INSTITUT Montaigne

institutmontaigne.org
NAC2304-03

NOTE D'ACTION - Avril 2023

Flux transfrontaliers de données : les choix pour l'Europe

1. Introduction

Les flux transfrontaliers de données sont omniprésents dans notre quotidien. Pour les États-nations, le dilemme est de taille et subsistera longtemps : protéger ses propres données contre l'action d'autres acteurs étatiques (ou contre les piratages), grâce à la souveraineté et aux garanties qu'on peut en attendre, ou tirer parti de la libre circulation, en profitant des avantages concrets offerts par les échanges internationaux de données. **Ce dilemme doit être arbitré en permanence**.

La construction de régimes de données véritablement multilatéraux se heurte à un ensemble d'obstacles, liés à des enjeux de confiance, de contrôle, d'arbitrage juridique et à des différences d'ordre systémique. Cette note d'action n'écarte pas la possibilité de régimes de données multilatéraux. Mais, elle prend comme postulat l'idée selon laquelle le monde numérique a déjà, en pratique, entamé sa fragmentation. L'heure est donc à la recherche des options les moins mauvaises par rapport à ce qui pourrait être un espace numérique mondial sans faille, aux règles universellement acceptées.

2. Les termes du débat

Toutes les nations ne sont pas égales. L'arbitrage entre souveraineté des données et efficacité de leur libre circulation varie fortement en fonction du **niveau de compétence numérique d'un pays**.

- **Les États-Unis dominent le champ numérique à l'échelle mondiale**, les grandes entreprises américaines assurant au pays une souveraineté numérique de fait sur les flux transfrontaliers de données.

- **Les pays en position intermédiaire** incluent ceux qui disposent d'un marché numérique conséquent (Inde), des nations particulièrement compétentes dans ce domaine (Israël ou l'Estonie), et des nations autoritaires qui donnent la priorité absolue au contrôle des données et à leur accès par les autorités, au détriment de toute autre considération (Chine). La Chine et l'Inde font l'objet d'analyses dédiées dans cette note d'action. Le cas chinois est unique en cela qu'il combine un fort niveau de réussite numérique et une tendance généralisée au contrôle, qui va jusqu'à toucher l'ensemble des entreprises.

- **Les pays plus petits ou moins avancés** n'ont d'autre choix que d'accepter la suprématie de fournisseurs étrangers, souvent aux dépens de la souveraineté sur leurs données. Ils conservent toutefois l'option de graviter entre un cadre technologique dominé par les États-Unis et un modèle autoritaire principalement défendu par la Chine.

Dans ce contexte, l'idée d'une souveraineté numérique européenne est-elle réaliste ? L'Europe reste sous-dimensionnée en matière d'industries du numérique et un *outsider* dans la course à l'innovation et aux start-ups, mais son marché est organisé de manière plus rationnelle. L'« effet Bruxelles » lui accorde par ailleurs un certain pouvoir d'influence pour faire valoir sa vision de la protection des données personnelles au-delà de ses frontières. Il n'en demeure pas moins qu'au-delà des aspects normatifs, avoir des infrastructures numériques et une position dominante sur le marché sont des facteurs essentiels.

À cet arbitrage entre souveraineté numérique et efficacité de la libre circulation s'ajoute un autre défi : la **protection des données personnelles** contre la collecte et l'exploitation à des fins commerciales ou de surveillance étatique. Du côté de la collecte commerciale, les approches américaine et européenne diffèrent sur la notion de consentement : *notice-and-choice* d'un côté, consentement explicite de l'utilisateur de l'autre. S'agissant de surveillance, on a souvent tendance à opposer systèmes démocratiques et autoritaires. Or cette **opposition n'est ni absolue, ni simple**. Les États autoritaires sont certes peu susceptibles de protéger leurs citoyens contre des phénomènes de surveillance étatique, mais le niveau de protection des données personnelles octroyé par les systèmes démocratiques peut aussi varier considérablement.

Le fait de mettre plus ou moins l'accent sur la souveraineté est également déterminé par les **intérêts économiques des pays concernés**. Un certain nombre d'entreprises américaines tirent parti de leur statut de premier arrivé et d'un marché du capital-risque plus mature, là où l'Europe subit les effets d'une industrie plus dispersée, de la difficulté pour ses nouveaux entrants à atteindre les mêmes économies d'échelles que leurs concurrents bien installés, et de politiques publiques d'innovation moins efficaces. La réaction logique voudrait que l'Europe cherche à créer un « cocon industriel » permettant de faire prospérer son écosystème local. C'est plus facile à dire qu'à faire.

