[30])[1]. Les décideurs s'interrogent en outre sur la nécessité éventuelle de renforcer la responsabilité des plateformes à l'égard des actions de leurs utilisateurs, afin de mieux protéger les consommateurs.

3 Flux transfrontières de données : moteur d'échanges et de coopération à l'échelle mondiale, mais source de préoccupations pour les pouvoirs publics

L'architecture de l'internet permet aux informations de circuler entre les différents réseaux et par-delà les frontières. Entreprises et consommateurs en ont rapidement profité pour concevoir de nouveaux modèles économiques et accéder aux marchés mondiaux. À tel point qu'aujourd'hui, les flux de données sous-tendent les échanges internationaux de nombreux biens et services. Ils permettent aux entreprises de bâtir et gérer des chaînes logistiques mondiales complexes, aux organisations de partager des données à l'appui de la recherche, et aux consommateurs de s'informer sur les produits et les services proposés partout dans le monde.

Si la contribution des flux transfrontières de données à la valeur ajoutée mondiale est probablement notable, elle n'est pas bien comprise. Il est difficile de distinguer leur valeur des statistiques relatives aux échanges ou aux technologies de l'information et des communications (TIC), et l'on continue de manquer de données empiriques concluantes. Cela dit, on estime que les TIC ont impulsé la vague la plus récente d'intégration mondiale, qui a ouvert la voie à un développement économique rapide dans certains pays en développement (Baldwin, 2017[31]).

En même temps, les flux transfrontières de données exacerbent certaines préoccupations des pouvoirs publics, les poussant à instaurer des conditions et des modalités spécifiques pour transférer les données par-delà les frontières. Les raisons justifiant la mise en place de réglementations et de politiques sont les suivantes (Casalini et López-Gonzalez, 2019[32] ; Aaronson, 2019[33]) :

- **Protection de la vie privée.** Les flux transfrontières de données à caractère personnel soulèvent des questions liées à la protection des données et de la vie privée, en particulier lorsque les cadres réglementaires nationaux diffèrent de ceux des pays ou territoires destinataires. Certains gouvernements s'inquiètent par ailleurs du risque que les données à caractère personnel ainsi transférées ne fassent l'objet d'une surveillance par les pays étrangers.
- **Sécurité.** Les pouvoirs publics pourraient réglementer les flux transfrontières de données dans le but de protéger des informations qu'ils jugent sensibles du point de vue de la sécurité nationale ou d'éviter que des consommateurs et des entreprises nationaux ne subissent des préjudices (utilisation frauduleuse de cartes de crédit, vol d'identité pour les premiers, ou attaques par rançongiciel pour les secondes, par exemple).

- **Protection des droits de propriété intellectuelle.** Les pouvoirs publics pourraient réglementer les flux transfrontières de données dans le but de protéger les droits de propriété intellectuelle (marques, droits d'auteur, secrets commerciaux, etc.).
- **Accès réglementaire.** Les autorités de réglementation nationales ont souvent besoin d'accéder à des données aux fins du contrôle de l'application des lois. Les pouvoirs publics de certains pays pourraient exiger que les données soient stockées sur le territoire national pour en garantir l'accès.

Par ailleurs, on avance souvent que les pouvoirs publics pourraient assortir les flux transfrontières de données de conditions ou exiger des entreprises qu'elles stockent les données sur le territoire national dans le cadre de ce qui constituerait une politique industrielle du numérique (ou un protectionnisme numérique). Des régimes autocratiques ont également été accusés d'entraver les flux transfrontières de données pour brider la liberté d'expression ou comme une forme d'oppression politique (Fan et Gupta, 2018[34]).

