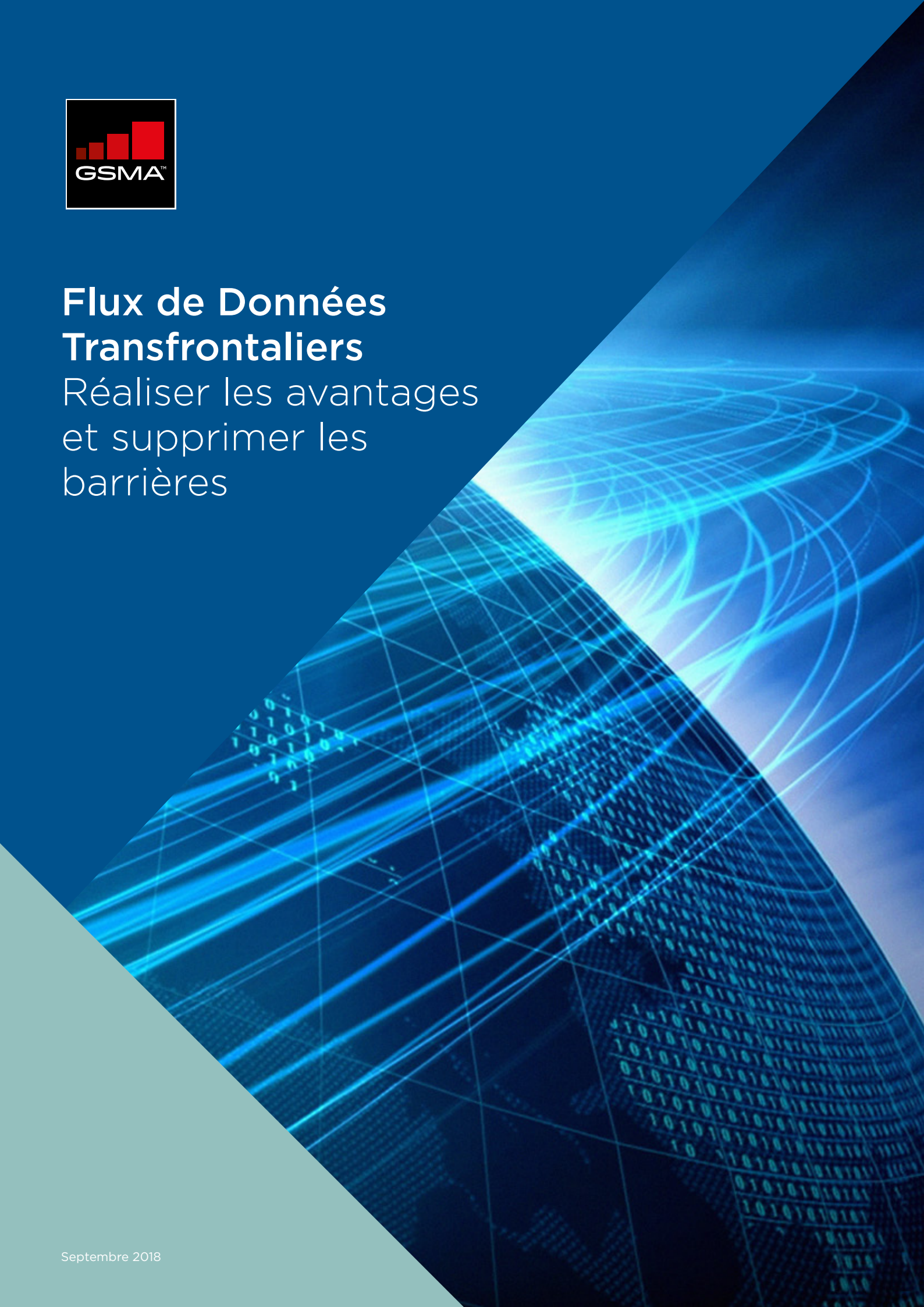
Flux de Données Transfrontaliers

Réaliser les avantages et supprimer les barrières



Septembre 2018

La GSMA, qui représente les intérêts des opérateurs de téléphonie mobile dans le monde entier, rassemble plus de 750 opérateurs et plus de 350 entreprises de l'écosystème mobile au sens large (fabricants de téléphones et appareils mobiles, éditeurs de logiciels, fournisseurs d'équipements, prestataires Internet et organismes issus de secteurs liés). La GSMA organise également des événements de premier plan dans le secteur, tels que le Mobile World Congress, le Mobile World Congress Shanghaï, le Mobile World Congress Americas et la série de conférences Mobile 360.

Pour de plus amples informations, rendez-vous sur le site Web de la GSMA : www.gsma.com et le site dédié aux politiques publiques sur www.gsma.com/publicpolicy

Pour consulter les ressources en ligne de la GSMA relatives aux flux de données transfrontaliers, visitez www.gsma.com/CrossBorderDataFlows

Suivez la GSMA sur Twitter : @GSMA et @GSMAPolicy

Auteurs

La GSMA a mandaté Wickham Heath Consulting pour conduire cette étude et les les recherches correspondantes et rédiger ce rapport. Wickham Heath Consulting Limited est un bureau de consultants basé au Royaume-Uni qui s'occupe avant tout de la règlementation de nouveaux produits de communication et de produits sur Internet.

SOMMAIRE

Résumé

Aujourd'hui, le commerce repose principalement sur la capacité des organisations à faire circuler des données, y compris des données personnelles des consommateurs, au-delà des frontières et sans restriction. Cette possibilité génère des résultats positifs non seulement pour les organisations mais également pour les particuliers et les Etats.

Toute organisation, aussi petite soit-elle, peut utiliser Internet pour commercialiser et livrer ses idées, produits et services, partout où les données peuvent être distribuées. Les transferts de données transfrontaliers permettent un accès plus ou moins immédiat aux biens et aux services et la commande de produits physiques pour qu'ils soient (ensuite) livrés, indépendamment de l'endroit où ces articles sont produits. Les organisations répondent à la demande des consommateurs en s'agrandissant pour couvrir des marchés géographiques plus grands et en augmentant le choix à la disposition des consommateurs. En parallèle, les entreprises opérant dans plusieurs pays sont plus efficaces en centralisant et en dématérialisant l'analyse, le traitement et le stockage de leurs données.

Certains pays ont introduit des restrictions sur les flux de données transfrontaliers, en raison de questions de sécurité nationale, de confidentialité des données ou de la volonté de protéger les marchés intérieurs. Ces restrictions prennent différentes formes, comme le fait d'obtenir l'accord explicite des particuliers ou une autorisation préalable des autorités de protection des données. Les règles les plus restrictives interdisent aux organisations tout transfert de données ou de métadonnées personnelles.

Les effets de telles restrictions sont nombreux. Par exemple, le fait de demander aux organisations de conserver une copie supplémentaire des données générées par leurs activités dans un pays augmente les coûts de production des biens physiques et numériques sur ce marché. Les coûts augmentent encore lorsque l'analyse et le traitement des données doivent se faire localement, de même que le stockage.

Comme les autres entreprises internationales, les opérateurs de télécoms veulent profiter des gains de la centralisation et de la virtualisation. Cependant, les métadonnées qu'ils génèrent en rapport avec les communications des particuliers sont souvent soumises à des règlementations sectorielles ou à des obligations du cahier des charges qui interdisent la circulation des métadonnées hors du pays et imposent leur collecte et leur stockage qui datent d'avant le numérique. De telles restrictions spécifiques aux télécoms défavorisent les opérateurs de télécommunications par rapport aux fournisseurs de services de communications qui ne sont pas soumis à ces réglementations comme les plateformes Internet.

En réponse à l'importance croissante des mesures de localisation des données dans le monde, ce rapport présente plusieurs recommandations aux gouvernements afin de permettre de bénéficier des avantages des flux de données transfrontaliers pour les particuliers, les organisations, les gouvernements et l'économie, tout en assurant que des règles suffisantes de confidentialité des données soient mises en place pour protéger les citoyens et conserver leur confiance dans l'écosystème numérique.

Recommandation 1 :	S'engager à faciliter les flux de données transfrontaliers et à supprimer les mesures de localisation inutiles
Recommandation 2 :	Assurer que le cadre de protection des données soit adapté à l'âge numérique
Recommandation 3 :	Passer en revue les règles sectorielles de confidentialité traditionnelles
Recommandation 4 :	Encourager les initiatives régionales de protection des données
Recommandation 5 :	Eviter la localisation en répondant de manière pragmatique aux questions de surveillance étrangère
Recommandation 6 :	Eviter la localisation en répondant de manière pragmatique aux questions de sécurité nationale et conformité aux lois nationales

Introduction : Comprendre les avantages de la libre circulation des données

Aujourd'hui les données sont d'une importance fondamentale pour le commerce physique et numérique et elles servent de catalyseur vital pour l'innovation. Le développement de l'économie numérique et la croissance continue de la productivité des industries traditionnelles dépendent de la capacité des organisations à transférer des données. En tenant compte des données personnelles des consommateurs, au sein et entre les Etats pour une analyse, un traitement et un stockage efficaces. La liberté de circulation des données personnelles sans restrictions entre les pays ne génère pas uniquement des résultats positifs pour les organisations, mais également pour les individus et les Etats.

