COMMISSION
EUROPÉENNE

Bruxelles, le 10.1.2017
COM(2017) 9 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

«CRÉER UNE ÉCONOMIE EUROPÉENNE FONDÉE SUR LES DONNÉES»

{SWD(2017) 2 final}

«CREER UNE ECONOMIE EUROPEENNE FONDEE SUR LES DONNEES»

1. INTRODUCTION

Les données sont devenues une ressource essentielle pour la croissance économique, la création d'emplois et le progrès sociétal. L'analyse des données permet d'améliorer le processus décisionnel, l'innovation et la prévision des événements. Cette tendance mondiale représente un énorme potentiel dans divers domaines, allant de la santé, de l'environnement, de la sécurité alimentaire, du climat et de l'utilisation efficace des ressources à l'énergie, aux systèmes de transport intelligents et aux villes intelligentes.

L'«économie fondée sur les données»[1] est caractérisée par un écosystème constitué de différents acteurs du marché – tels que des fabricants, des chercheurs et des fournisseurs d'infrastructures – qui collaborent pour rendre les données accessibles et utilisables. Ces acteurs peuvent alors extraire de la valeur de ces données, en créant diverses applications susceptibles de faciliter grandement la vie au quotidien (gestion du trafic, optimisation des récoltes ou soins de santé à distance).

On estimait que l'économie fondée sur les données représentait 257 milliards d'euros dans l'UE en 2014, soit 1,85 % du PIB de l'Union[2]. En 2015, ce chiffre est passé à 272 milliards d'euros, soit 1,87 % du PIB de l'Union (croissance de 5,6 % en glissement annuel). Selon la même estimation, si les conditions-cadres politiques et juridiques relatives à l'économie fondée sur les données sont mises en place en temps voulu, cette économie devrait représenter 643 milliards d'euros d'ici à 2020, soit 3,17 % du PIB global de l'Union.

Le règlement général sur la protection des données (RGPD)[3], prévoit que, à partir de mai 2018, les 28 législations nationales qui coexistent actuellement seront remplacées par un ensemble unique de règles paneuropéennes. Le mécanisme de guichet unique[4] nouvellement créé prévoit qu'une autorité de contrôle unique est chargée du contrôle des opérations de traitement de données transfrontalier effectuées par une entreprise dans l'UE. Il est garanti que les nouvelles règles seront interprétées de manière cohérente. En

---

1 L'économie fondée sur les données mesure l'incidence globale du marché des données – c'est-à-dire le marché sur lequel les données numériques s'échangent sous forme de produits ou services dérivés de données brutes – sur l'économie dans son ensemble. Elle englobe la production, la collecte, le stockage, le traitement, la distribution, l'analyse, l'élaboration, la fourniture et l'exploitation des données grâce aux technologies numériques (European Data Market study, SMART 2013/0063, IDC, 2016).

2 European Data Market study, SMART 2013/0063, IDC, 2016

3 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 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, et abrogeant la directive 95/56/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

4 Article 56 du RGPD.

particulier, dans un contexte transfrontalier, lorsque plusieurs autorités de contrôle nationales sont concernées, une décision unique sera adoptée pour faire en sorte que les problèmes communs soient réglés par des solutions communes. En outre, le RGPD établit une égalité de traitement entre les entreprises de l'UE et les entreprises étrangères dans la mesure où les entreprises établies hors de l'UE devront appliquer les mêmes règles que les entreprises européennes si elles offrent des biens et des services ou surveillent le comportement de personnes dans l'UE. Les opérateurs commerciaux de l'UE comme ceux des pays tiers ne pourront que bénéficier d'une confiance accrue des consommateurs.

La directive «vie privée et communications électroniques» concerne la confidentialité des services de communications électroniques en Europe. Le réexamen de cette directive, qui a débouché sur une proposition de règlement présentée parallèlement à la présente communication[5], vise à garantir un niveau élevé de protection, en parfaite cohérence avec le RGPD. L'existence de règles strictes en matière de protection des données permettra de susciter la confiance nécessaire pour que l'économie numérique se développe dans l'ensemble du marché intérieur.