Compte tenu de ces diverses motivations et des différences culturelles et historiques qui président aux approches privilégiées, les pouvoirs publics du monde entier optent pour différents types de mesures pour réglementer les flux transfrontières de données. Certains énoncent des principes de responsabilité généraux ayant une portée extraterritoriale. D'autres assortissent les transferts transfrontières de garanties spécifiques, telles que l'obligation que le pays figure sur une liste de destinations autorisées dressée par les autorités nationales (bien que les critères varient selon les pays et ne soient pas toujours transparents), ou que des contrats lient les parties qui échangent les données (avec dans certains cas des clauses pré-approuvées). D'autres mesures encore exigent que tout transfert de données à l'étranger soit examiné et approuvé. Au-delà des différences quant à la teneur des mesures réglementaires, celles-ci s'appliquent à divers types de données et de secteurs. Les définitions et notions peuvent également varier : par exemple, il n'existe pas de consensus sur ce que recouvrent les informations à caractère personnel.

Les réglementations qui visent à renforcer la confiance en ligne abordent les données comme un levier de l'économie mondiale. Mais elles peuvent également s'avérer coûteuses, en particulier lorsqu'elles sont vagues, fragmentées, ou qu'elles manquent de transparence. Lorsque la portée et l'application des règles varient selon les pays ou territoires, les entreprises du numérique se retrouvent confrontées à un environnement réglementaire mondial complexe et incertain. Par exemple, les tentatives de fournir une base juridique aux transferts de données à caractère personnel entre les États-Unis et l'UE ont avorté à deux reprises depuis 2015. Les entreprises ont besoin d'un environnement réglementaire stable pour prendre leurs décisions et définir leurs plans d'investissement, et certaines craignent que le contexte confus et changeant ne mette en péril les débouchés économiques. Les exigences peuvent être difficiles, voire impossibles, à mettre en œuvre d'un point de vue technique, et les petites entreprises – y compris les start-ups à forte croissance – peuvent avoir plus de mal à supporter les coûts de mise en conformité. Avec, à la clé, le risque d'une concentration plus élevée encore des marchés numériques et d'une baisse du dynamisme des entreprises.

La coopération internationale en faveur de la « libre circulation des données dans des conditions de confiance » est essentielle pour réduire la fragmentation et affronter les défis qui se font jour. Les fondements existent, à l'instar des Lignes directrices de l'OCDE sur la protection de la vie privée, qui jettent les bases d'une réglementation dans ce domaine ; du système de certification mis au point par la Coopération économique Asie-Pacifique pour les transferts de données entre les économies participantes ; ou de la Convention 108 du Conseil européen, qui énonce des règles sur la protection et les transferts de données entre les parties. Par ailleurs, certains accords commerciaux contiennent des dispositions contraignantes visant à préserver la circulation des données entre les pays lorsque des cadres de protection sont en place. Le renforcement de l'interopérabilité des cadres de protection de la vie privée a fait l'objet d'une attention particulière, afin de permettre aux pays disposant de normes différentes en la matière de continuer d'échanger des données. Enfin, les technologies protectrices de la vie privée pourraient contribuer à réduire les risques d'atteinte à la vie privée et, partant, favoriser le partage et

l'utilisation de données à caractère personnel, y compris à l'échelle internationale. Les pouvoirs publics doivent évaluer ces avancées et déterminer les prochaines étapes pour définir des politiques qui servent les intérêts des individus et des entreprises.

4 Sécurité : levier fondamental ou talon d'Achille de la transformation numérique ?

À mesure que de plus en plus de secteurs de l'économie dépendent des technologies numériques, la cybersécurité devient un enjeu majeur. La confiance dans la transformation numérique et sa progression passent en effet par une sécurité efficace. Or, jusqu'à présent, le rythme effréné de la transformation numérique ne s'est pas accompagné d'une augmentation proportionnée du niveau de sécurité des appareils et des services. Si des progrès ont été accomplis en termes de normalisation des bonnes pratiques (gestion coordonnée des vulnérabilités ou exigences de sécurité pour l'internet des objets, par exemple), les prescriptions de base n'ont pas été mises en œuvre par les organisations à toutes les échelles. Les décideurs du monde entier ont aujourd'hui la possibilité de relever ces défis, qui ont souvent une dimension internationale, en concentrant leurs efforts sur les résultats souhaités pour l'utilisateur final et en s'appuyant sur les normes techniques et les meilleures pratiques sectorielles mondiales pour renforcer l'interopérabilité.