Avantages pour les particuliers

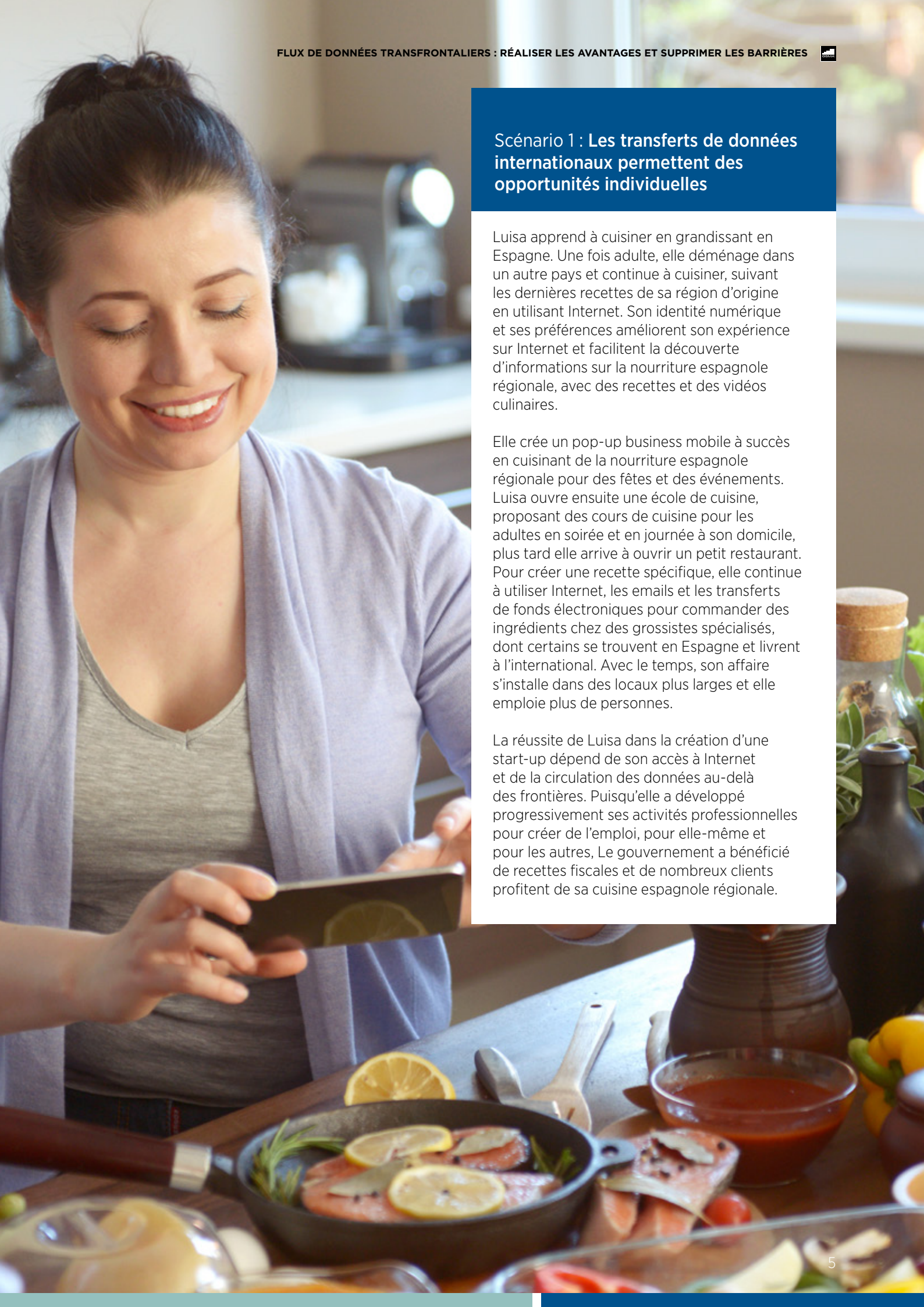
Pour les particuliers, l'accès à Internet offre le moyen d'interagir avec des personnes et des organisations partout dans le monde – que ce soit à l'échelle locale, nationale, dans un pays voisin ou sur un autre continent.

Les flux de données internationaux permettent d'accéder à une large gamme de produits et de services disponibles en ligne. L'accès aux biens et aux services numériques est plus ou moins instantané et les produits physiques peuvent être commandés en livraison, indépendamment de l'endroit où ils sont produits.

Les organisations répondent à la demande des consommateurs en s'agrandissant pour couvrir plus de marchés géographiques, augmentant le choix des consommateurs en produits et services. Globalement, ce développement de la commercialisation numérique et physique renforce le choix et la satisfaction des clients. La libre circulation des données au-delà des frontières permet aux organisations d'utiliser une même infrastructure pour plusieurs marchés, ainsi les biens et les services numériques atteignent les clients plus rapidement. Ceci profite en particulier aux petites et moyennes entreprises qui ne disposent pas d'une emprise internationale.

Le Scénario 1[1] décrit l'usage d'Internet, reposant sur les transferts de données internationaux, par une personne pour élargir ses chances dans la vie, se développer professionnellement et poursuivre des opportunités professionnelles.

1. Les scénarios de ce rapport sont fictifs et ont pour but d'illustrer les avantages des flux de données transfrontaliers et les inconvénients d'une restriction de ceux-ci. Ils reposent sur la provenance des discussions menées avec les opérateurs des télécoms et les représentants de l'industrie au sujet d'expériences réelles ; ils ne devraient pas être vus comme des cas concrets.



Scénario 1 : **Les transferts de données internationaux permettent des opportunités individuelles**

Luisa apprend à cuisiner en grandissant en Espagne. Une fois adulte, elle déménage dans un autre pays et continue à cuisiner, suivant les dernières recettes de sa région d'origine en utilisant Internet. Son identité numérique et ses préférences améliorent son expérience sur Internet et facilitent la découverte d'informations sur la nourriture espagnole régionale, avec des recettes et des vidéos culinaires.

Elle crée un pop-up business mobile à succès en cuisinant de la nourriture espagnole régionale pour des fêtes et des événements. Luisa ouvre ensuite une école de cuisine, proposant des cours de cuisine pour les adultes en soirée et en journée à son domicile, plus tard elle arrive à ouvrir un petit restaurant. Pour créer une recette spécifique, elle continue à utiliser Internet, les emails et les transferts de fonds électroniques pour commander des ingrédients chez des grossistes spécialisés, dont certains se trouvent en Espagne et livrent à l'international. Avec le temps, son affaire s'installe dans des locaux plus larges et elle emploie plus de personnes.

La réussite de Luisa dans la création d'une start-up dépend de son accès à Internet et de la circulation des données au-delà des frontières. Puisqu'elle a développé progressivement ses activités professionnelles pour créer de l'emploi, pour elle-même et pour les autres, Le gouvernement a bénéficié de recettes fiscales et de nombreux clients profitent de sa cuisine espagnole régionale.

Avantages pour les Etats et la société

En permettant les échanges des données par-delà les frontières, il est possible de ramener plus d'entreprises et de consommateurs du pays dans le giron numérique, encourageant l'adoption de stratégies commerciales reposant sur les données et stimulant l'économie nationale.

La croissance des services Internet au niveau national est soutenue par des approches flexibles du transfert transfrontalier des données. La liberté de circulation des données personnelles produit des avantages sociaux et économiques plus rapidement que l'alternative, qui demanderait que les entreprises développent leurs structures de traitement et de stockage en back-office de manière spécifique pour plusieurs marchés individuels.