Comme l'a souligné le président Juncker dans son discours sur l'état de l'Union prononcé le 14 septembre 2016, «*[Ê]tre européen, c'est avoir le droit de voir ses données à caractère personnel protégées par une législation forte, une législation européenne. Car les Européens n'aiment pas que des drones planent au-dessus de leur tête pour enregistrer leur moindre geste, ni que des entreprises consignent chacun de leurs clics de souris. C'est pourquoi le Parlement, le Conseil et la Commission se sont entendus en mai dernier sur un règlement européen commun sur la protection des données. Cette législation européenne stricte s'applique aux entreprises, où qu'elles se trouvent, à chaque fois qu'elles traitent nos données. Car en Europe, la vie privée n'est pas un vain mot. C'est une question de dignité humaine*.»

Dans sa communication de 2012 intitulée «Protection de la vie privée dans un monde en réseau – Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle»[6] comme dans sa communication de 2014 intitulée «Vers une économie de la donnée prospère»[7], la Commission reconnaissait que des règles modernes et cohérentes dans l'ensemble de l'UE s'imposaient pour que les données puissent circuler librement d'un État membre à l'autre, que l'économie numérique européenne avait été lente à embrasser la révolution des données par rapport aux États-Unis et qu'elle ne disposait pas d'une capacité industrielle comparable. En conclusion, elle constatait que l'absence d'environnement juridique adapté aux échanges de données dans l'UE risquait de restreindre l'accès aux grands ensembles de données, de créer des barrières à l'entrée pour les nouveaux venus sur le marché et de freiner l'innovation.

Des **restrictions** injustifiées **à la libre circulation des données** sont susceptibles d'entraver le développement de l'économie fondée sur les données. Ces restrictions résultent des exigences imposées par les autorités publiques quant à la localisation des données à des fins de stockage ou de traitement. La question de la libre circulation des

5 COM(2017) 10 final.

6 COM(2012) 9.

7 COM(2014) 442.

données concerne tous les types de données: les entreprises et les acteurs de l'économie fondée sur les données travaillent avec des données industrielles et produites par des machines, à caractère personnel ou non, ainsi qu'avec des données générées par une action humaine. Dans sa stratégie relative au marché unique numérique, la Commission a annoncé qu'elle proposerait une initiative visant à lutter contre les restrictions à la libre circulation des données motivée par des raisons autres que la protection des données à caractère personnel au sein de l'UE et contre les restrictions injustifiées quant à la localisation des données à des fins de stockage ou de traitement. Au nombre de ces restrictions figurent des actes juridiques adoptés par les États membres ainsi que des règles et pratiques administratives d'effet équivalent. Leur nombre tend à augmenter avec la croissance de l'économie fondée sur les données, ce qui suscite des incertitudes quant aux possibilités de localisation du stockage ou du traitement des données. Tous les secteurs de l'économie et les organisations du secteur public comme celles du secteur privé risquent d'en pâtir, car cela pourrait rendre plus difficiles d'accès les services de données plus innovants et/ou moins onéreux. Les restrictions injustifiées quant à la localisation des données restreignent la liberté de prestation de services et la liberté d'établissement inscrites dans le traité et enfreignent également le droit dérivé applicable. Cela risque d'entraîner un morcellement du marché, de faire baisser la qualité du service pour les utilisateurs et de diminuer la compétitivité des prestataires de services de données, notamment les plus petits.

La question des exigences injustifiées en matière de localisation des données fait également partie des thèmes abordés dans les discussions entre l'UE et ses partenaires commerciaux, compte tenu de l'importance croissante des données et des services de données dans l'économie mondiale et des attitudes potentielles des pays tiers à cet égard. Les règles de l'UE en matière de protection des données ne peuvent pas faire l'objet de négociations dans le cadre d'un accord de libre-échange. Comme cela est expliqué dans la communication «Échange et protection de données à caractère personnel à l'ère de la mondialisation»[8], les dialogues relatifs à la protection des données doivent suivre une voie distincte des négociations commerciales avec les pays tiers. En outre, conformément à la communication «Le commerce pour tous»[9], la Commission s'efforcera d'utiliser les accords de libre-échange pour fixer des règles pour le commerce électronique et les flux de données transfrontières et s'attaquer à de nouvelles formes de protectionnisme numérique, dans le plein respect et sans préjudice des règles de l'UE sur la protection des données.