L'internet des objets (IdO) – qui allie des appareils et des objets connectés à l'internet – présente un défi plus large encore en termes de sécurité numérique. L'IdO grand public, également connu sous le nom de produits « intelligents » ou « connectés », augmente la surface d'attaque, jusque-là cantonnée aux technologies de l'information et des communications (TIC) traditionnelles utilisées par les consommateurs, les entreprises et les pouvoirs publics. Les appareils intelligents constituent une surface d'attaque croissante de produits vulnérables adoptés par les consommateurs et intégrés aux réseaux. On dénombrait, en 2019, quelque 7.7 milliards d'appareils IdO (Statista, 2022[35]) et, selon une récente enquête, 78.4 % des fabricants de dispositifs IdO grand public ne disposent pas d'un processus interne de gestion des vulnérabilités (IoT Security Foundation, 2021[36]), pourtant essentielle à la protection continue des produits et de leurs utilisateurs.

Un nombre relativement restreint d'acteurs malveillants sont parvenus à capitaliser sur la transformation numérique en adoptant les modèles économiques de la cybercriminalité pour tenter de se soustraire aux lois conventionnelles. Les raçongiciels sont devenus une menace courante qui vise des entreprises et des organisations de tous types, quelles que soient leur taille et leur localisation. En 2021, aux États-Unis, les opérateurs d'infrastructures critiques ont déposé 649 plaintes auprès du FBI, et dans 14 des 16 secteurs d'infrastructures critiques, au moins un membre avait été la cible d'une attaque par rançongiciel (FBI, 2021[37]). De même, les systèmes d'information présentent des vulnérabilités liées à la façon dont les logiciels ont été conçus, développés, mis en œuvre et mis à jour. Les cybercriminels développent, vendent et utilisent des outils, tels que des logiciels malveillants, dans le but d'exploiter ces vulnérabilités en perpétrant des attaques qui portent préjudice à des entreprises, des administrations et des personnes, menacent les activités critiques et sapent la confiance placée dans la transformation numérique.

Les coûts inhérents à un écosystème numérique vulnérable peuvent être considérables. On estime en effet que le coût potentiel mondial des cyberattaques atteint 6 000 milliards USD par an (soit l'équivalent du PIB cumulé de l'Allemagne et de la France) et qu'il augmente chaque année (OCDE, 2021[38]). Les

criminels visent des personnes ou des organisations qui dépendent du numérique. Selon le CyberPeace Institute, en 2021, 253 incidents ont touché le secteur de la santé dans 32 pays, avec des conséquences opérationnelles qui ont duré en moyenne plus de 21 jours, et quelque 13 millions de dossiers concernés (CyberPeace Institute, s.d.[39]).

Dans un monde idéal, le jeu des forces du marché devrait faire que les produits, notamment ceux contenant du code (logiciels, appareils IdO, etc.) et les services connexes (d'infonuagique, par exemple) soient suffisamment sécurisés, et que les développeurs adaptent la sécurité en fonction du risque qui pèse sur les utilisateurs, et ce, tout au long du cycle de vie des produits. Des analyses de l'OCDE montrent toutefois que des défaillances de marché empêchent les parties prenantes de déterminer avec précision la valeur de la sécurité numérique des produits et des services, et qu'il est peu probable que les mécanismes d'incitation du marché puissent à eux seuls permettre de combler les lacunes de la gestion du risque de sécurité numérique (OCDE, 2021[38]). En particulier, l'attribution des responsabilités quant à la correction des vulnérabilités et l'amélioration de la sécurité reste floue, compte tenu de la complexité et de l'opacité des chaînes logistiques.

Il est généralement difficile aux utilisateurs finaux, notamment aux petites et moyennes entreprises et aux consommateurs, de savoir quel niveau de sécurité a été intégré dès la phase de conception aux produits et services qu'ils acquièrent. Sans cette pression, outre les complexités inhérentes notamment aux chaînes logistiques internationales, les fournisseurs tendent à reléguer au second plan la sécurité numérique, ce qui permet aux acteurs malveillants d'utiliser ces produits pour lancer des attaques, y compris par-delà les frontières. De manière plus générale, on méconnaît le risque de sécurité numérique et les incitations du marché sont inadaptées. Une enquête réalisée en 2020 révèle qu'au Royaume-Uni, 28 % des consommateurs ont indiqué qu'ils ne cherchaient pas activement à acheter des produits connectés par crainte des risques de sécurité (DCMS, 2020[40]).