Le rôle stratégique du transfert transfrontalier des données a été reconnu par les responsables politiques :

- Le Conseil de l'Europe[2] explique que : « les flux de données mondiaux jouent un rôle de plus en plus significatif dans la société moderne, permettant l'exercice de droits et de libertés fondamentaux tout en suscitant de l'innovation et en encourageant le progrès social et économique, et en jouant également un rôle vital pour assurer la sécurité publique. »

- L'APEC[3] reconnaît : « l'importance du développement de protections efficaces de la vie privée qui évitent d'imposer des barrières aux flux d'informations et assurent un commerce et une croissance économique continus dans la région Asie-Pacifique. [...] Les systèmes règlementaires limitant inutilement ce flux ou l'alourdissant ont des conséquences néfastes sur le commerce mondial, les économies et les individus. C'est pourquoi, via la promotion et l'application de pratiques éthiques de l'information, il est également nécessaire de développer des systèmes de protection de la vie privée qui prennent en compte ces réalités de l'environnement mondial. »

- La CNUCED[4] cite des travaux du McKinsey Global Institute : « La dimension internationale des flux [de biens, services et de fonds a] fait croître le PIB mondial d'environ 10 %, soit une valeur de 7,8 trillions de dollars en 2014. Les flux de données représentent environ 2,8 trillions de dollars de cette valeur ajoutée. »

- L'OCDE[5] affirme que : « Les flux de données transfrontaliers ont augmenté l'efficacité et la productivité économique, relevant le bien-être et le niveau de vie. »

- La Commission européenne[6] soutient que : « Les restrictions injustifiées de la libre circulation des données sont susceptibles de limiter le développement de l'économie des données de l'UE [...] risquent de fragmenter le marché, en réduisant la qualité des services pour les utilisateurs et la compétitivité des fournisseurs de services de données, surtout pour les plus petites structures. »

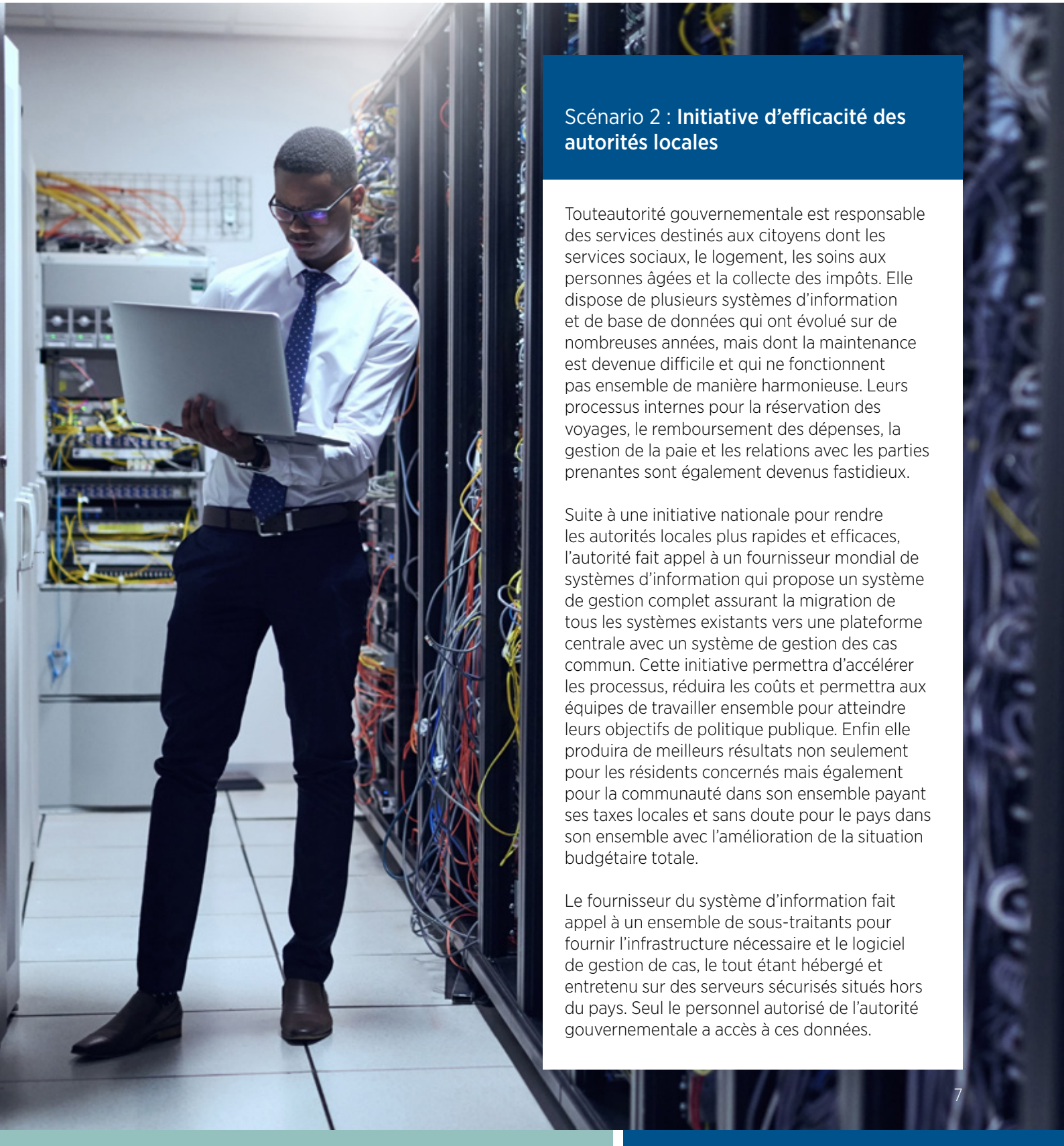
- La Chambre de commerce internationale (ICCI)[7] appelle les gouvernements « à assurer que tous les citoyens et compagnies puissent réaliser l'ensemble du potentiel d'Internet [...] en adoptant des politiques qui facilitent l'adoption de nouvelles technologies et la circulation mondiale des données qui les permettent. »

- En évoquant le rôle des flux de données transfrontaliers dans le secteur manufacturier, le Conseil national du commerce de Suède[8] soutient : « Un flux constant et ininterrompu de biens, de services, de capital, de personnes et de données est nécessaire pour une production optimale. [...] la circulation des données est déjà aujourd'hui une partie indispensable du processus de production [et] elle sera encore plus au cœur de la production du futur. »

2. Conseil d'Europe, « Explanatory Report to the Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data », (CETS 223), 2018. Para 12.
3. Coopération économique pour l'Asie-Pacifique, « Updates to the APEC Privacy Framework », 2016/CSOM/012app17.
4. Conférence des Nations unies sur le commerce et le développement (CNUCED), « Data protection regulations and international data flows: Implications for trade and development », 2016.
5. OCDE, 2012 Internet Economy. Paper 143.
6. Commission européenne, « Building a European Data Economy », COM (2017) 9 final.
7. CCI, « Trade in the digital economy – A primer on global data flows for policymakers », 2016.
8. Conseil National du Commerce (Suède), « No Transfer, No Production – A Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods », 2015.

Les régimes règlementaires qui facilitent les transferts internationaux de données permettent à de petites organisations spécialisées d'établir une présence sur Internet qui soit à la fois nationale et internationale. Des services peuvent émerger et être adoptés avec succès sur un marché national, puis s'étendre à d'autres marchés, créant rapidement des avantages pour le deuxième pays et les pays suivants.

Les organismes publics et les services gouvernementaux bénéficient également des flux de données transfrontaliers qui leur permettent de fournir des services publics de meilleure qualité à moindre coût et de poursuivre des objectifs de politique publique qui ne seraient autrement pas réalisables, comme le montrent les deux scénarios suivants.



Scénario 2 : **Initiative d'efficacité des autorités locales**

Touteautorité gouvernementale est responsable des services destinés aux citoyens dont les services sociaux, le logement, les soins aux personnes âgées et la collecte des impôts. Elle dispose de plusieurs systèmes d'information et de base de données qui ont évolué sur de nombreuses années, mais dont la maintenance est devenue difficile et qui ne fonctionnent pas ensemble de manière harmonieuse. Leurs processus internes pour la réservation des voyages, le remboursement des dépenses, la gestion de la paie et les relations avec les parties prenantes sont également devenus fastidieux.

Suite à une initiative nationale pour rendre les autorités locales plus rapides et efficaces, l'autorité fait appel à un fournisseur mondial de systèmes d'information qui propose un système de gestion complet assurant la migration de tous les systèmes existants vers une plateforme centrale avec un système de gestion des cas commun. Cette initiative permettra d'accélérer les processus, réduira les coûts et permettra aux équipes de travailler ensemble pour atteindre leurs objectifs de politique publique. Enfin elle produira de meilleurs résultats non seulement pour les résidents concernés mais également pour la communauté dans son ensemble payant ses taxes locales et sans doute pour le pays dans son ensemble avec l'amélioration de la situation budgétaire totale.

Le fournisseur du système d'information fait appel à un ensemble de sous-traitants pour fournir l'infrastructure nécessaire et le logiciel de gestion de cas, le tout étant hébergé et entretenu sur des serveurs sécurisés situés hors du pays. Seul le personnel autorisé de l'autorité gouvernementale a accès à ces données.

Scénario 3 : **Big Data pour le Bien de la Société**

Le maire d'une ville a fixé des objectifs ambitieux de réduction de la pollution. Son équipe commande un projet combinant les données des stations météo, de capteurs fixes de qualité d'air et d'opérateurs téléphoniques. Les données rendus anonymes et les données agrégées issues des opérateurs téléphoniques offrent des informations détaillées sur les motifs de déplacement des visiteurs en continu. Cela permet à la ville d'inciter les gens à se déplacer à d'autres moments ou en utilisant d'autres moyens de transport et permet une surveillance plus précise et plus économique de la pollution dans la ville par rapport à un réseau de capteurs statiques collectant des données équivalentes.

Pour obtenir des meilleurs résultats encore, le projet prévoit de collaborer avec d'autres villes du monde afin de comparer la sévérité des niveaux de pollution entre les villes et découvrir des motifs et tirer des enseignements des décisions politiques les plus efficaces. Ceci sera bénéfique pour toutes les villes participantes, pour leurs habitants et leurs visiteurs.

