Cas d'utilisation sur le Mode de fonctionnement du réseau Internet

Localisation des données

Septembre 2020

Quels sont les effets de la localisation forcée des données sur le mode de fonctionnement du réseau Internet ?

Ce cas d'utilisation analyse l'effet que des politiques gouvernementales relatives à la localisation des données sont susceptibles d'avoir sur le mode de fonctionnement du réseau Internet. Pour comprendre comment de telles politiques pourraient nuire à l'ensemble des avantages qu'offre Internet, notamment en termes d'innovation et de croissance économique, nous les analysons à travers le prisme des propriétés essentielles d'Internet.

Qu'est-ce que la localisation forcée des données ?

Le terme « localisation forcée des données » fait référence aux exigences gouvernementales relatives au contrôle du stockage et des flux de données, et visant à conserver celles-ci au sein d'une juridiction spécifique. Les lois sur la localisation des données, parfois appelées « résidence des données » ou « souveraineté sur les données », visent généralement à conserver les données personnelles ou les données sur des transactions financières au sein d'un pays, où elles sont soumises à la réglementation locale et peuvent être consultées. Les mesures de localisation forcée des données vont d'une simple obligation de conserver physiquement les données dans leur pays d'origine à une restriction, ou même une interdiction, de les transférer vers d'autres pays. Que signifie la localisation forcée des données pour les propriétés essentielles d'Internet, et que pourrait-il se passer si d'autres pays imposaient des restrictions en ce sens ?

Tendances actuelles

Ces dernières années, l'Inde, l'Indonésie et le Vietnam ont adopté ou envisagé d'adopter des lois exigeant que les données personnelles ou commerciales soient conservées au sein des frontières nationales et ne soient pas traitées dans d'autres pays.[1] Même si la Loi sur la protection des données personnelles de 2019 en Inde a fini par abandonner les mesures visant à conserver l'intégralité du traitement des données sur le territoire indien, elle oblige toujours à localiser un ensemble non défini de « données personnelles critiques ».
L'Indonésie dispose de mesures sur l'obligation de localiser des données depuis 2012, même si celles-ci ont été quelque peu assouplies en 2019. La Loi sur la cybersécurité de 2019 au Vietnam exigeait à l'origine que toutes les sociétés de service sur Internet non établies au Vietnam et traitant des données personnelles vietnamiennes

1 https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/ et https://www.fticonsulting-asia.com/~/media/Files/apac-files/insights/articles/localization-to-fragment-data-flows-asia.pdf

créent une présence physique dans le pays, mais cette exigence est devenue plus spécifique dans la législation ultérieure.

Mais, si certains pays ont envisagé (avant de se rétracter partiellement) de contraindre les entreprises à conserver les données personnelles et commerciales au sein de leurs frontières[2], il n'en reste pas moins vrai que, « au cours des dernières années, plus de soixante-dix pays ont adopté de nouvelles lois ou modifié des lois existantes sur la confidentialité comprenant une forme de localisation des données ».[3]

De récentes lois en Russie et en Chine interdisent aux entreprises d'envoyer les données personnelles des citoyens en dehors de ces pays. Une loi russe de 2019 impose des amendes aux entreprises et aux employés ne se conformant pas à la loi nationale de 2015 relative à la localisation des données (ce qui a donné lieu au blocage du site Internet LinkedIn en Russie). La loi chinoise de 2017 sur la cybersécurité exige que les opérateurs d'infrastructures essentielles et de réseaux conservent les « données importantes », à la fois personnelles et commerciales, en Chine, ou se soumettent à une « évaluation de sécurité » rigoureuse et très exhaustive pour demander le droit d'exporter ces données. Ces lois ont entraîné une augmentation des charges et des risques pour les entreprises, ce qui a réduit la disponibilité de services à valeur ajoutée. De nombreuses entreprises ont purement et simplement abandonné ces marchés.

