Centres for European Policy Network
FREIBURG | BERLIN | PARIS | ROMA

Les **Études** du cep

Un leadership européen en matière d'économie numérique

Dix-sept recommandations

Bert Van Roosebeke, Martina Anzini, Philipp Eckhardt & Anne-Carine Pierrat

Le présent document est la synthèse d'une étude réalisée pour la société SAP. Les opinions exprimées dans cette étude sont celles de ses auteurs et ne reflètent pas nécessairement le point de vue de la société SAP.

L'intégralité de l'étude est disponible en langue anglaise en cliquant ici.

Fribourg-en-Brisgau, février 2020

Auteurs :

Bert Van Roosebeke, Directeur de recherches

Martina Anzini

Philipp Eckhardt

Anne-Carine Pierrat

Centrum für Europäische Politik FREIBURG | BERLIN

Kaiser-Joseph-Strasse 266 | D-79098 Freiburg

Schiffbauerdamm 40 4315 | D-10117 Berlin

Tel. + 49 761 38 69 30

cep@cep.eu

Traduction et publication :

Centre de Politique Européenne PARIS

350, rue Lecourbe | F-75015 Paris

Tel. + 33 1 45 54 91 55

cepfrance@cep.eu

Le **Centre de Politique Européenne** PARIS et ses instituts partneraires,
Centrum für Europäische Politik FREIBURG | BERLIN et **Centro Politiche Europee** ROMA,
constituent le **Centres for European Policy Network** FREIBURG | BERLIN | PARIS | ROMA.

Les instituts cep sont spécialisés dans l'analyse et l'évaluation de la politique d'intégration européenne. Ils publient leurs travaux scientifiques indépendamment de tout intérêt partisan, à la faveur d'une Union européenne respectueuse de l'état de droit et des principes de l'économie sociale de marché.

SYNTHESE

L'écart entre l'Europe et les États-Unis ou la Chine se creuse de plus en plus, en particulier dans les domaines de l'Intelligence artificielle et du *Cloud Computing*, deux des principales évolutions techniques mondiales qui auront un impact considérable sur la croissance économique dans les années à venir. La présente étude identifie trois priorités principales et formule dix-sept recommandations détaillées de mesures politiques à l'échelle de l'UE, à l'aide desquelles l'UE pourrait reprendre un rôle de leader dans le domaine de l'économie numérique. Il est urgent de définir ces priorités.

Alors que les effets de réseau et les économies d'échelle ont permis aux entreprises américaines et chinoises d'occuper une position dominante sur les marchés B2C, l'UE devrait maintenant prendre les mesures nécessaires pour éviter que cela ne se reproduise sur les marchés B2B.

Les mesures protectionnistes ne permettront pas de regagner une souveraineté technologique européenne. Les trois priorités identifiées ont au contraire toutes une approche orientée vers le marché, stimulant l'innovation et préservant la concurrence entre les fournisseurs de l'économie numérique.

Priorité n°1 : l'UE devrait aspirer à la mise en place d'un véritable marché intérieur des données, puisqu'elle est encore loin d'exploiter le potentiel économique lié au partage et à la (ré-)utilisation des données présentes sur son territoire. A toutes les étapes politiques et réglementaires, les initiatives dans ce domaine devraient concerner les données personnelles, publiques et non personnelles.

Concernant les données personnelles, nous préconisons une plus grande harmonisation et l'utilisation de *sandboxes* et de sas réglementaires (*regulatory hubs*) afin d'accroître la sécurité juridique lors de l'application du Règlement Général sur la Protection des Données (RGPD).

La disponibilité des données publiques devrait être simplifiée par la normalisation des formats de données. La mise à disposition des données devrait être un critère décisif lors de l'attribution de marchés publics. L'accès aux données publiques de grande valeur („high-value datasets“) devrait être assoupli.

Les raisons pour lesquelles les entreprises sont réticentes à partager et à mettre en commun des données non personnelles sont très diverses et ne peuvent pas toutes être résolues par des mesures réglementaires. L'initiative de l'UE visant à créer des espaces de données sectoriels peut cependant contribuer à réduire les coûts de transactions liés à l'utilisation commune de données B2B.