Les politiques publiques ciblant les flux transfrontaliers de données doivent donc composer avec deux dilemmes fondamentaux : le premier porte sur le **triangle entre objectifs d'efficacité, de protection des données personnelles et de sécurité** ; le second est à la fois **géopolitique et géoéconomique, les États-Unis, l'Union européenne et la Chine** cherchant à contrôler leurs propres données tout en accédant à celles des autres. Ces dilemmes ne peuvent être complètement résolus : ils peuvent seulement faire l'objet d'arbitrages dans l'une ou l'autre direction.

3. Réguler les flux transfrontaliers de données

La régulation des flux de données (y compris transfrontaliers) ne signifie pas pour autant contraindre ces flux ou les empêcher. Au contraire, cette régulation est une condition de leur développement car elle garantit le respect de plusieurs objectifs : protection des données et confiance pour les individus et les entreprises, respect d'impératifs de nature publique comme la sécurité nationale ou l'ordre public, prévention de la criminalité, et libre concurrence.

Le défi réside dans l'**arbitrage entre des systèmes juridiques différents, et dans la capacité effective de l'application de règles communes**. Afin d'y répondre, divers accords internationaux ont émergé au fil du temps : recommandations non contraignantes de l'OCDE, Convention 108 du

Conseil de l'Europe – elle, juridiquement contraignante –, et des initiatives régionales comme celles de l'*Asia-Pacific Economic Cooperation* (APEC) et de l'ASEAN. Plus importante encore est l'**adoption du Règlement général sur la protection des données (RGPD) de l'Union européenne**, qui inclut des dispositions sur les transferts de données hors de l'UE, comme des décisions d'adéquation, des clauses contractuelles standards et des règles contraignantes pour le secteur privé, ainsi qu'une liste de dérogations.

Au-delà de ces initiatives, qui sont celles qui se rapprochent le plus d'accords multilatéraux, **une approche entièrement multilatérale reste à ce stade hors de portée**. Les tentatives existent, avec des propositions portées par l'ONU, l'OMC ou la Banque mondiale. De plus en plus, les accords de libre-échange conclus récemment incluent aussi des clauses, souvent contraignantes, qui couvrent la question des transferts numériques. Le Chili, la Nouvelle-Zélande et Singapour ont également initié un accord de partenariat sur l'économie numérique **(*Digital Economy Partnership Agreement*, DEPA)** ; s'il n'est pas contraignant, cet accord semble susciter l'intérêt d'autres pays.

L'autre élan en faveur d'une meilleure réglementation se déroule au niveau du G7 et du G20. Il est en grande partie poussé par le gouvernement japonais. A travers son **initiative *Data Free Flow with Trust* (DFFT)**, le Japon cherche à combler le fossé entre un régime universel idéaliste qui permettrait un monde numérique sans faille, et le constat pragmatique selon lequel un régime plurilatéral est la seule option pour avancer à court terme.

En contrepoint, les États-Unis privilégient des **accords bilatéraux** sur les transferts de données et pourraient devenir le centre de gravité d'un modèle « en étoile », adossé à des mécanismes leur octroyant des accès directs à ces espaces numériques nationaux.

4. Souveraineté numérique

La croissance exponentielle de la révolution numérique a profité aux États-Unis et à la Chine, avec une domination respective du software et du hardware. L'Europe est peut-être à l'avant-garde pour influencer la régulation du numérique, mais **« les arbitres ne remportent pas les matchs »**. Le marché européen des données reste plus petit en taille relative par habitant, en comparaison des marchés américain ou japonais. La Commission européenne, à la suite de certains États membres, cherche à combler cet écart en visant une souveraineté numérique. Après tout, **qui ne voudrait pas « reprendre le contrôle » ?**

Il convient en conséquence de clarifier ce qu'on entend par souveraineté lorsque la notion est appliquée au numérique. Alors que le terme a longtemps été tabou dans l'Union européenne, les déclarations y faisant référence abondent à présent, tant au niveau de la Commission que des États membres. Les Européens voient surtout la **souveraineté comme un outil au service de leur autonomie** sans aller jusqu'à sacrifier l'interdépendance ou la libre circulation des données, et donc sans adopter un projet d'autosuffisance et de fermeture à l'image de la « Grande Muraille » chinoise. L'indépendance est une voie certes louable, mais irréaliste. De plus, l'approche européenne de la souveraineté numérique se limite principalement à des options défensives, contrairement à l'approche américaine qui dispose à la fois de **caractéristiques défensives et offensives**.

De nombreux politiques se sont emparés du discours sur la souveraineté, mais ce avec des ambitions diverses. En Europe, cette rhétorique a migré de l'échelon national à l'échelon européen, car aucun État membre, pris individuellement, ne saurait présenter un niveau d'investissement, d'innovation ou de taille de marché suffisant. **Mutualiser les forces et les moyens au niveau européen** est donc, dans de nombreux cas, inévitable au nom de l'efficacité. Mais la force même de l'engagement de l'Europe en faveur de valeurs comme la protection

des données personnelles ou des droits individuels a une autre conséquence : elle crée des **obstacles juridiques qui freinent ou gênent l'innovation de rupture et le passage des start-ups à une économie d'échelle. Et notre propre réticence à partager nos données**, sur le fondement du principe de précaution, constitue un autre problème à traiter.