La plupart des enjeux inhérents à la sécurité numérique (et plus largement à la transformation numérique) ont une portée mondiale. Les chaînes logistiques sont complexes et internationales, ce qui pose des difficultés aux législateurs. Dans le même temps, les prestataires de services infonuagiques et de services gérés opèrent à l'échelle transfrontières, ce qui les rend vulnérables aux attaques d'acteurs malveillants, où qu'ils soient. Pour autant, les chercheurs en sécurité travaillent eux aussi par-delà les frontières, et les cadres juridiques instaurant des « sphères de sécurité » (*safe harbour*) doivent, pour être efficaces, reposer sur des principes reconnus au plan international.

5 Conclusion : Un Bretton Woods pour le numérique ? Le rôle de l'OCDE dans la gouvernance mondiale du numérique

L'internet a évolué pour s'adapter à la croissance exponentielle du nombre d'utilisateurs et d'appareils à l'échelle internationale (OCDE, 2016[3]) et a ouvert la voie à une ère d'activité économique elle aussi mondiale. Avec la transformation numérique, les services, les technologies et applications, et les appareils sont disponibles partout sur la planète. Dans un monde interconnecté et interdépendant, les défis auxquels sont confrontés les pouvoirs publics ont par nature une portée internationale, avec des effets qui dépassent aisément le cadre des frontières.

Néanmoins, c'est souvent par le biais des politiques nationales que l'on a géré les questions de fond soulevées par les plateformes électroniques, les flux transfrontières de données et la sécurité numérique. Non seulement ces politiques ont moins de chances d'être efficaces, mais la fragmentation de l'environnement qui en résulte ouvre la voie à des règles du jeu inéquitables et à une protection inégale des consommateurs et des entreprises qui profitent de l'économie mondiale.

La période qui a suivi la Première Guerre mondiale a été marquée par des crises économiques et une montée des tensions géopolitiques. Pourtant, au lieu de faire le choix de la coopération internationale, les pays ont adopté des politiques qui les avantageaient au détriment des autres, creusant par là même les divisions. À la fin de la Seconde Guerre mondiale, un groupe de pays s'est réuni à Bretton Woods, dans l'État américain du New Hampshire, pour créer un système d'institutions internationales, partant du principe que seule la coopération permettrait de tirer parti d'une économie mondiale.

Les observateurs invoquent de plus en plus cette vague de multilatéralisme de l'après-guerre lorsqu'ils plaident pour la mise en place de cadres d'action mondiaux en matière de numérique. Bien que la terminologie varie, les messages convergent : des appels ont en effet été lancés en faveur d'un « Bretton Woods pour les politiques du numérique » (Rockefeller Foundation, 2021[41] ; Greenwald, 2020[42] ; Clegg, 2021[43] ; Tett, 2019[44]), d'un « Conseil de stabilité numérique » (CIGI, 2019[45]), ou d'une « Convention de Genève relative au numérique » (Microsoft, 2017[46]). Les institutions publiques défendent elles aussi la nécessité de mettre au point des cadres d'action mondiaux en matière de numérique, mettant l'accent sur trois caractéristiques : (1) l'élaboration de normes et de principes minimums communs à l'échelle internationale ; (2) l'amélioration de la mesure et du suivi des technologies numériques et des questions connexes ; et (3) un engagement multipartite inclusif (Banque mondiale, 2021[47] ; Nations Unies, 2019[48] ; CNUCED, 2021[49] ; Haksar et al., 2021[50]).