Les exigences nationales de localisation des données relatives au stockage des données personnelles, publiques ou non personnelles sont un obstacle à la réalisation d'économies d'échelle et sont généralement incompatibles avec l'idée d'un marché intérieur des données. Elles doivent demeurer l'exception. La Commission devrait poursuivre de manière conséquente les États membres lorsque leurs exigences de localisation qui, selon le RGPD et le règlement relatif au libre flux des données non personnelles, ne sont justifiées.

Deuxième priorité, l'UE devrait garantir une concurrence effective sur les marchés numériques dans le domaine du B2B. Les marchés B2B sont très différents des marchés B2C et nous ne considérons pas qu'une action réglementaire soit nécessaire pour y préserver la concurrence. Dans le secteur du *cloud computing* (informatique en nuage), la concurrence pourrait toutefois être limitée à l'avenir par une intégration verticale des acteurs du marché et un accès limité aux infrastructures aux différentes niveaux de la marché (IaaS, PaaS et Saas). Le droit de la concurrence est capable de répondre à de tels problèmes et une réglementation sectorielle n'est pas nécessaire. Sur ces mêmes marchés, un accès limité à des données essentielles peut également limiter la concurrence. Dans ces cas précis, une intervention réglementaire visant à garantir la portabilité des données sur les marchés du *cloud* peut s'avérer nécessaire. Dans tous les cas, une telle intervention ne devrait viser que les fournisseurs de cloud ayant une position dominante sur le marché.

La **troisième priorité** porte sur la nécessité d'une politique industrielle numérique européenne. Elle met l'accent sur la compétitivité générale de l'économie numérique européenne, qui est une condition préalable à la souveraineté numérique. Une politique industrielle numérique devrait garantir l'ouverture de l'économie, permettre des économies d'échelle, inclure une réglementation des infrastructures qui soit favorable aux investissements et promouvoir les compétences numériques des citoyens européens.

Nous proposons un cadre européen pour un *cloud computing* sécurisé et fiable, qui serait l'élément principal d'une telle politique industrielle numérique. Ce cadre répondrait aux préoccupations liées à la sécurité des données, à leur gestion et à la disponibilité des services dans le *cloud*. Ces préoccupations résultent de l'utilisation répandue d'« *hyperscalers* » non européens par les entreprises de l'UE. Elles reflètent le fait que la disponibilité des solutions de cloud pour nos économies et nos sociétés a désormais atteint le rang d'un bien public.

Le cadre proposé est proportionné, efficace et non discriminatoire. Il comprend des schémas de certification pour la classification volontaire par les fournisseurs de *cloud* sur la base de l'acte législatif de l'UE sur la cybersécurité. Nous proposons ensuite une structure de gouvernance garantissant une utilisation sécurisée des *cloud* par un nombre limité d'opérateurs de services essentiels tels que les services financiers, l'énergie ou les transports. Il est important de considérer que notre proposition vise à éviter toute distorsion de concurrence entre les fournisseurs privés de ces infrastructures essentielles.

17 recommandations pour un leadership européen en matière d'économie numérique

NEUF RECOMMANDATIONS EN FAVEUR D'UN MARCHE INTERIEUR EUROPEEN DES DONNEES

- **Recommandation n° 1 :** La Commission devrait continuer à **suivre de près** l'évolution du **marché des dépositaires de données** afin d'identifier en temps utile les obstacles éventuels à ces services soient assurés entre les États.

- **Recommandation n° 2 :** La Commission devrait profiter de la prochaine révision du **RGPD** pour assurer la **sécurité juridique par un degré d'harmonisation plus élevé.**

- **Recommandation n° 3 :** Il convient de soutenir les initiatives qui renforcent la **sécurité juridique du RGPD** par le biais de dialogues entre les autorités chargées de la protection des données et les entreprises ou les innovateurs. Elles peuvent permettre aux autorités chargées de la protection des données d'identifier plus facilement les nouveaux développements et innovations technologiques tout en garantissant dans le même temps le respect des droits des utilisateurs en matière de vie privée et de protection des données. Dans le même temps, ces initiatives, qu'elles soient appelées **« bacs à sable réglementaires » ou « centres de régulation », ne doivent pas avoir d'incidence sur le marché** (c'est-à-dire qu'elles doivent être accessibles à tous les acteurs du marché).