Nous devons aujourd'hui prendre clairement conscience des handicaps que crée notre appétit de réglementation. Il en découle un nombre trop limité de champions numériques européens, la dépendance actuelle de l'UE aux technologies et fournisseurs de logiciels non-européens, auxquels s'ajoute la dispersion des acteurs privés. Les décideurs publics doivent continuer d'encourager une mobilisation « *bottom-up* » des ressources. Un **changement global des mentalités au niveau européen** doit plus largement s'opérer pour donner la priorité à des avancées fondées sur la science et la technologie plutôt qu'à une approche défensive mue par la méfiance et par une tendance récurrente à faire primer le principe de précaution.

5. Clouds et infrastructures

On serait tenté de croire que les câbles et nœuds sous-marins sont en haut de la liste lorsqu'il s'agit de protection des données. Ils sont l'objet d'une compétition sino-américaine silencieuse, avec un rapport de force penchant progressivement en faveur des entreprises américaines. Les **dépendances d'approvisionnement en matériels informatiques créent aussi des risques d'exfiltration de données ou de sabotage à distance**.

Mais ces risques bien réels sont moins sur le devant de la scène que les débats relatifs aux opérateurs de services cloud et à leurs composants, qu'il s'agisse de serveurs ou de logiciels. Les clouds peuvent être localisés dans un autre pays, ou des fournisseurs, applications et opérateurs étrangers peuvent être régis par des juridictions différentes. Il est alors **plus difficile pour les utilisateurs de garder le contrôle sur leurs données et leurs possibles utilisations**.

La domination des fournisseurs américains de cloud en Europe a engendré des discussions sur le degré d'auto-suffisance et d'indépendance à l'égard des fournisseurs étrangers, tant à l'échelle des États membres qu'au niveau européen. Beaucoup de voix ont initialement posé le débat comme relevant en premier lieu de l'enjeu de la localisation des clouds – comme si avoir un cloud sur « son » propre territoire garantissait une sécurité cyber et juridique. Mais les clouds ne sont plus seulement des conteneurs de données, ou des infrastructures physiques qui ressembleraient à des coffres-forts. Le traitement des données dans les clouds a largement pris le pas sur cet aspect physique.

Les tentatives françaises et allemandes visant à mettre en place des clouds souverains n'ont pas été sans remous. Si la création de clouds privés destinés à des usages gouvernementaux limités est envisageable, trouver des solutions commercialement viables sans les grands fournisseurs de services établis sur ce marché reste une tâche ardue. Il semble à ce jour **impossible de construire un cloud compétitif sans s'appuyer sur des technologies américaines**.

Des doutes persistent quant à l'étendue extraterritoriale du *CLOUD Act* américain et d'autres types de législations. La France a de nouveau entrepris de créer des clouds avec des degrés variables d'ambitions en matière de souveraineté, et défend l'introduction de mécanismes de certification au niveau national et européen. Pourtant, les **débats persistent sur la réalité de l'immunité face aux lois extraterritoriales**, car toutes les entreprises s'appuient dans une certaine mesure sur des fournisseurs américains de technologie, voire chinois. Ce débat trouve son écho au niveau européen, où la présence d'industriels non-européens parmi les membres de Gaia-X a fait l'objet de controverses.

La trajectoire vers l'émergence de clouds européens importe d'un point de vue sécuritaire et économique, mais elle doit être progressive et suivre un schéma prévisible. À court terme, **une politique de concurrence qui assurerait plus d'égalité entre acteurs arrivés en premier et nouveaux entrants est une priorité, pour limiter les effets de rente**. À moyen et long termes, pour plus de résultats, cette politique devra s'accompagner d'une politique d'achats publics qu'il conviendra de définir judicieusement.

6. Garder l'espace numérique transatlantique ouvert

L'**élaboration de règles dans l'espace numérique international passe par le choix des parties avec lesquelles on souhaite s'entendre – et par la définition du point jusqu'où peut aller cette entente**. Défendre des positions radicales en matière de flux de données et exiger non pas tant une adéquation que des règles et normes identiques reviendrait à empêcher ces flux. En particulier, garder l'espace numérique transatlantique ouvert, et en faire un exemple international, ne pourra se faire sans des concessions de part et d'autre.