L'OCDE, qui puise ses racines dans cette vague de multilatéralisme et dispose d'une connaissance pointue de l'élaboration des politiques du numérique, est bien placée pour répondre à ces appels :

- **L'OCDE joue de longue date un rôle de premier plan dans le domaine des politiques du numérique, notamment dans l'élaboration de normes et de cadres d'action internationaux**. En 1980, elle a élaboré les *Lignes directrices de l'OCDE sur la protection de la vie privée*, qui ont été révisées en 2013 et continuent de faire office de norme minimum sur laquelle s'appuient les pays du monde entier pour codifier la protection de la vie privée et des données. L'Organisation est également à l'origine des premières normes approuvées au plan international sur la sécurité numérique au service de la croissance et de la prospérité (OCDE, à paraître[13] ; OCDE, à paraître[14] ; OCDE, à paraître[15] ; OCDE, à paraître[16]), des principes relatifs à l'accès aux données et à leur partage (OCDE, 2021[11]), des *Principes de l'OCDE sur l'intelligence artificielle* (OCDE, 2019[51]), les premiers du genre, et de la *Recommandation du Conseil sur la protection du consommateur dans le contexte du commerce électronique* (OCDE, 2016[9]). La mise en œuvre de ces recommandations fait l'objet d'un suivi régulier. De plus, l'OCDE dispose de connaissances pointues dans les domaines d'action concernés par les données et les technologies numériques– fiscalité, concurrence, protection des consommateurs, protection de la vie privée, gouvernance des données, sécurité numérique, échanges, ou encore marchés financiers et du travail. On lui doit par ailleurs le premier cadre d'action intégré complet pour la conception et la mise en œuvre de politiques du numérique faisant intervenir toutes les sphères de l'action gouvernementale (OCDE, 2020[52]).
- **L'OCDE est reconnue pour ses travaux de mesure, de suivi et d'évaluation des technologies numériques et de leurs effets économiques et sociaux**. L'Organisation mène les efforts internationaux déployés pour mesurer différents aspects de la transformation numérique – dont les échanges numériques (OCDE-OMC-FMI, 2020[53]) et les données (OCDE, à paraître[54]) – dans les statistiques économiques et dans le cadre de la *Feuille de route sur la mesure de la transformation numérique* (OCDE, 2022[55]). Pour le suivi des retombées de l'économie numérique, l'OCDE a mis au point des outils et des indicateurs afin d'éclairer l'action des pouvoirs publics ; la *Boîte à outils de l'OCDE sur la transformation numérique* et l'*Observatoire OCDE des politiques relatives à l'IA* en sont des exemples. En outre, l'Organisation examine et évalue les effets de technologies numériques émergentes telles que l'intelligence artificielle et la technologie des chaînes de blocs (OCDE, 2022[56]).
- **L'OCDE offre un modèle de dialogue inclusif, mondial et multipartite sur les politiques de l'économie numérique**. En tant que forum d'échange d'idées et de bonnes pratiques entre plus de 100 pays, l'OCDE rassemble des décideurs et des responsables de l'action publique venant partager des enseignements, identifier les meilleures pratiques et élaborer des politiques fondées sur des données probantes pour un monde numérique en constante évolution. Les débats sur les politiques de l'économie numérique qui s'y tiennent suivent une approche multipartite où l'expérience et l'expertise des entreprises, des syndicats, de la société civile et de la communauté technique de l'internet sont mises en commun pour faire en sorte que la transformation numérique soit porteuse de prospérité, tout en intégrant les questions de sécurité. Les travaux de l'OCDE sur la réforme de la fiscalité internationale à l'ère numérique illustrent par ailleurs sa capacité à faire émerger un consensus sur les questions transversales complexes soulevées par la transformation numérique (OCDE, 2022[57]). Le *Forum mondial sur la concurrence* (OCDE, 2022[58]) et le *Forum mondial sur la sécurité numérique pour la prospérité* (OCDE, 2022[59]) témoignent également de l'engagement multilatéral pluridisciplinaire mené par l'Organisation.

Institutions internationales et organismes responsables des politiques publiques reconnaissent la nécessité de mettre au point des cadres d'action mondiaux dans le domaine du numérique. De par le mandat que lui confient les pays et en concertation avec les organisations internationales compétentes, l'OCDE peut mettre à profit son rôle bien établi, son savoir-faire institutionnel, son éventail d'outils d'analyse et sa capacité avérée à travailler de concert avec des pays et des groupes de parties prenantes pour dessiner une trajectoire ambitieuse pour l'élaboration des politiques du numérique et traiter les

questions de fond qui vont de pair avec une économie et une société mondiales interdépendantes et tournées vers le numérique.