Afin de collaborer efficacement, les villes et les compagnies participantes signent un accord et désignent ensemble un fournisseur d'analyses principal qui héberge les données anonymes et agrégées sur une plateforme commune. Même si les analyses sont effectuées sur tous les ensembles de données, aucune ville ni compagnie n'a accès aux données brutes fournies par une autre partie. Cependant elles bénéficient toutes des enseignements exploitables dégagés. Par conséquent, le maire de la ville a atteint ses objectifs ambitieux et les gens bénéficient d'une meilleure qualité de vie au quotidien et de meilleurs résultats médicaux sur le long terme.

Avantages pour les organisations

Chaque organisation, aussi petite soit-elle, peut utiliser Internet pour commercialiser et livrer ses idées, biens et services, partout où la circulation des données est autorisée. Ce ne serait pas possible sans circulation de données entre pays pour permettre aux organisations de fournir des informations et des produits en réponse aux demandes des particuliers.

Les flux de données transfrontaliers permettent également aux organisations multinationales d'être plus efficaces en centralisant et en virtualisant leurs opérations. Ces organisations peuvent développer leur activité de manière économique, en utilisant une infrastructure flexible reposant sur le cloud et sur les fournisseurs de services applicatifs spécialisés tout en minimisant l'investissement dans des équipements supplémentaires de technologies de l'information.

Les entreprises internationales de tout genre adoptent des stratégies de transformation numérique orientées sur les données pour sécuriser leur avenir. Ceci peut impliquer une réforme des processus internes ou une sous-traitance externe des technologies de l'information et commerciales. Ces stratégies compétitives dépendent de la capacité de collecter, analyser, traiter et stocker les données dans des opérations impliquant plusieurs pays. Là où les flux de données sont possibles, de nouvelles formes d'analyses de données émergent, permettant aux organisations de générer des enseignements sur les opinions de leurs clients et la performance de leurs opérations et produits.

La libre circulation des données personnelles à l'international permet aux entreprises d'améliorer la qualité de leur service et de réduire les coûts, ce qui, en situation de concurrence, mène à des prix plus bas pour les clients. Les fournisseurs d'infrastructure Internet, les fournisseurs d'informatique hébergés et les opérateurs téléphoniques peuvent structurer leurs services pour servir de grands nombres de clients sur des marchés multiples au prix global le plus bas.

Par exemple, le scénario 4 décrit un opérateur télécom majeur en Asie qui utilise des transferts de données transfrontaliers pour améliorer la qualité de service de son réseau mobile et démontre comment cela bénéficie aux clients et aux gouvernements.

Scénario 4 : **La centralisation et la virtualisation des données améliorent la qualité de service du réseau mobile**

Un opérateur télécom majeur en Asie améliore la qualité de service de son réseau en créant un seul centre pour fournir une gestion de réseau et une assurance de qualité améliorées pour ses entreprises nationales. Le nouveau centre à l'échelle du groupe surveille la performance du réseau, la congestion et les défauts. Cette capacité virtuelle permet à l'opérateur d'accéder aux données de performance et de défauts et de les comparer à l'échelle de son emprise, ce qui serait impossible avec uniquement une gestion de réseau à l'échelle nationale.

Le nouveau centre accède à des outils de gestion du réseau et des services plus élaborés proposés par les fournisseurs d'équipements et est capable d'utiliser les outils de diagnostic et de surveillance d'un seul fournisseur sur de nombreux marchés nationaux. Ceci a permis d'améliorer la qualité du réseau mobile tout en optimisant l'investissement. En formant un 'centre d'excellence' pour améliorer sa gestion de réseau et des services, l'opérateur a pu développer les capacités techniques des employés du pays via des délocalisation issus d'entreprises nationales et d'autres activités de développement des parcours professionnels.

L'analyse des données collectées sur les marchés nationaux implique que l'opérateur peut, de manière proactive diagnostiquer les conditions de défaut, y compris les défauts de réseau plus complexes, tout en répartissant son capital et ses frais de personnel sur tous les clients dans son emprise. Pour les consommateurs et les gouvernements, la qualité de service et la qualité d' Internet mobiles sont améliorés via la centralisation des données.

Les gouvernements peuvent aider à réaliser les avantages ci-dessus via des cadres politiques publiques qui facilitent au maximum les flux de données transfrontaliers, tout en réalisant d'autres objectifs de politique publique comme la confidentialité et la sécurité des données.

Restrictions applicables aux flux de données transfrontaliers

Raisons généralement données pour justifier la mise en place de restrictions

Certains pays ont introduit des restrictions sur le flux transfrontalier de données. Les raisons derrière ces restrictions varient d'un pays à un autre, mais comprennent typiquement une ou plusieurs des justifications suivantes :

- **Confidentialité et sécurité des données.** Les données peuvent être traitées dans des pays qui ne disposent pas d'une règlementation équivalente sur la confidentialité des données et pourraient être plus vulnérables au piratage.
- **Surveillance étrangère.** Les données détenues à l'international peuvent être vulnérables à la surveillance d'autres gouvernements ou groupes étrangers.
- **Sécurité nationale.** Les sociétés Internet et les opérateurs téléphoniques détenant les données à l'international peuvent ne pas être forcés à apporter le même soutien aux organisations d'application de la loi ou de sécurité nationale.
- **Economie numérique nationale.** L'encouragement de l'analyse, du traitement et du stockage des données dans le pays peut être vu comme une façon de protéger ou de stimuler l'économie numérique nationale.

Types de restrictions

Pour les organisations, l'impact des restrictions sur les flux de données transfrontaliers varie en fonction de la restriction appliquée. Les types de restrictions comprennent :

- **Flux de données conditionnels** – Lorsque la confidentialité et la sécurité des données sont à l'origine de la restriction, les organisations peuvent devoir demander une autorisation préalable auprès des régulateurs, des autorités de protection des données et obtenir l'accord des particuliers ou spécifier des clauses contractuelles imposées pour chaque destinataire des données. Les cadres autorisant des permissions générales comme les Règles de Confidentialité Transfrontalières de l'APEC et les Règles Contraignantes pour le Sociétés de l'UE peuvent être plus attractifs car elles permettent aux organisations de transférer des données en continu au sein d'un groupe de sociétés ou vers des destinataires spécifiques. Cependant, les processus pour obtenir de telles permissions peuvent être fastidieux et coûteux. Lorsqu'un pays estime qu'un autre pays dispose d'un régime de confidentialité proposant un 'niveau adéquat de protection' ou

'équivalent' au sien, les données peuvent être librement transférées entre les pays. Cependant de telles conclusions 'd'adéquation' sont établies lentement et ne s'appliquent qu'à très peu de pays.

- **Localisation + propagation des flux** – Les organisations peuvent être forcées à conserver une copie de toutes les données et métadonnées personnelles dans le pays d'origine, alors que des copies supplémentaires de ces données peuvent être transférées à l'étranger pour une analyse, un traitement et un stockage centralisés.
- **Localisation** – Les organisations peuvent être soumises à des règles plus prohibitives qui les empêchent de transférer toute donnée ou big data personnelle. Elles peuvent résulter d'obligations du cahier des charges historiques ou d'autres autorisations exigées des opérateurs télécom ou d'autres fournisseurs, ou de nouvelles règlementations qui peuvent s'appliquer à toute entreprise dont l'activité concerne la fourniture de services numériques.
- **Indirectes** – Des règles indirectes (et dans certains cas tacites) peuvent avoir pour effet de conserver les données dans un pays spécifique ou d'exiger qu'elles soient détenues par un fournisseur national.

Impact des restrictions

Lorsque des conditions supplémentaires, comme des clauses contractuelles standards ou d'accord des particuliers, sont exigées pour chaque transfert de données personnelles, cela peut représenter une charge administrative importante pour les organisations. Cela peut aussi conduire à ce que la garantie ne soit perçue que comme un simple exercice administratif avec peu d'intérêt réel pour les personnes concernées. Les mécanismes sont nettement plus efficaces lorsqu'ils encouragent les organisations à mettre en place des programmes systémiques de protection des données personnelles à chaque fois qu'elles sont susceptibles d'être traitées. De tels mécanismes donnent aux organisations des permissions générales pour transférer les données au-delà des frontières tout en permettant aux organisations de se concentrer sur l'identification et la minimisation du risque.

En exigeant que les organisations conservent une copie supplémentaire des données générées par leurs activités dans un pays, on augmente le coût de production des biens et des services pour ce marché. Les compagnies doivent également commander et opérer des centres de données à l'échelle nationale qui pourraient autrement supporter de multiples marchés nationaux, voire à l'échelle mondiale à partir d'un ou (pour renforcer la résilience) deux centres de données.