Les mesures de localisation des données se concentrent généralement sur les données personnelles et commerciales et visent donc principalement les entreprises qui traitent des données de ce type, comme les entreprises s'adressant directement aux consommateurs, les banques et les plateformes technologiques gérant majoritairement des données de tiers.

Les politiques actuelles ciblent également les données « au repos », celles qui ne sont pas en cours de transit d'un appareil à un autre ou d'un réseau à un autre, telles que les données conservées sur un disque dur, un ordinateur portable, ou archivées/stockées d'autres façons. Elles ne ciblent donc pas les services d'infrastructure d'Internet qui transportent ces données sans en connaître le contenu. Les lois actuelles, si elles représentent différents extrêmes, ont toutes tendance à confiner les données de ce type au sein des frontières nationales, en reflet de réalités géopolitiques plus vastes. Tandis que des États adoptent des approches plus nationalistes et basées sur la souveraineté qui remettent en question la mondialisation et la coopération internationales[4], la localisation des données devient un outil puissant qui permet aux acteurs étatiques de créer des « frontières numériques » sur Internet.[5] Cette tendance comprend par exemple GAIA-X, le récent projet d'architecture fédérée pour le cloud européen qui se concentre sur la notion de « souveraineté des données »[6]. De plus, Brunéi, la Chine, l'Indonésie, le Nigéria et la Russie disposent tous de législations strictes sur la localisation des données, qui exigent notamment le stockage sur des serveurs situés dans ces pays.[7]

Mais il existe déjà des exemples de pays qui imposent des mesures encore plus radicales sur la localisation des données, notamment pour les données « en transit ». Par exemple, la Russie et la Chine prévoient d'adopter des mesures visant à centraliser, contrôler et restreindre les services d'infrastructure d'Internet, ce qui entraînerait une fragmentation d'Internet à tous les niveaux (réf. à la loi « Souveraineté sur Internet » russe et à l'article 29 du « Projet de mesure pour la gestion de la sécurité des données » chinois de 2020).

Si une telle tendance à la localisation des données se poursuivait, elle augmenterait les goulots d'étranglement et amoindrirait la résilience d'un réseau réaménagé pour correspondre aux frontières nationales et aux performances non optimales. Les entreprises devraient réduire leurs choix et leurs capacités, et les opérateurs de réseaux pourraient être contraints de recourir à des modes de routage onéreux et moins résilients. La cybersécurité pourrait en pâtir, car les organisations seraient moins en mesure de conserver des données hors

2 https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/

3 https://foreignpolicy.com/2020/05/13/data-governance-privacy-internet-regulation-localization-global-technology-power-map/

4 https://www.theatlantic.com/ideas/archive/2020/03/dont-abandon-globalizationmake-it-better/608872/

5 https://www.centerforfinancialinclusion.org/data-globalization-vs-data-localization

6 https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/das-projekt-gaia-x-executive-summary.pdf?__blob=publicationFile&v=6

7 https://bigbang360.com/data-localization-laws/

des frontières afin d'améliorer la fiabilité et d'atténuer une grande variété de risques, notamment en cas de cyberattaques et de catastrophes naturelles.

Les pays cherchant à contraindre la localisation des données nuiront à l'ouverture et à l'accessibilité de l'Internet mondial. Les données ne pourront plus circuler sans interruption en se basant sur l'efficacité du réseau, car des dispositifs spéciaux devront être mis en œuvre pour que les données restent confinées à une juridiction. Il en résultera une augmentation des barrières d'entrée, au détriment des utilisateurs, des entreprises et des gouvernements cherchant à accéder à Internet. Pour finir, la localisation forcée des données fera qu'Internet perdra en résilience, en utilité et en internationalité, et deviendra plus onéreux.

Quelles propriétés essentielles sont impactées par la localisation forcée des données ?

Propriété essentielle n° 1 : une infrastructure ouverte et accessible dotée d'un protocole commun

La seule condition nécessaire pour qu'un réseau ou qu'un nœud puisse accéder à Internet est que celui-ci adopte ses protocoles communs, et au minimum le protocole Internet (IP). Ce modèle « sans autorisation » de plus petite barrière technique possible à l'entrée est la base du développement rapide et de la portée mondiale d'Internet. Il ne nécessite pas que les opérateurs de réseaux suivent les frontières nationales pour échanger du trafic entre les réseaux.