Notes

[1] Au titre des « engagements en matière de sécurité des produits », les plateformes s'engagent à prendre des mesures qui dépassent le cadre de leurs obligations juridiques pour protéger les consommateurs contre les produits dangereux (déréférencement des produits dangereux dans un délai donné à compter de la notification par les autorités compétentes, par exemple). Le Groupe de travail de l'OCDE sur la sécurité des produits de consommation a publié récemment un communiqué appelant les pouvoirs publics à élaborer davantage d'accords d'engagements de ce type, et les places de marché à envisager l'intégration de quatre engagements afin de favoriser la cohérence l'échelle internationale (OCDE, 2021[30]).

Références

Aaronson, S. (2019), « What Are We Talking about When We Talk about Digital Protectionism? », *World Trade Review*, vol. 18/4, pp. 541-577, https://doi.org/10.1017/S1474745618000198. [33]

Bajgar, M. et al. (2019), *Industry Concentration in Europe and North America*, Éditions OCDE, Paris, https://doi.org/10.1787/2ff98246-en. [24]

Bajgar, M., C. Criscuolo et J. Timmis (2021), *Intangibles and industry concentration: Supersize me*, Éditions OCDE, Paris, https://doi.org/10.1787/ce813aa5-en. [26]

Baldwin, R. (2017), *The Great Convergence*, Harvard University Press, https://doi.org/10.4159/9780674972667. [31]

Banque mondiale (2021), *World Development Report*, World Bank Publishing, Washington DC, https://www.worldbank.org/en/publication/wdr2021. [47]

Burdon, T. (2021), « The role of online marketplaces in enhancing consumer protection », *OECD Going Digital Toolkit Notes No. 7*, Éditions OCDE, Paris, https://doi.org/10.1787/ddca0e2e-en. [20]

Calvino, F. et C. Criscuolo (2019), *Business dynamics and digitalisation*, Éditions OCDE, Paris, https://doi.org/10.1787/6e0b011a-en. [25]

Casalini, F. et J. López-Gonzalez (2019), *Trade and Cross-Border Data Flows*, OECD, Paris, https://doi.org/10.1787/b2023a47-en (consulté le 4 mars 2022). [32]

CIGI (2019), *Digital Platforms Require Global Governance Frameworks*, https://www.cigionline.org/articles/digital-platforms-require-global-governance-framework/. [45]

Clegg, N. (2021), *A Bretton Woods for the Digital Age can Save the Open Internet*, https://www.afr.com/technology/a-bretton-woods-for-the-digital-age-can-save-the-open-internet-20211115-p5994h. [43]

CNUCED (2021), *Édition 2021 des Report de l'économie numérique*, https://unctad.org/page/digital-economy-report-2021. [49]

Corrado, C. et al. (2021), *New evidence on intangibles, diffusion and productivity*, Éditions OCDE, Paris, https://doi.org/10.1787/de0378f3-en. [63]

Cory, N. et L. Dascoli (2021), *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*, Information Technology & Innovation Foundation, https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost (consulté le 5 avril 2022). [62]

CyberPeace Institute (s.d.), *Cyber Incident Tracer #HEALTH*, https://cit.cyberpeaceinstitute.org/explore (consulté le 11 juillet 2022). [39]

DCMS (2020), *Evidencing the Cost of the UK Government's Proposed Regulatory Interventions for Consumer IoT*, UK Department for Digital, Culture, Media & Sport, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/900330/Evidencing_the_cost_of_the_UK_government_s_proposed_regulatory_interventions_for_consumer_internet_of_things__IoT__products.pdf (consulté le 11 juillet 2022). [40]

Fan, Z. et A. Gupta (2018), *The Dangers of Digital Protectionism*, https://hbr.org/2018/08/the-dangers-of-digital-protectionism (consulté le 6 octobre 2022). [34]