Les coûts augmentent encore lorsqu'en plus du stockage, l'analyse et le traitement des données doivent être effectués à l'échelle nationale. Dans ce cas, la règlementation impose que les organisations fournissent effectivement des biens et des services numériques en utilisant des entreprises en double à l'échelle nationale, créées spécifiquement pour des marchés nationaux réglementés individuellement. En fonction de l'architecture et de la mise en œuvre technique des compagnies, ce type de régime plus coûteux retarde et fragmente l'introduction de biens et de services numériques et réduit leur visibilité.

En guise d'exemples, voici le Scénario 5 qui aborde la détection des défauts à distance par un fabricant de véhicules et le Scénario 6 qui présente en détail le déploiement international du service d'Internet des Objets (IdO) par un opérateur de télécommunications mondiale.

Scénario 5 : **Détection des défauts de véhicules par-delà les frontières**

Les véhicules modernes sont de plus en plus intelligents, équipés de capteurs pour mesurer des données de performance du moteur et détecter les défauts du véhicule. Les mécaniciens peuvent consulter ces données pour diagnostiquer les défauts plus efficacement. Certains fabricants utilisent la technologie de communication entre machines (M2M) pour envoyer les données de surveillance des défauts vers des serveurs centraux, permettant la détection et le diagnostic d'un défaut avant qu'il ne devienne apparent pour le propriétaire de la voiture. Le M2M est également utilisé pour alerter les clients sur le besoin d'entretien du véhicule. Les flux de données transfrontaliers sont importants dans ces scénarios qui renforcent la fiabilité et peuvent potentiellement sauver des vies, car les voitures et les véhicules commerciaux traversent des frontières en permanence.

Pour renforcer d'autant plus les avantages, les véhicules connectés permettent l'analyse de big datas par les fabricants, indiquant les caractéristiques de performance de toute une ligne de véhicules connectés. Ce scénario ne s'applique toutefois que dans des marchés ou des juridictions où les fabricants sont autorisés à se connecter aux véhicules des clients et à analyser les données collectées. Les pays ne permettant pas la libre circulation transfrontalière des flux de données empêchent par conséquent le diagnostic des véhicules à distance et donc la concrétisation de transports plus sûrs et plus fiables.

Scénario 6 : **Service IdO des multinationales reposant sur un seul centre de données**

Un opérateur télécom internationale a développé un service permettant aux consommateurs, en utilisant une application mobile, de localiser, surveiller et suivre des objets comme les véhicules familiaux, les sacs à dos, les animaux de compagnie ou le bétail. Via ce service, la condition en temps réel des objets peut être inspectée, les objets perdus retrouvés et des alarmes peuvent être définies en fonction de l'emplacement de l'objet.

Ce service est lancé à l'international en utilisant un centre de données commun, pour que chaque marché national puisse être desservi sans devoir répliquer les systèmes informatiques en interne. Les fabricants peuvent également tester leurs produits pour découvrir ce que les clients des différents marchés nationaux et des différents segments trouvent utile.

Sur les marchés nécessitant un centre de données localisé dans le pays, le fournisseur de service fait face à des coûts plus élevés pour la personnalisation et le déploiement de l'architecture du produit. C'est pourquoi il décide de renoncer au lancement du service sur ces marchés pour le moment. La conséquence des restrictions des flux de données transfrontaliers est que les clients n'ont pas accès à un suivi à bas coût des objets personnels ; les fabricants ne peuvent pas tester les produits pour évaluer leur valeur sur le marché national et les gouvernements passent à côté d'avantages économiques et fiscaux apportés par ce service innovant et utile.

Il faudrait noter que la manière dont de telles restrictions de localisation sont implémentées ou interprétées par les autorités nationales peut significativement réduire leur impact négatif.

Lorsque les gouvernements insistent pour la mise en place de telles mesures, ils devraient donc interagir avec l'industrie et d'autres acteurs avant leur implémentation.

Exemples de restrictions nationales

Certains marchés se sont significativement éloignés ou envisagent de s'éloigner d'un modèle permettant la libre circulation transfrontalière des flux de données.

Dans la catégorie des restrictions basées sur les questions de confidentialité des données, le niveau des flux de données personnelles est variable. La Corée du Sud, par exemple, impose des exigences d'accord strictes pour le transfert de données personnelles avec des exceptions très limitées comme lorsque le transfert des données est exigé par la loi, nécessaire pour assurer une fonction publique ou pour protéger des intérêts vitaux en situation d'urgence. La Côte d'Ivoire n'autorise les transferts de données qu'avec une autorisation préalable ou vers des pays disposant d'un niveau adéquat de protection, mais sans pouvoir définir clairement quels pays rentrent dans cette catégorie. D'autres pays proposent aux organisations un ensemble d'exceptions et de mécanismes de transfert plus flexibles qui réduisent significativement l'impact de la restriction.

Les restrictions générant le plus de difficultés pour les organisations sont celles qui demandent, directement ou indirectement, de conserver les données dans le pays. La Russie, par exemple, demande aux organisations (y compris aux filiales des compagnies étrangères) qui collectent les données de ses citoyens via des communications électroniques de stocker ces données au niveau national.[9] Les données personnelles doivent être stockées dans une base de données primaire située et gérée en Russie. Même si les données peuvent par la suite être transférées à l'étranger et stockées dans des bases de données secondaires, sid'autres exigences légales[10] pour le traitement de telles données sont remplies, l'exigence de conserver

9. La loi Fédérale du 21 juillet 2014 No. 242-FZ a modifie certains actes législatifs de la Fédération de Russie en rapport avec les informations de traitement des données personnelles et les réseaux de télécommunication.
10. Incluant la Loi sur les Données Personnelles du 27 juillet 2006 N 152-FZ qui interdit les transferts transfrontaliers de données vers des pays ne disposant pas de la protection adéquate des données.

les données originales en Russie demande des ressources supplémentaires.

Les opérateurs télécoms, les sociétés Internet et d'autres entreprises en Indonésie proposant un 'service public' aux clients indonésiens via un système électronique, doivent créer un centre de données national et un centre de sauvegarde en cas de sinistre.[11] Ceci comprend les services proposés par des institutions non-gouvernementales dans les domaines bancaires, des communications, de la santé, des assurances, des services industriels, de la sécurité et des réseaux sociaux. Les justifications données pour la création à la fois d'un centre de données national et d'un centre de sauvegarde en cas de sinistre répondent à des exigences d'application de la loi et de la protection des données. Les transferts de données sont en principe autorisés, sous réserve de l'accord du Ministère Indonésien des Communications et de l'Informatique, même si ce processus reste à clarifier.

L'Autorité des Télécommunications et la Banque d'Etat du Pakistan interdit aux compagnies téléphoniques et financières de transférer les données des clients à l'étranger. Cependant, d'autres données, dont les contenus d'emails, peuvent être légalement transmises hors du pays. Les meme conditions de licence s'appliquent en Inde.

Au Vietnam, l'existance de stockage des données sur des serveurs locaux a récemment été remplacée par une exigence pour les fournisseurs de services téléphoniques et Internet étrangers avec plus de 10 000 abonnés de disposer d'un siège social ou de bureaux de représentation au Vietnam et de stocker les données personnelles des utilisateurs vietnamiens dans le pays.

En Allemagne, les opérateurs téléphoniques sont obligés de conserver les données de trafic et de localisation allemandes (même si cette exigence n'est pas appliquée du fait de nombreux problèmes juridiques). Le Kazakhstan considere une loi qui obligerait les opérateurs téléphoniques à stocker les données des abonnés uniquement au Kazakhstan en dehors des besoins d'itinérance.

Réponses aux préoccupations (nationales) en matière de confidentialité nationale

Lorsque la logique annoncée pour la restriction des flux de données transfrontaliers relève de la protection des données, les responsables politiques estiment que les données pourraient ne pas être protégées lors de transferts internationaux et les individus pourraient ne pas disposer de droits suffisants dans des pays ne proposant pas les mêmes règles.

Cette préoccupation est valide mais une réponse proportionnée et efficace devrait passer par un cadre national ou régional de confidentialité des données, protégeant les citoyens et les consommateurs à l'échelle nationale tout en proposant des mécanismes adaptés pour les transferts internationaux de données avec les conditions associées.

Lorsque les questions de confidentialité concernent la sécurité de l'information, elles reposent sans doute sur la fausse idée que les données stockées dans un marché national spécifique sont plus sûres que les données stockées à l'international. Cependant, la sécurité effective de l'information ne peut pas se résumer à un seul élément, comme l'emplacement physique des données. Elle dépend d'une combinaison de nombreux facteurs, dont l'infrastructure de stockage, l'intelligence des protocoles de sécurité, l'utilisation du cryptage et d'autres bonnes pratiques en technologies de l'information.

Le fait d'imposer un stockage national des données crée des problèmes de sécurité des données car cela demande un investissement spécifique pour des marchés nationaux. Ce processus est plus coûteux et plus vulnérable aux intrusions que des défenses professionnelles internationales à une échelle plus large.[12]

De nombreux pays et régions adoptent aujourd'hui des modèles règlementaires visant à assurer des flux de données transfrontaliers, sous réserve d'exigences appropriées en termes de protection des données.