L'un des effets négatifs des politiques sur la localisation des données est le niveau important de barrières d'entrée pour de nouveaux prestataires de services, ce qui nuira à la connectivité mondiale et à la croissance. Dans un contexte de localisation forcée des données, un prestataire de service, comme un portail Web, ne devrait pas seulement mettre en place un serveur Web (ou l'héberger dans un réseau de diffusion de contenu) pour assurer les services de base, mais également disposer d'infrastructures de stockage distinctes dans les pays concernés par une législation sur la localisation des données.

Les lois sur la localisation des données, telles que celles envisagées en Inde ou au Vietnam, ciblent généralement le traitement et l'utilisation de certaines catégories d'informations personnelles et commerciales par la couche applicative d'Internet, par exemple une application d'informatique en nuage. Elles ne ciblent pas directement les fournisseurs d'infrastructure d'Internet en exigeant que le trafic qui y transite respecte les frontières nationales. Cependant, nous pouvons observer les conséquences indésirables de ces lois, en particulier en termes d'augmentation des frais de gestion des services associés. Les politiques sur la localisation des données exigent que les fournisseurs de services créent des infrastructures supplémentaires pour l'hébergement, ce qui implique qu'ils ont besoin d'une infrastructure fiable pour la conservation physique des données au sein du pays. Tous les pays n'étant pas en mesure d'assurer une infrastructure de ce type, ou ne disposant pas nécessairement des équipements nécessaires, les prestataires de services pourraient être sujets à des frais supplémentaires et à de potentielles vulnérabilités des infrastructures, et ils pourraient également décider de ne pas offrir leurs services dans certains pays.

Propriété essentielle n° 3 : une gestion décentralisée et un système unique de routage distribué

Internet est un « réseau de réseaux » composé de près de 70 000 réseaux indépendants qui utilisent les mêmes protocoles techniques et décident de collaborer et de se connecter entre eux. Chaque réseau prend des décisions indépendantes sur la façon de faire le routage du trafic vers ses voisins, en fonction de ses propres besoins, de son modèle commercial et des exigences locales. Il n'existe pas de contrôle ou de coordination centralisés.

L'une des conséquences négatives de la localisation des données est le fait que la conservation des données n'est pas optimale, à la fois en termes de résilience et de connectivité. L'emplacement le plus proche sur le plan topologique (et donc le plus rapide d'accès) n'est pas nécessairement situé dans le même pays. Les données sont conservées à l'endroit le plus logique, et cela tient davantage compte d'aspects évolutifs liés à l'efficacité et à la fiabilité des performances que de l'emplacement géographique. Même si les données sont situées dans un même pays, le trajet de transmission peut traverser les frontières nationales afin d'améliorer la résilience ou les

performances. Les mesures de localisation des données peuvent contraindre les données sur Internet, de manière directe ou indirecte, à respecter les frontières nationales au détriment de l'efficacité.

Certaines politiques vont même encore plus loin, et s'intéressent également aux données en transit. Même si la localisation des données regroupe de nombreuses approches, l'une des manières de l'appliquer est d'exiger des intermédiaires d'Internet qu'ils imposent des impératifs supplémentaires aux politiques de routage. Ainsi, l'article 29 du Projet de mesure pour la gestion de la sécurité des données chinois de 2020 stipule que, lorsque des utilisateurs situés en Chine accèdent à des sites Internet locaux, leur trafic ne doit pas être envoyé vers des serveurs hors de Chine.[8] Des politiques de ce type pourraient avoir un impact sur la façon dont les informations sont transmises entre les réseaux, ce qui pourrait à terme nuire au travail accompli pour réduire la latence, garantir la redondance et la duplication pour assurer une distribution le plus près possible de la destination, et répondre à d'autres objectifs de base pour l'ingénierie et l'optimisation du trafic. Cela réduirait l'autonomie des opérateurs de réseaux en matière de routage, ainsi que leur capacité à optimiser la connectivité. Dans l'ensemble, le fait de conformer la politique de routage aux exigences de différentes juridictions entraînerait une complexité et une inefficacité superflues, car le routage n'obéirait plus simplement aux exigences de connectivité, de résilience et d'optimisation des flux.