L'Europe a de bonnes raisons de viser l'innovation et la résilience des chaînes d'approvisionnement dans le domaine du numérique. Cela ne doit toutefois pas se faire au détriment de l'efficacité, des économies d'échelle et du coût. Même dans les espaces numériques les plus restrictifs et les plus sensibles, il sera extrêmement difficile de ne pas s'appuyer sur des fournisseurs non-européens, d'autant que les alternatives locales sont souvent à l'état de projet.

L'UE doit ainsi trouver un terrain d'entente avec les États-Unis. Cela implique de restreindre, des deux côtés, les subventions encourageant la localisation, d'accepter des solutions mixtes, et de mener une politique de concurrence forte en Europe (et aux États-Unis). **Il s'agit d'un enjeu d'ordre concurrentiel, financier et d'innovation, non pas d'une division stratégique ou géopolitique**. Par contraste, une fragmentation à des fins d'autosuffisance isolerait l'Europe, l'éloignerait considérablement de marchés tiers, et instaurerait un climat propice à des querelles politiques inutiles.

7. Conclusion et recommandations

L'Europe fait face à la fois à une menace et à un défi. La menace provient clairement de la Chine, et découle du fait que la Chine combine une présence numérique avancée et un manque total de transparence et de responsabilité juridique dans sa propre gestion des données. Le défi est celui de l'avance prise par les États-Unis grâce à son statut de premier arrivé sur le marché, de plus grand pourvoyeur de R&D et de capacité d'investissement, et d'acteurs ayant une aptitude remarquable à créer des synergies entre acteurs publics et privés. En gardant à l'esprit ce double environnement, cette note d'action formule une série de recommandations pour l'Europe :

1. Se projeter vers un **espace européen commun des données plus efficace** est une première étape essentielle, qui ne pourra être atteinte qu'à travers une **hiérarchisation réaliste des priorités**. L'UE n'étant pas compétente en matière d'enjeux et de données de sécurité nationale, elle devrait se fixer comme horizon de court terme la couche suivante de données critiques pour les solutions cloud européennes, tout en mettant à profit sa politique de concurrence pour garantir des conditions équitables entre concurrents dans le cloud public.

2. L'UE doit **augmenter ses moyens financiers publics et privés au-delà du soutien traditionnel qu'apporte la Commission aux mécanismes d'innovation** afin de créer davantage de synergies avec le monde industriel.

3. Il convient pour l'UE d'également **adopter une approche plus pragmatique et plus inclusive dans l'élaboration de ses politiques de financement et de l'emploi** pour attirer les start-ups et les centres de recherche, les entreprises et les talents étrangers.

4. **La force du marché commun et la capacité européenne à réguler sont de grands atouts pour renforcer la sécurité des données**, sans pour autant viser une autosuffisance radicale, ou « à la chinoise ».

5. L'UE doit **limiter les contraintes réglementaires et éviter de promulguer des règles trop vastes ou trop englobantes**, qui présentent le risque d'être trop lourdes voire irréalistes, afin d'éviter que des standards moins ambitieux à l'image du DEPA ne l'emportent en dehors de l'Europe.

6. Sur la démocratie, les valeurs et les règles locales, aucune convergence complète n'existe entre les différents systèmes. Malgré les difficultés rencontrées ces dernières années, un **compromis sur un accord transfrontalier transatlantique renouvelé** est donc nécessaire d'un point de vue stratégique.

7. Sur la localisation des données, il est essentiel de distinguer cybersécurité et sécurité juridique. **En se concentrant sur sa capacité à mettre en œuvre et appliquer des sanctions, y compris via le levier extraterritorial des données**, l'Europe pourrait plus aisément exiger d'être consultée et d'obtenir des décisions conjointes avec les États-Unis.

8. Bien qu'il n'existe pas de garantie absolue en matière de confidentialité et d'intégrité des données, **le principe de minimisation et certaines limites à imposer pour la conservation des données et le stockage en périphérie, peuvent réduire les risques, ainsi que l'empreinte carbone du secteur numérique**.

9. La responsabilité juridique des intervenants doit être renforcée. Aux États-Unis, elle reste actuellement limitée, avec des pénalités pré-définies qui demeurent minimes lorsqu'il s'agit de sanctionner l'insuffisance de mesures pour prévenir les fuites de sécurité. Ceci réduit l'incitation pour les fournisseurs informatiques (hardware, software, plateformes, CSOs) à investir dans la cybersécurité. **Une plus grande responsabilisation des fournisseurs permettrait aussi de réduire l'écart transatlantique sur l'utilisation des données**.

10. Nous devons enfin regarder au-delà de la relation transatlantique et trouver les formats internationaux les plus appropriés. Les propositions de la présidence japonaise dans le cadre du G7, qui cherchent à être **inclusives sans s'obstiner à viser l'universalité et un multilatéralisme improbable**, constituent une voie prometteuse pour la coordination des efforts internationaux.