La confidentialité des données est réglementée à des

11. Le Règlement No. 20 du 1 décembre 2016 sur la Protection des Données Personnelles dans les Systèmes Electroniques qui implémente le Règlement du Gouvernement 82 de 2012 : Sur la Provision de Systèmes et de Transactions Electroniques.
12. Le Livre Blanc d'Amazon sur la Localisation des Données de février 2018 propose une discussion étendue sur la sécurité du point de vue d'un fournisseur de service cloud à 'hyper-échelle' sur : https://d1.awsstatic.com/whitepapers/compliance/Data_Residency_Whitepaper.pdf

niveaux différents aux Etats-Unis. Certaines lois fédérales ciblent des secteurs ou des activités comme les rapports de solvabilité ou l'usage de données médicales alors que les lois des états vont des rapports de failles de sécurité à des lois plus générales. Au niveau fédéral, la Commission fédérale du commerce impose les bonnes pratiques de confidentialité des données dans le cadre de sa juridiction sur les actes et pratiques commerciaux malhonnêtes et mensongers et en lien avec des problématiques spécifiques comme la vie privée des enfants. La Commission fédérale des communications fixe les règles et supervise les fournisseurs des réseaux. En général ces lois ne restreignent pas la circulation des données hors des Etats-Unis, mais se concentrent sur la responsabilité des organisations quant à l'utilisation des données par elles-mêmes ou leurs fournisseurs. Les Etats-Unis interagissent positivement avec les cadres régionaux pour faciliter les flux de données transfrontaliers, participant au système CBPR de l'APEC et au Privacy Shield UE-EU. L'approche américaine axée sur la responsabilisation a permis la croissance rapide des entreprises de biens et de services numériques nationales et, sans doute, la domination d'une grande partie de l'économie internationale pour les biens et les services numériques.

L'Union européenne a adopté l'influente Directive de Protection des Données[13] en 1995. Cette approche a évolué en un Règlement Général de la Protection de Données[14] (RGPD). Le RGPD vise à offrir une protection des données personnelles cohérente au niveau de l'UE, tout en leur permettant de circuler dans l'UE et vers des pays tiers dont on estime qu'ils disposent de régimes de protection des données 'adéquates'. Dans le cadre du RGPD, les organisations pouvant démontrer aux autorités de protection des données qu'elles gèrent les données personnelles de manière responsable, soit via ce qu'on appelle des 'règles d'entreprise contraignantes' soit via des certifications, pouvant bénéficier d'autorisations générales pour transférer des données personnelles hors de l'UE. La loi permet également un ensemble de mécanismes et d'exceptions[15] visant à donner aux organisations un degré de flexibilité pour couvrir leurs besoins en flux de données d'une manière qui pourrait correspondre le mieux à l'organisation. Les propositions récentes dans plusieurs pays du monde ont commencé à suivre le modèle du RGPD. Au Brésil, par exemple, les transferts de données personnelles seront autorisés dans le cadre de la nouvelle loi à condition que le pays tiers dispose des mécanismes adéquats de protéger les données personnelles et faciliter la coopération institutionnelle et juridique.

En septembre 2017, la Commission européenne a publié une proposition supplémentaire visant à assurer la libre circulation des données 'non-personnelles' afin de renforcer l'économie numérique européenne. Cette mesure propose :

- La libre circulation des données non-personnelles au sein de l'UE (pour complémenter celle des données personnelles) ;
- L'accès des autorités publiques aux données situées dans un autre Etat-Membre de l'UE ou sur le cloud ;
- Une approche d'autorégulation pour permettre aux utilisateurs professionnels de changer de fournisseurs de services cloud.

L'opérabilité de la mesure de règlementation des données non-personnelles n'a pas été encore clarifiée. Cependant, la Commission européenne estime que l'assurance de la libre circulation des données au sein de l'UE soutiendra l'économie numérique européenne et générera un excédent de 0,7 % du PIB d'ici 2020, par comparaison au 0,2 % en 2013.[16]

Les pays de la région Asie-Pacifique ont développé un modèle commun de réglementation des flux de données internationaux sous les auspices de l'APEC, dont les Règles de Confidentialité Transfrontalières (CBPR) décrivent le fonctionnement des flux de données entre les économies de l'APEC.

Les CBPR de l'APEC comptent trois éléments majeurs :

- L'adoption de principes partagés dans le traitement des données personnelles ;
- La création de mise en place des mécanismes dans lesquels les données sont transférées entre les économies membres de l'APEC ;
- La responsabilité des organisations qui doivent pouvoir démontrer qu'elles ont mis des conditions en place avant de se voir accorder une autorisation générale pour transférer des données.

Pour le moment, six économies y participent : les Etats-Unis, le Mexique, le Japon, le Canada, Singapour et la République de Corée, d'autres faisant des démarches pour s'y joindre dans un futur proche.

13. La directive 95/46/EC relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
14. Le règlement (EU) 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Le RGPD a été adopté en 2016 et s'applique aux organisations qui traitent les données depuis le 25 mai 2018.
15. Pour plus d'informations sur la gamme de mécanismes de transfert typiquement mis à disposition, veuillez consulter le document du CIPL : « Cross-Border Data Transfer Mechanisms », d'août 2015.
16. L'étude « SMART 2013/0043 - Uptake of cloud in Europe » de l'IDC sur les estimations quantitatives de la demande en termes de services informatiques en cloud en Europe et les obstacles probables à sa réalisation. Citée dans « Measuring the economic impact of cloud computing in Europe » de Deloitte, citée à son tour par la Commission européenne en soutien de sa Directive.

L'Acte sur la protection des Informations Personnelles du Japon a été initialement publié en 2003, amendé en 2015 et est finalement entré en vigueur le 30 mai 2017. En plus d'avoir établi une autorité indépendante de protection des données entièrement fonctionnelle, l'amendement visait à faciliter les flux de données transfrontaliers en introduisant une série de mécanismes, reconnaissant l'importance des flux de données dans une économie numérique. Ceux-ci comprennent à dessein la possibilité pour les organisations de démontrer une gouvernance responsable des données via la certification dans le cadre des CBPR.

Les discussions récentes entre le Japon et l'UE ont conduit à l'annonce par la Commission européenne en juillet 2018 de la reconnaissance formelle des deux systèmes de protection des données réciproques comme proposant un niveau de protection équivalent aux consommateurs des deux marchés. Ceci créera la zone la plus large au monde, comprenant 37 % du commerce global en valeur, au sein de laquelle les données personnelles peuvent circuler librement tout en recevant un niveau de protection cohérent. L'UE et le Japon s'attendent à ratifier le processus de reconnaissance de leurs systèmes de protection des données respectifs comme étant 'adéquats' avant fin 2018. Le Japon est actuellement bien placé pour soutenir la libre circulation des données internationales à la fois en Asie-Pacifique et avec l'UE, même si les cadres restent différents.

Les pays qui adoptent des approches de protection de données acceptées au niveau international profitent au niveau économique d'une infrastructure de services numériques partagés opérant à une échelle mondiale. De tels marchés de 'données connectées' forment un flux de données intégré à l'international où les biens et les services numériques peuvent être produits à une échelle et avec une qualité mondiales.

Réponses aux préoccupations en matière de surveillance étrangère et de sécurité nationale

Les informations révélées par Edward Snowden en 2013 sur les activités de l'Agence de sécurité nationale (NSA) américaine ont exposé l'existence d'accords avec un certain nombre de sociétés Internet pour obtenir un accès aux données privées de non-ressortissants des Etats-Unis. Sans surprise, la révélation d'une surveillance étendue et secrète par la NSA des données privées de services numériques situées aux Etats-Unis a troublé les gouvernements du monde entier. Ceci a donné un élan aux préoccupations en termes de surveillance étrangère de données détenues sur d'autres marchés nationaux.

Dans les cinq années qui ont suivi les révélations de Snowden, une réponse partielle à ces préoccupations a été la diversification des pays dans lesquels les sociétés Internet et les fournisseurs de service informatique dématérialisés opèrent des centres de données ou des hubs régionaux. Ceci permet aux organisations et aux gouvernements préoccupés par les activités de surveillance étrangère d'éviter que les données ne soient stockées dans des juridictions particulières. Cependant, le fait de permettre ce niveau de contrôle géographique aux organisations s'accompagne inévitablement de coûts qui doivent être absorbés soit par les clients professionnels, soit par le consommateur en bout de chaîne.

De plus, les fournisseurs de service informatique hébergés peuvent proposer à des clients, comme les opérateurs téléphoniques, la capacité de crypter les données numériques en toute sécurité – les clés de telles données pourraient être détenues au niveau national et protéger ainsi contre le décryptage. D'autres techniques comme l'anonymisation et l'agrégation, peuvent également être utilisées pour éviter l'identification de données personnelles transmises à l'international. Ces développements, pris ensemble, réduisent sensiblement les risques de surveillance étrangère lorsque les données sont détenues à l'international.