Si la tendance actuelle venait à se poursuivre, la localisation forcée des données nuirait à l'autonomie et à l'agilité du routage distribué d'Internet, ce qui réduirait la capacité à interagir avec d'autres réseaux, et finirait par restreindre la portée mondiale d'Internet.

Propriété essentielle n° 5 : un réseau technologiquement neutre et à usage général

Internet est « un réseau technologiquement neutre et à usage général », car les utilisations que permet son infrastructure n'ont pas de limite définie. Un réseau à usage général nécessite que les opérateurs des services de réseaux effectuent uniquement des fonctions très basiques : la transmission des paquets de données vers leur prochaine destination, sans tenir compte de leur contenu.

La localisation forcée des données exigerait de limiter les services pouvant être proposés dans certains pays si ces services impliquaient l'envoi de données personnelles ou commerciales à l'étranger. Bien que les lois actuelles présentent peu de risque d'exiger immédiatement des changements directs pour les prestataires de réseaux, ces exigences pourraient créer un filtre au fil du temps. Des législations plus strictes en matière de localisation des données pourraient nécessiter davantage de coordination entre les entreprises et les gouvernements afin de déterminer les données que les réseaux transportent, ainsi qu'entre les réseaux pour s'assurer que des flux de données spécifiques ne franchissent pas les frontières nationales. Toute exigence supplémentaire reposant sur la compréhension par tous les opérateurs de la nature des données/contenus rendrait le réseau plus spécialisé, avec un usage moins général, ce qui nécessiterait des fonctionnalités supplémentaires comme l'inspection du trafic et définirait de façon plus stricte le fonctionnement des réseaux dans leur ensemble.

La réduction de la simplicité et du caractère basique du fonctionnement au niveau des couches de transit d'Internet qu'entraîneraient les mesures de localisation des données rendrait les réseaux plus complexes et moins efficaces, et exacerberait le besoin de coordination. Cela nuirait au modèle d'innovation sans permission d'Internet et créerait des barrières d'entrée pour les nouveaux opérateurs de réseaux et fournisseurs d'infrastructure d'Internet.

Conclusion

Si certains pays d'Asie du Sud ont récemment reculé au sujet de l'imposition de législations strictes sur la localisation des données, dans d'autres régions, notamment en Union européenne, de nouvelles mesures visant à soutenir la « souveraineté sur les données » sont actuellement envisagées.[9] Si cette tendance à la localisation des

8 Texte de loi d'origine : http://www.moj.gov.cn/news/content/2019-05/28/zlk_235861.html ; traduction non officielle, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-draft-data-security-management-measures/

9 https://www.bmwi.de/Redaktion/EN/Dossier/gaia-x.html

données venait à se poursuivre, cela restreindrait les services qui peuvent être proposés à des internautes de différents pays (comme l'informatique dans le nuage), ce qui, à son tour, transformerait l'Internet tel que nous le connaissons aujourd'hui en un réseau plus étroitement national. Les mesures pour la localisation des données conçues pour modifier les pratiques des entreprises risquent également de façonner et de restreindre le flux sans entraves du trafic au sein des infrastructures d'Internet. L'impact des lois sur la localisation forcée des données finira par toucher l'infrastructure d'Internet et par nuire aux propriétés essentielles du mode de fonctionnement du réseau Internet.

Cet effet probable sur ses propriétés essentielles réduira l'intérêt d'Internet pour les utilisateurs du monde entier, car celui-ci ne sera plus un réseau « de bout en bout » offrant à tous les individus, où qu'ils se trouvent, la plus grande diversité d'opportunités possible.