Par ailleurs, alors que la transformation induite par les données touche tous les secteurs de l'économie et de la société, des volumes toujours croissants de données sont produits par des machines, des capteurs ou des procédés fondés sur des technologies émergentes, telles que l'internet des objets, les usines du futur et les systèmes connectés autonomes. Désormais, c'est la connectivité qui change la manière d'accéder aux données: celles qui étaient auparavant accessibles via des connexions physiques le sont maintenant à distance. On commence à peine à prendre conscience de l'immense diversité des types et des sources de données et des très nombreuses possibilités d'application des connaissances obtenues grâce à l'analyse de ces données à une série de domaines, notamment le développement des politiques publiques. Pour profiter de ces possibilités,

[8] COM(2017) 7.

[9] COM(2015) 497.

les acteurs publics et privés du marché des données doivent avoir accès à des ensembles de données vastes et diversifiés. Les questions d'accès et de transfert en ce qui concerne les données produites par ces processus et machines revêtent donc une importance capitale pour l'apparition d'une économie fondée sur les données et doivent faire l'objet d'une évaluation approfondie.

Au nombre des nouveaux problèmes qui vont se poser figurent l'application des règles relatives à la responsabilité pour tout dommage résultant d'un dispositif connecté ou robot défectueux ainsi que la portabilité et l'interopérabilité des données. Dans le contexte des nouvelles technologies telles que l'internet des objets ou la robotique, il existe des interdépendances complexes et sophistiquées à la fois entre les produits (sur la base des matériels et logiciels) et entre les différents dispositifs interconnectés. Des problèmes d'un type nouveau peuvent également se poser avec les machines autonomes qui, en cas de comportement imprévu et non désiré, pourraient causer des dommages à des personnes et des biens. Ces facteurs peuvent être à l'origine d'une insécurité juridique en ce qui concerne l'application du cadre existant relatif à la responsabilité et à la sécurité.

Dans sa stratégie pour un marché unique numérique, la Commission a annoncé que son objectif était de créer un cadre juridique et politique clair et adapté pour l'économie fondée sur les données, en supprimant les entraves qui s'opposent encore à la libre circulation des données et en dissipant l'insécurité juridique créée par les nouvelles technologies liées aux données. La présente communication vise aussi à accroître l'accessibilité et l'utilisation des données, à promouvoir de nouveaux modèles économiques dans le secteur des données et à améliorer les conditions d'accès aux données et le développement de l'analyse de ces dernières dans l'UE. À cette fin, la Commission propose des axes de discussion ciblés en vue de créer une économie européenne fondée sur les données.

Elle examine dès lors les questions suivantes: libre circulation des données; accès et transfert en ce qui concerne les données produites par des machines; responsabilité et sécurité dans le contexte des technologies émergentes et portabilité des données à caractère non personnel, interopérabilité et normes. La présente communication contient aussi des propositions pour la mise à l'épreuve de solutions réglementaires communes en situation réelle.

La Commission va engager un vaste dialogue avec les parties prenantes sur les questions évoquées dans la présente communication. La première étape de ce dialogue consiste en une consultation publique lancée parallèlement au paquet de mesures sur l'économie fondée sur les données[10].