Contrairement aux démarches pour répondre aux préoccupations de surveillance étrangère, les progrès dans la réponse aux préoccupations d'application de la loi et de la sécurité nationale des pays n'ont pas été aussi sensibles. Il est entendu que les gouvernements sont préoccupés par le fait de perdre l'accès à des données

qui pourraient être utiles à leurs autorités judiciaires et policières, mais qui sont traitées et contrôlées par des sociétés Internet basées hors de leurs pays.

Les dispositions multilatérales en vigueur pour le partage de données en soutien à l'application de la loi peuvent être utilisées, mais il a été évoqué qu'elles opèrent lentement et de manière imparfaite.

Face à ces imperfections, les intérêts de l'application de la loi et de la sécurité nationale se sont orientés vers un stockage national des données et/ou une opération nationale des services car ceci donne un point de contrôle sur les activités des sociétés Internet et des opérateurs téléphoniques. Certains gouvernements sont allés plus loin en limitant les activités des sociétés Internet lorsque celles-ci ne coopéraient pas avec les autorités ou remettaient en cause la sécurité nationale.

Cependant, les développements récents dans ce domaine comprennent le CLOUD Act américain, la proposition eEvidence de l'UE et un protocole supplémentaire à la Convention de Budapest sur la Cybercriminalité. Ces initiatives apportent l'espoir que de nouvelles façons seront établies pour créer des cadres de référence clairs et prévisibles qui donnent une certitude juridique aux organisations et permettent un accès plus direct et plus rapide des autorités aux données à l'étranger dont elles ont besoin, supprimant ainsi le besoin de mesures de localisation.

La réponse aux préoccupations en matière de surveillance étrangère et de sécurité nationale demande une approche pragmatique à la fois de la part des Etats et des entreprises. Au final, les pays qui tourneront le dos aux services disponibles dans l'économie numérique globale devront se tourner vers une production de biens et de services à l'échelle nationale. De leur côté, les grands acteurs économiques d'un marché national auront des difficultés à assurer une activité durable si leurs opérations sont vues comme remettant en cause la loi ou la sécurité nationale.

Réponses aux préoccupations en matière d'économie numérique nationale

La régulation des flux de données transfrontaliers peut aussi être vue par certains comme un moyen de protéger les intérêts économiques des nations et de leurs entreprises. Pourtant cette notion présente des défauts majeurs. En particulier, le fait d'exiger un traitement et un stockage national des données ou une production nationale des services numériques :

- Restreint ces activités à l'échelle nationale et risque d'entraîner des coûts d'opération par client nettement plus élevés ;
- Intègre d'autres facteurs de production nationaux dans les services numériques (ex. si un pays est soumis à des contraintes d'approvisionnement en électricité, celles-ci peuvent être résolues en partie via le recours au stockage international des données et à la production internationale de services numériques) ;
- Risque de retarder, limiter, voire bloquer l'accès des citoyens à des services numériques innovants qui émergent sur la scène mondiale ; et
- Ignore le bénéfice pour l'économie nationale de compétences et de connaissances qui ne sont disponibles que si les données peuvent traverser les frontières.

Encore une fois, une approche politique alignée et coordonnée, supprimant les restrictions et libérant le flux de données sera bénéfique pour les marchés nationaux.

Par exemple, le Scénario 7 illustre comment les restrictions sur les flux de données transfrontaliers affectent non seulement le développement de produits numériques, mais aussi l'efficacité de la fabrication traditionnelle.

Scénario 7 : **Les applications M2M soutiennent le commerce international et réduisent les déchets**[17]

Les chaînes de production et de logistique, que ce soit au sein d'une même entreprise internationale ou entre fournisseurs et clients, peuvent être très complexes. Cette complexité est gérée par des "emballeuses électroniques" qui suivent les produits dans les dépôts et les ports, de la source à la destination.

En utilisant la télémétrie M2M, la documentation électronique est aujourd'hui employée pour étendre la capacité des fournisseurs logistiques à suivre les biens lors de leur transport international. Par exemple, un container de pièces mécaniques peut être suivi de l'usine jusqu'au port, lors de son trajet en mer et jusqu'à son arrivée dans le pays de destination et sa livraison au client.

Les flux de données transfrontaliers permettent une logistique et un suivi plus fiables et plus sûrs, réduisant les coûts de fabrication et les déchets. Cela soutient les chaînes d'approvisionnement internationales et les consommateurs bénéficient de prix bas. Les gouvernements bénéficient d'une capacité accrue à examiner de près le commerce international et à appliquer des droits de douane adaptés.

Les pays exigeant que les données M2M soient gérées sur des serveurs nationaux limiteront la capacité du pays à prendre part à l'économie mondiale.

17. Conseil National du Commerce (Suède), « No Transfer, No Production – A Report on Cross-border Data Transfers, Global Value Chains, and the Production of Goods », 2015.

En l'absence d'approches régionales partagées, les restrictions nationales de la libre circulation des flux de données dans certains marchés risquent de créer deux trajectoires divergentes de développement du marché numérique :

- **Des marchés de données connectées,** comprenant la plupart des marchés développés et de nombreux marchés émergeants où les produits et services numériques sont peu coûteux à produire et proposés à des clients à une échelle et avec une qualité mondiale.

- **Des marchés numériques à l'échelle nationale,** soumis à des restrictions sur la circulation transfrontalière des données et limitant ainsi les opportunités des fournisseurs et les avantages économiques des clients.

Etant données les divergences politiques, il semble probable que les marchés de données connectés seront privilégiés en tant que lieux de production et de consommation, et étendront progressivement leur part du commerce numérique et physique dans le temps.

Les législateurs envisageant le modèle alternatif du marché numérique à l'échelle nationale devraient prendre soigneusement en compte les conséquences économiques de la séparation entre l'analyse, le traitement et le stockage des données dans leur pays et le flux de données international intégré. Cette approche risque de laisser leurs pays dans une impasse sur le plan national qui limitera la croissance numérique de leur marché, par comparaison à la concurrence internationale.

Impact des restrictions des données transfrontalières sur le secteur des télécoms

L'objectif premier des opérateurs téléphoniques est de connecter les gens indépendamment de leur localisation et de la distance. Alors que les télécommunications ont commencé par les télégrammes et ont progressé vers les appels vocaux, les SMS et les e-mails, elles comprennent aujourd'hui des échanges massifs de données et ce sont les infrastructures et les services des opérateurs qui transportent ces données.

Les opérateurs télécoms partagent un objectif commun avec les autres sociétés internationales : ils veulent que les données circulent pour pouvoir profiter de l'efficacité de la centralisation et de la virtualisation. Cependant, puisqu'ils ont traditionnellement été des acteurs nationaux avec une infrastructure physique dans un pays donné, les métadonnées qu'ils génèrent au sujet de communications individuelles – avec qui les usagers se connectent, d'où et pour combien de temps – sont souvent l'objet de règlementations pré-numériques sectorielles ou d'obligations du cahier des charges qui interdisent la circulation des métadonnées hors du pays et imposent leur collecte et leur stockage.

De telles restrictions spécifiques aux télécoms font office d'obstacle à la réalisation du niveau d'efficacité qui est devenu la norme pour la plupart des autres entreprises internationales et pénalisent les opérateurs téléphoniques par rapport à des fournisseurs de services de communication non-réglementés comme les sociétés Internet.

Les opérateurs télécoms sont également en première ligne de l'émergence de l'Internet des Objets et soutiennent les progrès dans l'automatisation, des capteurs météorologiques à distance aux voitures connectées. Pour permettre à ces technologies de déverrouiller leurs potentiels, les opérateurs ont besoin de modèles commerciaux et de technologies communs qui fonctionneront partout dans le monde. Si les opérateurs télécoms doivent subir des restrictions historiques sur les flux de données transfrontaliers spécifiques aux télécoms, ils seront pénalisés par rapport aux sociétés Internet et le développement de ces technologies et modèles commerciaux sera nettement plus lent et plus coûteux.

Dans la mesure où ces restrictions spécifiques aux télécoms reposent sur le caractère sensible perçu des métadonnées et le besoin de protéger la vie privée des personnes concernées, ce document avance qu'il est plus efficace de protéger la vie privée des personnes via des mécanismes horizontaux de protection des données reposant sur une analyse de risque. Plutôt que de constituer une catégorie spécifique de données toujours considérées comme sensibles, le caractère sensible des métadonnées dépend du contexte dans lequel elles sont traitées et des conditions appliquées dans chaque cas. Des lois de confidentialité des données horizontales, s'appliquant au traitement de toutes les données personnelles apportent une protection suffisante en imposant aux organisations d'identifier et de réduire les risques de préjudice pour les individus. Lorsque les données sont transmises

à l'étranger, ces conditions peuvent s'appliquer par extension sans interrompre le flux de données.