FBI (2021), *Internet Crime Report*, U.S. Federal Bureau of Investigation, Washington, D.C., https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (consulté le 11 juillet 2022). [37]

Furman, J. et al. (2019), *Unlocking digital competition: Report from the Digital Comeptition Expert Panel*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/785547/unlocking_digital_competition_furman_review_web.pdf. [22]

Gierten, D. et M. Lesher (2022), *Assessing National Digital Strategies and Their Governance*, Éditions OCDE, Paris, https://doi.org/10.1787/baffceca-en (consulté le 11 juillet 2022). [4]

Gray, M. (1996), *Web Growth Summary*, https://www.mit.edu/people/mkgray/net/web-growth-summary.html (consulté le 17 October 2022). [2]

Greenwald, M. (2020), *A new era in financial diplomacy: The third evolution of Bretton Woods*, https://www.atlanticcouncil.org/blogs/new-atlanticist/a-new-era-in-financial-diplomacy-the-third-evolution-of-bretton-woods/. [42]

Haksar, V. et al. (2021), *Toward a Global Approach to Data in the Digital Age*, https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/10/06/Towards-a-Global-Approach-to-Data-in-the-Digital-Age-466264. [50]

Internet Live Stats (2022), *Total number of Websites*, https://www.internetlivestats.com/total-number-of-websites/ (consulté le 8 juillet 2022). [61]

IoT Security Foundation (2021), *The Contemporary Use of Vulnerability Disclosure in IoT (Report 4)*, https://www.iotsecurityfoundation.org/wp-content/uploads/2021/11/The-Contemporary-Use-of-Vulnerability-Disclosure-in-IoT-IoTSF-Report-4-November-2021.pdf (consulté le 11 juillet 2022). [36]

McFadden, J. et al. (2022), *The digitalisation of agriculture: A literature review and emerging policy issues*, Éditions OCDE, Paris. [60]

Microsoft (2017), *The need for a Digital Geneva Convention*, https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/. [46]

Nations Unies (2019), *The age of digital interdependence*, https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf. [48]

Netcraft (2022), *Web Server Survey*, https://news.netcraft.com/archives/category/web-server-survey/ (consulté le 17 October 2022). [1]

OCDE (2022), « Dark Commercial Patterns », *Documents de travail de l'OCDE sur l'économie numérique,* N° 336, https://doi.org/10.1787/44f5e846-en. [29]

OCDE (2022), *Forum mondial sur la concurrence*, https://www.oecd.org/fr/concurrence/forum-mondial/. [58]

OCDE (2022), *Forum mondial sur la sécurité numérique pour la prospérité*, https://www.oecd.org/digital/global-forum-digital-security/about/. [59]

OCDE (2022), *Global Blockchain Policy Centre*, https://www.oecd.org/daf/blockchain/. [56]

OCDE (2022), *International collaboration to end tax avoidance*, https://www.oecd.org/tax/beps/. [57]

OCDE (2022), *OECD Handbook on Competition Policy in the Digital Age*, https://www.oecd.org/daf/competition/oecd-handbook-on-competition-policy-in-the-digital-age.pdf. [21]

OCDE (2022), « The Evolving Concept of Market Power in the Digital Economy », *Forum mondial sur la concurrence - Note du Secrétariat*, https://www.oecd.org/daf/competition/the-evolving-concept-of-market-power-in-the-digital-economy-2022.pdf. [27]

OCDE (2022), *The OECD Going Digital Measurement Roadmap*, Éditions OCDE, Paris, https://doi.org/10.1787/bd10100f-en. [55]

OCDE (2022), « The role of online marketplaces in protecting and empowering consumers: Country and business survey findings », *Documents de travail de l'OCDE sur l'économie numérique*, n° 329, Éditions OCDE, Paris, https://doi.org/10.1787/9d8cc586-en. [6]

OCDE (2021), *Encouraging vulnerability treatment: Overview for policy makers*, Éditions OCDE, Paris. [19]