2. LIBRE CIRCULATION DES DONNEES

Pour que l'économie fondée sur les données soit dynamique et fonctionne bien, il faut que la circulation des données au sein du marché intérieur soit possible et qu'elle soit protégée. Dans un contexte technologique en évolution rapide, la sécurité et la fiabilité de la libre circulation des données sont essentielles pour la protection des quatre libertés

[10] https://ec.europa.eu/digital-single-market/news-redirect/52039

fondamentales du marché unique de l'Union européenne, inscrites dans les traités (liberté de circulation des biens, des travailleurs, des services et des capitaux). Les services de données connaissent une croissance rapide dans l'UE et dans le monde. L'existence d'un marché unique efficace et sans entraves dans ce secteur offrirait des possibilités considérables en matière de croissance et de création d'emplois.

La croissance et l'innovation dans l'économie fondée sur les données et la mise en œuvre de services publics transfrontaliers peuvent être compromises par des entraves à la libre circulation des données dans l'UE, telles que des exigences injustifiées en matière de localisation des données imposées par les pouvoirs publics. Les mesures relatives à la localisation des données réintroduisent en fait des «contrôles aux frontières» numériques[11]. Elles vont des exigences des autorités de contrôle, qui obligent les prestataires de services financiers à stocker localement leurs données, à des réglementations draconiennes qui imposent le stockage local des informations archivées produites par le secteur public, quel qu'en soit le caractère sensible, en passant par l'application de règles relatives au secret professionnel qui impliquent le stockage ou le traitement local des données.

Les préoccupations relatives au respect de la vie privée sont légitimes mais elles ne devraient pas être utilisées par les pouvoirs publics comme une raison suffisante pour restreindre la libre circulation des données de manière injustifiée. Comme indiqué ci-dessus, le RGPD prévoit un ensemble unique de règles assurant un niveau élevé de protection des données à caractère personnel pour l'ensemble de l'UE. Il renforce la confiance des consommateurs dans les services en ligne et garantit une application uniforme des règles dans tous les États membres en confortant les autorités nationales chargées de la protection des données. Le RGPD favorise la confiance nécessaire dans le traitement des données et constitue le socle de la libre circulation des données à caractère personnel dans l'UE. Il interdit les entraves à la libre circulation des données à caractère personnel dans l'Union lorsqu'elles sont fondées sur des motifs liés à la protection de ces données[12]. Toutefois, il ne s'applique pas aux obstacles relevant de considérations autres que la protection des données à caractère personnel, telles que la fiscalité ou la législation comptable. En outre, les données à caractère non personnel, c'est-à-dire les données ne se rapportant pas à une personne physique identifiée ou identifiable[13], sont exclues du champ d'application du RGPD. Il peut s'agir par exemple de données à caractère non personnel produites par des machines.

Les entraves quant à la localisation des données peuvent résulter de la réglementation ou d'orientations ou pratiques administratives qui requièrent que le stockage ou le traitement

---

11 OCDE, «Emerging Policy Issues: Localisation Barriers to Trade», 2015 et travaux en cours.

12 Article 1er, paragraphe 3. Ainsi, une adresse IP dynamique enregistrée par un fournisseur de services de médias en ligne à l'occasion de la consultation par une personne d'un site internet que ce fournisseur rend accessible au public constitue, à l'égard dudit fournisseur, une donnée à caractère personnel, lorsqu'il dispose de moyens légaux lui permettant de faire identifier la personne concernée grâce aux informations supplémentaires dont dispose le fournisseur d'accès à internet sur cette personne. Voir l'arrêt dans l'affaire C-582/14, Breyer, ECLI:EU:C:2016:779, point 49.

13 Définie à l'article 4, paragraphe 1, du RGPD.

de données[14] sous un format électronique[15] soit limité à une zone géographique ou à un territoire particulier. Parfois, ces restrictions sont imposées par des États membres qui pensent que les autorités de contrôle pourront ainsi examiner plus facilement les données stockées localement. La localisation tient aussi lieu d'assurance en ce qui concerne la protection de la vie privée, l'audit et le contrôle de l'application de la législation, ainsi que la sécurité des données. Dans la pratique, toutefois, ces mesures contribuent rarement aux objectifs qu'elles visent à atteindre.