- **Recommandation n° 4 :** La Commission devrait, en collaboration avec les parties prenantes concernées, élaborer des **normes ouvertes pour les plates-formes et les formats de données** afin de permettre aux **organismes du secteur public** de rendre leurs données accessibles. L'élaboration de ces normes devrait s'effectuer de manière sectorielle.

- **Recommandation n° 5 :** La Commission devrait **étendre le champ d'application de la directive ISP** (directive sur les informations du secteur public) **aux entreprises privées fournissant des services d'intérêt public.** Cela garantirait que soient disponibles les données tenues par des organismes privés et qui sont en rapport avec le service d'intérêt public assuré. La Commission devrait encourager les États membres et les autorités nationales à conditionner l'accès aux marchés publics à ce que les données générées dans ce contexte soient accessibles.

- **Recommandation n° 6 :** La Commission devrait examiner la nécessité d'une **obligation générale d'accès aux données du secteur public et aux données d'intérêt public, principalement pour les informations de haute qualité**. Elle devrait notamment examiner les pratiques existantes de partage de données entre les entreprises publiques et privées dans des secteurs spécifiques – par exemple les transports, les géodonnées – afin d'évaluer si le partage de données basé sur des accords volontaires est suffisant ou si d'autres mesures sont nécessaires – soit des mesures non contraignantes, soit une législation de l'Union européenne contraignante.

- **Recommandation n° 7 : L'initiative** européenne **relative aux espaces de données** de la Commission européenne **peut réduire les coûts de transaction** du partage **des données B2B en Europe**. L'initiative mérite d'être intensifiée tant qu'elle n'a pas d'incidence sur le marché de par sa conception.

- **Recommandation n° 8 : L'introduction d'un droit de la propriété des données n'est pas pertinent**. Le contrôle de facto des données par le biais de règlements contractuels et de restrictions techniques est une base suffisante pour le développement du marché des données.

- **Recommandation n° 9 :** Comme les exigences de localisation des données entravent le développement d'un marché unique des données dans l'UE, la Commission européenne devrait de manière conséquente prendre des **mesures contre les exigences nationales de localisation des données** qui ne sont pas justifiées par le règlement général sur la protection des données et le règlement sur la libre circulation des données. Pour identifier les exigences en matière de localisation des données dans le cadre du RGPD, on devrait envisager l'introduction d'un registre des exigences nationales en matière de localisation des données.

CINQ RECOMMANDATIONS POUR MAINTENIR UNE CONCURRENCE EFFICACE SUR LES MARCHES DE L'INFORMATIQUE DEMATERIALISEE ET DU NUMERIQUE

- **Recommandation n° 10 :** Actuellement, le marché du cloud extrêmement évolutif (**marché des hyperscalers**) est caractérisé par une concurrence rude entre un nombre relativement restreint de concurrents ayant des coûts fixes élevés. Il reste à voir si le niveau actuel de concurrence sera maintenu à l'avenir. En tout état de cause, toute **intervention concurrentielle** par exemple par le biais de réglementations sur les coûts engendrés par le changement de fournisseur d'accès aux services du cloud, les exigences d'interopérabilité ou les prix pour l'utilisateur final - **ne devrait avoir lieu que dans le cas** où un fournisseur de cloud dispose **d'une puissance significative et non contestable**. En cas d'abus de ce pouvoir de marché, le droit de la concurrence est bien placé pour apporter une réponse appropriée. Une **réglementation sectorielle** visant les fournisseurs de cloud ayant une position dominante n'est actuellement **pas recommandée**.

- **Recommandation n° 11 :** La question de savoir si un **fournisseur de services PaaS** dispose d'un pouvoir de marché significatif doit être évaluée au cas par cas. En tout état de cause, l'**intervention concurrentielle ne** doit avoir lieu **qu'après l'établissement d'un pouvoir de marché non ciblé** du fournisseur de PaaS. Si une telle domination du marché est prouvée, elle peut être traitée de manière appropriée en appliquant le droit général de la concurrence. **La nécessité d'une réglementation sectorielle n'est actuellement pas univoque.**