OCDE (2021), « Ex Ante Regulation and Competition in Digital Markets », *Document de travail du Comité de la concurrence de l'OCDE*, https://www.oecd.org/daf/competition/ex-ante-regulation-and-competition-in-digital-markets-2021.pdf. [28]

OCDE (2021), *Orientations pratiques concernant les engagements relatifs à la sécurité des produits de consommation*, https://one.oecd.org/document/DSTI/CP/CPS(2021)8/FINAL/fr/pdf. [30]

OCDE (2021), *Recommandation du Conseil sur l'amélioration de l'accès aux données et de leur partage*, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0463 (consulté le 21 avril 2022). [11]

OCDE (2021), *Smart Policies for Smart Products: A Policy Maker's Guide to Enhancing the Digital Security of Products*, Éditions OCDE, Paris, https://www.oecd.org/digital/smart-policies-for-smart-products.pdf (consulté le 11 juillet 2022). [38]

OCDE (2021), *Strengthening Economic Resilience Following the COVID-19 Crisis: A Firm and Industry Perspective*, Éditions OCDE, Paris, https://doi.org/10.1787/2a7081d8-en. [23]

OCDE (2021), *Understanding the digital security of products: An in-depth analysis*, Éditions OCDE, Paris. [18]

OCDE (2020), *Going Digital integrated policy framework*, Éditions OCDE, Paris, https://doi.org/10.1787/dc930adc-en. [52]

OCDE (2019), *An Introduction to Online Platforms and Their Role in the Digital Transformation*, Éditions OCDE, Paris, https://doi.org/10.1787/53e5f593-en. [7]

OCDE (2019), *Recommandation du Conseil sur l'intelligence artificielle*, OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0449. [51]

OCDE (2019), *Unpacking E-commerce: Business Models, Trends and Policies*, Éditions OCDE, Paris, https://doi.org/10.1787/23561431-en. [8]

OCDE (2016), *Digital Convergence and Beyond: Innovation, Investment and Competition in Communication Policy and Regulation for the 21st Century*, Éditions OCDE, Paris, https://doi.org/10.1787/5jlwvzzj5wvl-en. [3]

OCDE (2016), *Recommandation du Conseil sur la protection du consommateur dans le contexte du commerce électronique*, OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0422. [9]

OCDE (2013), *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OCDE, https://legalinstruments.oecd.org/fr/instruments/OECD-LEGAL-0188. [12]

OCDE (à paraître), « Data shaping firms and markets », *Documents de travail de l'OCDE sur l'économie numérique*, Éditions OCDE, Paris. [5]

OCDE (à paraître), « Fostering cross-border data flows with trust », *Documents de travail de l'OCDE sur l'économie numérique*, Éditions OCDE, Paris. [10]

OCDE (à paraître), « Measuring the value of data and data flows », *Documents de travail de l'OCDE sur l'économie numérique*, Éditions OCDE, Paris. [54]

OCDE (à paraître), *Policy Framework on Digital Security*, Éditions OCDE, Paris. [17]

OCDE (à paraître), *Recommandation sur la gestion des vulnérabilités de sécurité numérique*, OCDE. [16]

OCDE (à paraître), *Recommandation sur la gestion du risque de sécurité numérique*, OCDE. [13]

OCDE (à paraître), *Recommandation sur la sécurité numérique des produits et des services*, OCDE. [15]

OCDE (à paraître), *Recommandation sur les stratégies nationales en matière de sécurité numérique*, OCDE. [14]

OCDE-OMC-FMI (2020), *Handbook on Measuring Digital Trade*, https://www.oecd.org/sdd/its/Handbook-on-Measuring-Digital-Trade-Version-1.pdf. [53]

Rockefeller Foundation (2021), *A Bretton Woods for AI: Ensuring Benefits for Everyone*, https://www.rockefellerfoundation.org/blog/a-bretton-woods-for-ai-ensuring-benefits-for-everyone/;. [41]

Statista (2022), *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030*, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (consulté le 11 juillet 2022). [35]

Tett, G. (2019), *Do we need an IMF to regulate the internet?*, https://www.ft.com/content/4526982e-60a0-11e9-b285-3acd5d43599e (consulté le 20 February 2022). [44]