Indépendamment de la localisation physique des données, la sécurité de l'information dépend de facteurs très divers, tels que le maintien de la confidentialité et de l'intégrité des données lorsque celles-ci sont disponibles en dehors des installations de stockage. À cet égard, la sécurité du stockage et du traitement des données est bien mieux assurée par les bonnes pratiques de gestion les plus perfectionnées dans le domaine des TIC, appliquées à une échelle largement supérieure à celle des systèmes individuels, que par des restrictions relatives à la localisation. Par exemple, pour protéger les données contre les catastrophes naturelles ou les cyberattaques localisées, les installations de stockage situées dans différents État membres peuvent assurer des sauvegardes mutuelles et avoir recours aux mesures techniques et organisationnelles prévues dans la directive sur la sécurité des réseaux et des systèmes d'information[16] (la directive SRI). En outre, un renforcement de la coopération entre autorités nationales, ou entre ces autorités et le secteur privé, permettrait, bien mieux que des restrictions relatives à la localisation, d'assurer la disponibilité de données à des fins de réglementation ou de contrôle, disponibilité qui n'est nullement remise en question. De fait, dans un secteur caractérisé par une coopération étroite entre les autorités de contrôle tel que celui des services financiers, les exigences en matière de localisation des données pourraient se révéler contre-productives[17].

Néanmoins, les exigences relatives à la localisation des données peuvent être justifiées et proportionnées dans certains contextes ou en ce qui concerne certaines données. C'est notamment le cas avant que ne soient mis en place des accords de coopération transfrontaliers, visant par exemple à garantir la sécurisation du traitement de certaines données relatives aux infrastructures énergétiques critiques, ou la disponibilité de preuves électroniques (sous forme de copies localisées d'ensembles de données par exemple) pour les autorités répressives, ou le stockage local des données détenues dans certains registres publics.

Malheureusement, en Europe comme ailleurs dans le monde, la tendance est à une localisation des données accrue, cette approche reposant souvent sur la conception

[14] Données détenues par le secteur privé comme par le secteur public

[15] Y compris les copies des ensembles de données

[16] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union (JO L 194 du 19.7.2016, p. 1).

[17] Un certain nombre de dispositions de l'UE concernant les services financiers et le système européen de surveillance financière exigent que les autorités de contrôle aient accès aux données relatives aux transactions et aux établissements financiers en tout point du territoire de l'UE. Les exigences relatives au stockage de données sur un territoire national particulier, ou celles qui soumettent l'accès des autorités de contrôle à des procédures administratives, pourraient restreindre l'accès de ces autorités à des données qui leur sont indispensables pour l'exécution de leur mandat.

erronée selon laquelle les services localisés sont automatiquement plus sûrs que les services transfrontaliers. De surcroît, l'absence de règles transparentes et l'importance accordée à la nécessité de localiser les données influencent fortement le marché des services de données. Cela peut limiter l'accès des entreprises et des organisations du secteur public aux services de données plus innovants ou moins onéreux, ou obliger les entreprises qui ont des activités transfrontalières à trouver des solutions pour disposer de capacités de stockage et de traitement supplémentaires. Cela pourrait aussi empêcher les prestataires de services fondés sur des données, en particulier les start-ups et les PME, de développer leurs activités, d'entrer sur de nouveaux marchés (par exemple, parce qu'ils doivent investir dans des centres de données dans 28 États membres) ou de centraliser des capacités en matière de données et d'analyse pour mettre au point de nouveaux produits et services.

Actuellement, 84 % de la demande finale de «services liés aux TIC» (conseil, hébergement, développement) est satisfaite par le marché intérieur de l'UE. Si la disparition des restrictions en matière de localisation des données pouvait également faciliter le fonctionnement de ces services par-delà les frontières intérieures de l'UE, la hausse du PIB qui en résulterait, due aux économies de coûts et aux gains d'efficacité[18], pourrait atteindre 8 milliards d'EUR par an.