- **Recommandation n°12 :** Les pratiques de vente liée et groupée des **fournisseurs de cloud qui s'intègrent verticalement au marché du PaaS** ne posent pas de problème, à moins que ces fournisseurs ne disposent d'un pouvoir de marché inattaquable sur les marchés de cloud. Dans ce cas, le **droit de la concurrence** est approprié pour contrer ces comportements abusifs.
  En l'absence de vente liée et groupée, le **refus** d'un fournisseur de cloud verticalement intégré de permettre aux concurrents du PaaS d'**accéder à son infrastructure cloud** peut **être contré** par la théorie des installations essentielles (« essential facilities »). Cette doctrine offre un compromis convaincant entre la protection des droits de propriété intellectuelle et la concurrence sur les marchés d'après-vente. La nécessité d'une intervention est limitée aux cas où les critères suivants sont remplis : (1) le fournisseur de cloud a une position dominante inattaquable sur le marché du cloud, (2) l'utilisation du cloud est obligatoire, (3) les fournisseurs de PaaS concurrents offrent une nouveauté et (4) le fournisseur de cloud ne peut pas fournir de raisons objectives pour refuser

l'accès. Bien qu'un régime sectoriel de réglementation de l'accès au cloud puisse également s'appliquer aux fournisseurs de cloud dominants et verticalement intégrés sur le marché du PaaS, on ne distingue pas d'avantages évidents d'une telle réglementation par rapport au **droit général de la concurrence**.

- **Recommandation n° 13 :** L'accès privilégié aux données peut entraver la concurrence. Associée à un accès privilégié aux données, **l'intégration verticale des fournisseurs d'IaaS aux marchés du PaaS et du SaaS** et la concentration du marché qui en découle, peut exacerber les problèmes de concurrence sur le marché du SaaS. L'accès privilégié aux données **peut** également **entraîner des problèmes de concurrence** sur des marchés en aval très différents.
  Avec sa doctrine des « facilités essentielles », le **droit de la concurrence** fournit une base solide pour traiter les questions de concurrence liées à l'intégration verticale. Toutefois, lorsque des données s'avèrent être des facilités essentielles, il **peut** être très **difficile et difficilement réalisable d'en autoriser l'accès** dans la pratique**.** Dans ce cas, d'autres recours ou une **intervention réglementaire** peuvent être **nécessaires** pour empêcher les données d'être ou de devenir une « facilité essentielle ». De telles interventions **devraient viser à accroître la transférabilité des données**, que ce soit en supprimant les obstacles au changement de fournisseur prévenant les situations de verrouillage ou en accordant des droits de transférabilité directe.
  Toutefois, il faut dûment tenir compte des **droits de la propriété intellectuelle.** En tout état de cause, la constatation d'une **position dominante** en l'absence de concurrence potentielle sur un marché de données en amont bien défini doit être une **condition préalable à toute intervention**. Dans les cas où les marchés sont définis de manière très étroite (par exemple par marque), la constatation d'une position dominante peut être assez simple et une réglementation peut être appropriée. Dans tous les autres cas, le droit de la concurrence peut mieux garantir une définition du marché et une analyse de la position dominante appropriées.

- **Recommandation n° 14 :** Les instruments qui garantissent au mieux la **sécurité juridique** quant à la question de savoir si la **mise en commun de données (« data pooling »)** constitue un comportement anticoncurrentiel sont :
  - les **lignes directrices** de la Commission, car elles aident les entreprises à procéder à une auto-évaluation de leur comportement sur le marché en identifiant les conditions essentielles de l'application de l'article 101 à la mise en commun des données ;
  - les **lettres d'orientation** de la Commission, parce que l'ampleur des changements dans l'analyse de la concurrence induits par les Big Data est telle que des questions totalement nouvelles sont posées. La Commission pourrait donc accepter les demandes de lettres d'orientation.

TROIS RECOMMANDATIONS POUR UNE POLITIQUE INDUSTRIELLE NUMERIQUE EUROPEENNE

- **Recommandation n° 15 :** Une **économie numérique européenne compétitive est une condition préalable à la souveraineté numérique de l'Europe.** Le travail et les investissements des entreprises et des investisseurs privés sont essentiels à cet effet. Néanmoins, l'UE, les législateurs nationaux et les décideurs politiques devraient créer le cadre juridique approprié à cela. Ce cadre devrait garantir (1) l'ouverture de l'économie et (2) la concurrence, (3) permettre des économies

d'échelle, (4) comprendre une réglementation des infrastructures favorable aux investissements et (5) promouvoir les compétences numériques.