Des restrictions spécifiques aux télécoms sont également imposées afin de permettre aux autorités judiciaires et policières et aux services de renseignement d'obtenir un accès légal et approprié aux données. Historiquement, les opérateurs téléphoniques étaient des destinataires naturels de ce genre de demandes dans la mesure où ils disposaient déjà de l'infrastructure physique et des centres de traitement des données dans chaque pays et ce avant l'arrivée de l'Internet, leurs métadonnées étant l'une des sources de renseignement les plus fiables et les plus évidentes. Cependant, il faudrait également reconnaître que le secteur des télécoms est sous pression pour tirer avantage de l'infrastructure en cloud et des services logiciels au même titre que d'autres secteurs. Tout en étant efficace et bonne pour les consommateurs, l'utilisation de services en cloud implique qu'il n'y a pas de besoin opérationnel d'effectuer certaines activités de traitement à proximité physique des installations de communication dans un pays donné.

Les préoccupations des autorités juridiques et policières de ne plus pouvoir accéder aux données dont elles ont besoin pour leurs investigations sont légitimes. Cependant, plutôt que de forcer à une collecte et à un stockage local des données ou à ce que les opérateurs téléphoniques donnent accès à tout le trafic Internet transitant par leurs réseaux, les gouvernements devraient, à l'avenir, se tourner vers des initiatives comme le CLOUD Act américain et la proposition eEvidence de l'UE pour répondre à leurs préoccupations.

En parallèle, il revient également aux opérateurs télécoms qui commencent à centraliser et à virtualiser leurs opérations de fournir une assurance pragmatique aux autorités nationales sur le fait qu'ils continueront à soutenir les demandes légitimes des autorités juridiques et policières.

Approches renforcées pour faciliter les flux de données transfrontaliers

L'industrie mobile croit que les flux de données transfrontaliers sont essentiels pour débloquer des bénéfices pour les particuliers, les organisations, les gouvernements et l'économie à la fois au niveau national et international. Le fait d'identifier les bénéfices de la libre circulation des données ne veut pas dire qu'il ne devrait pas y avoir de règlementation dans ce domaine. Une vue partagée par de nombreux législateurs, organisations et par la société civile est qu'une réglementation intelligente de la confidentialité des données peut à la fois permettre les flux de données et protéger les citoyens en donnant aux consommateurs et aux législateurs des assurances sur les produits et les services numériques.

Afin de permettre les bénéfices soulignés dans ce document, la GSMA voudrait encourager les gouvernements à suivre les recommandations suivantes :

Recommandation 1 : S'engager à faciliter les flux de données transfrontaliers et à supprimer les mesures de localisation inutiles

Les gouvernements devraient s'engager fermement à faciliter les flux de données transfrontaliers et à supprimer les mesures de localisation inutiles afin de réaliser les bénéfices de la libre circulation des données pour les particuliers, les entreprises et les gouvernements.

L'engagement public, que ce soit au niveau national ou dans le cadre d'une instance régionale ou multilatérale, peut définir une direction et une vision stratégique claires pour stimuler l'économie numérique au niveau national et encourager un alignement dans la région. Lorsque les mesures de localisation sont mises en place, les gouvernements devraient consulter les acteurs sur l'interprétation et la mise en œuvre de ces mesures.

Recommandation 2 : Assurer que le cadre de protection des données soit adapté à l'âge numérique

Les législateurs devraient assurer que les cadres légaux couvrent efficacement les questions de protection des données dans leur pays. De tels cadres devraient décrire les droits à la vie privée des citoyens et des consommateurs ainsi que les obligations des organisations pour la collecte, l'analyse et le stockage des données.

Afin d'être adaptés à l'âge numérique, les cadres de confidentialité nationaux devraient reposer sur « l'ensemble central des principes de protection des données qui sont dits être au cœur de la plupart des lois [sur la vie privée] nationales et des régimes internationaux ».[18] De telles approches devraient refléter les préoccupations des consommateurs sur la confidentialité et la sécurité des données[19] et devraient opérer sur une base technologique et sectorielle neutre afin d'assurer les clients d'un traitement régulier de leurs données. Ils devraient également prévoir la création et le financement d'une autorité nationale de protection des données.

La règlementation de la vie privée devrait se concentrer sur les risques de préjudice des particuliers et incorporer des mesures pour assurer la responsabilisation des organisations collectant les données, tout en prévoyant une implémentation flexible afin de permettre aux organisations d'innover rapidement, d'atteindre une plus grande échelle de production et d'en réduire les coûts.

Recommandation 3 : Passer en revue les règles sectorielles de confidentialité traditionnelles

Historiquement, les opérateurs ont souvent fait l'objet de restrictions sectorielles sur les flux de données internationaux. L'objectif premier des opérateurs télécoms est de connecter les gens indépendamment de leur localisation et de la distance. Même si les télécommunications ont commencé par les télégrammes et ont progressé vers les appels vocaux, les SMS et les emails, elles comprennent aujourd'hui des échanges massifs de données et le transport de celles-ci par l'infrastructure et les services des opérateurs. Les données étant une force motrice de l'économie numérique, cela n'a aujourd'hui plus de sens de traiter les données des opérateurs télécoms différemment des données générées par d'autres fournisseurs de communications électroniques ou par l'économie numérique au sens large. La création d'un cadre de confidentialité national adapté à l'âge numérique donne l'opportunité de passer en revue les règles sectorielles historiques sur la confidentialité pour vérifier si elles sont encore pertinentes.

Recommandation 4 : Encourager les initiatives régionales de protection des données

Les organismes supranationaux comme l'APEC et l'Union européenne ont déjà adopté des modèles règlementaires pour la protection et la confidentialité des données tout en s'assurant qu'elles puissent circuler librement dans la région. Ces modèles apportent une réponse efficace et proportionnée aux législateurs qui souhaitent protéger les citoyens et les consommateurs tout en soutenant le commerce international de biens et de services physiques et numériques.

Les initiatives régionales de confidentialité des données devraient être encouragées et mises en œuvre sur la base de principes communs, soutenir les flux de données inter-régionaux et être interopérables avec les approches existantes de l'APEC et de l'UE[20], et avec des approches nationales similaires. Les initiatives régionales créent une capacité règlementaire couvrant la confidentialité des données et le développement des bonnes pratiques du secteur pour le traitement des données. Ceci développera la confiance entre les pays, facilitera le partage des bonnes pratiques entre les législateurs et permettra aux régulateurs de la vie privée de détecter et de résoudre plus facilement les non-conformités.

Le fait de répondre aux préoccupations de sécurité et de confidentialité des consommateurs nationaux de manière cohérente à l'échelle de la région facilitera les flux de données transfrontaliers tout en mettant en place des mécanismes de gouvernance des données visant à assurer la responsabilisation du secteur au niveau national et international.

18. CNUCED, « Data protection regulations and international data flows: Implications for trade and development », 2016. Voir : http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf
19. Voir, par exemple, les recherches sur la vie privée publiées par la GSMA en 2014 : https://www.gsma.com/publicpolicy/wp-content/uploads/2014/02/MOBILE_PRIVACY_Consumer_research_ insights_and_considerations_for_policymakers-Final.pdf
20. En particulier, être interopérable avec les Règles de Confidentialité Transfrontalières (CBPR) de l'APEC, les Règles d'entreprise contraignantes (BCR) de l'UE et le modèle de référence commun associé établi par un groupe de travail commun entre l'APEC et l'UE.

Recommandation 5 : Eviter la localisation en répondant de manière pragmatique aux questions de surveillance étrangère

Les gouvernements devraient prendre en compte la gamme d'options disponibles pour protéger les données considérées comme sensibles, plutôt que d'en exiger la localisation. Ces options comprennent le cryptage, l'anonymisation et l'agrégation, et, sous certaines circonstances, peuvent inclure la spécification de plateformes régionales particulières pour des types de données spécifiques.

Recommandation 6 : Eviter la localisation en répondant de manière pragmatique aux questions de sécurité nationale et conformité aux lois nationales

Les gouvernements devraient suivre des initiatives comme le protocole supplémentaire de la Convention de Budapest sur la Cybercriminalité, le CLOUD Act américain et la proposition eEvidence de l'UE afin d'établir des cadres clairs et prévisibles qui donnent aux organisations une certitude juridique et accordent aux autorités un accès plus rapide aux données dont ils ont besoin à l'étranger, supprimant par là même le besoin de mesures de localisation.

L'adoption de ces recommandations :

- Permettra à l'économie numérique de fonctionner efficacement et d'apporter des bénéfices sociaux et économiques plus rapidement dans de nombreuses nations et régions.
- Donnera aux gens l'accès à une gamme mondiale et une grande qualité de services, dépassant les contraintes des marchés nationaux lorsque celles-ci existent.
- Permettra aux entreprises établies, y compris aux opérateurs télécoms, d'adopter les stratégies de transformation numérique fondées sur les données afin de réduire les coûts et donc les prix des produits numériques et physiques sur le marché.

SIEGE SOCIAL DE LA GSMA
Floor 2
The Walbrook Building
25 Walbrook
Londres, EC4N 8AF,
Royaume-Uni
Tél : +44 (0)20 7356 0600
Fax : +44 (0)20 7356 0601