- **Recommandation n° 16 :** L'UE devrait négocier, par l'intermédiaire de la Commission, un **accord avec les États-Unis** clarifiant les règles relatives à l'accès transfrontalier aux preuves électroniques dans le cadre des procédures pénales. Cet accord devrait non seulement protéger les citoyens et les entreprises de l'UE, mais aussi accroître la sécurité juridique concernant les demandes d'accès aux données formulées par les autorités judiciaires américaines aux prestataires de services de l'UE, ce qui permettra d'éviter les conflits en termes de normes juridiques.

- **Recommandation n° 17 :** Nous proposons un cadre européen pour un cloud computing sécurisé et fiable. Ce cadre est une réponse aux préoccupations concernant la sécurité des données, la gestion des données et la disponibilité des services dans le cloud. L'utilisation croissante des services de cloud apporte de nombreux avantages économiques, mais nous confronte en même temps à des risques politiques et opérationnels. Ceux-ci peuvent menacer la disponibilité continue de services essentiels à nos économies. Comme la disponibilité des services de cloud a atteint le caractère d'un bien public, l'intervention publique est justifiée.

  Le cadre européen proposé pour un cloud computing sécurisé et fiable, efficace et non discriminatoire. Il se compose de trois étapes.

  - **Au cours de la première étape,** l'UE devrait définir des exigences communes pour un cloud computing sécurisé et fiable qui tienne compte des préoccupations des utilisateurs en matière de sécurité et de gestion des données et en termes de disponibilité des services. Comme l'a demandé la Commission européenne, l'ENISA – Agence européenne de cyber-sécurité (NdT) - devrait concevoir des systèmes de certification de sécurité de base pour l'informatique en nuage à usage général. En outre, l'ENISA devrait concevoir des systèmes de certification de sécurité complémentaires pour l'utilisation des clouds par les administrations publiques et les secteurs fournissant des services essentiels conformément à la directive NIS.
  - Dans une **deuxième étape,** les modalités actuelles de délivrance des certificats prévues par la loi sur la cyber-sécurité peuvent être appliquées sans modification à la certification des fournisseurs de cloud. Il n'est pas nécessaire de rendre la certification obligatoire.
  - À la **troisième étape,** l'utilisation des services de cloud par les acteurs économiques dans les différents secteurs peut être subordonnée à la condition que le fournisseur de cloud respecte un certain niveau de sécurité des systèmes de certification de la sécurité du cloud. Ces exigences réglementaires doivent être fondées sur le risque et proportionnées et elles ne doivent pas fausser la concurrence ni entre les fournisseurs de cloud ni entre les entités réglementées.
  - Afin de parvenir à une application cohérente de ces exigences réglementaires, nous recommandons, à une **étape 3a,** une identification cohérente des opérateurs de services essentiels auxquels les exigences réglementaires s'appliqueront. C'est pourquoi nous proposons que le « groupe de coopération » de la directive NIS aie un rôle plus formel afin d'identifier les opérateurs des secteurs de l'énergie, des transports et des marchés financiers (mais pas les banques).
  - Après qu'il aura été confirmé à une **étape 3b** que les exigences en termes de sécurité pour les cloud pour les opérateurs de services essentiels respectent le système de certification de l'UE pour la sécurité des clouds, il sera nécessaire,

- **A une étape 3c** de garantir une application uniforme du système de certification. Dans le secteur financier, la structure de surveillance éprouvée est suffisante pour atteindre cet objectif. Pour le secteur de l'énergie et des transports, nous proposons la mise en place de nouveaux organes décisionnels au niveau des régulateurs sectoriels et des autorités de cyber-sécurité, qui seront responsables de l'application uniforme des systèmes de certification. Étant donné que les marchés de la santé, de l'eau et des infrastructures numériques sont des marchés nationaux, nous proposons que les autorités nationales soient responsables de l'application des systèmes de certification des cloud.

Bien qu'une application uniforme du système de certification de l'UE pour la sécurité des cloud dans le secteur public soit peu probable, l'application nationale du système de certification par le secteur public augmenterait l'importance du système de certification de l'UE pour la sécurité des cloud et des fournisseurs qui y adhèrent.