La localisation des données entrave en outre la généralisation du stockage et de l'informatique dans le nuage, ce qui pourrait avoir des conséquences sociétales d'une plus grande ampleur. En effet, une utilisation plus efficace des ressources informatiques pourrait permettre une diminution nette de 30 % de la consommation d'énergie et des émissions de carbone. Une petite entreprise pourrait réduire sa consommation énergétique et ses émissions de carbone de plus de 90% en faisant fonctionner les applications nécessaires à son activité dans le nuage plutôt que sur sa propre infrastructure. Le marché mondial des centres de données économes en énergie devrait représenter près de 90 milliards d'euros d'ici à la fin de 2020. Un marché des services de données morcelé empêcherait les services plus efficaces sur le plan énergétique de se développer pleinement et compromettrait aussi la volonté d'investir.

Pour remédier aux problèmes et aux restrictions énumérés ci-dessus et réaliser tout le potentiel de l'économie européenne fondée sur les données, toute action des États membres ayant une incidence sur le stockage ou le traitement de données doit s'inspirer d'un «**principe de libre circulation des données au sein de l'UE**», corollaire des obligations qui incombent aux États membres en vertu des dispositions du traité et de la législation dérivée relatives à la libre circulation des services et à la liberté d'établissement. Toute restriction, nouvelle ou existante, en matière de localisation des données, doit pouvoir être dûment justifiée en vertu du traité et de la législation secondaire et doit constituer un moyen approprié et proportionné d'atteindre un objectif essentiel d'intérêt général tel que la sécurité publique[19].

---

[18] «Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States», ECIPE, 2016, calcul fondé sur une pression concurrentielle accrue dans le cadre d'un marché unique numérique «industriel» où la transparence des prix est totale.

[19] Compte tenu du fait que les dérogations au traité doivent être interprétées de manière restrictive. Parmi ces actes législatifs pertinents figurent le RGPD, la directive 2000/31/CE (directive sur le commerce électronique), la directive 2006/123/CE (la directive «Services») et, en ce qui concerne les projets de réglementations techniques et de règles relatives aux services de la société de l'information, la directive 2015/1535 (directive sur la transparence).

Le principe de la libre circulation des données à caractère personnel[20], inscrit dans le droit primaire et le droit dérivé, devrait aussi s'appliquer dans les cas où le RGPD autorise les États membres à réglementer des questions spécifiques. Les États membres devraient être encouragés à ne pas utiliser les «clauses d'ouverture» prévues par le RGPD pour restreindre davantage la libre circulation des données.

Dans ses conclusions du 15 décembre 2016, le Conseil européen a demandé la levée des obstacles qui subsistent au sein du marché unique, y compris ceux qui entravent la libre circulation des données[21].

Afin de mettre en œuvre le principe de la libre circulation des données, la Commission entend prendre les deux mesures suivantes:

- après la publication de la présente communication, elle engagera des dialogues structurés avec les États membres et d'autres parties prenantes en vue d'examiner les justifications et la proportionnalité des restrictions en matière de localisation des données, en prenant comme point de départ les restrictions qu'elle a recensées jusqu'à présent;

- en se fondant sur les résultats des dialogues et du processus de collecte d'éléments supplémentaires sur l'ampleur et la nature des restrictions en matière de localisation et sur leur incidence, en particulier sur les PME et les start-ups, processus qui se poursuit dans le cadre de la consultation publique, elle lancera également, s'il y a lieu, des procédures d'infraction portant sur les mesures injustifiées ou disproportionnées en matière de localisation des données et prendra, si nécessaire, d'autres initiatives sur la libre circulation des données. Toute action de suivi entreprise à cet égard sera conforme aux principes d'une meilleure réglementation.

3. ACCES AUX DONNEES ET TRANSFERT

Des volumes toujours croissants de données sont produits par des machines ou des processus fondés sur des technologies émergentes, tels que l'internet des objets. Ces données constituent une composante de plus en plus importante des nouveaux services innovants qui permettent d'améliorer les produits ou processus de production et de fournir une assistance à la prise de décision.

La diversité des données produites par ces machines ou processus offre aux acteurs du marché des données des perspectives très intéressantes en matière d'innovation et d'application des connaissances acquises grâce à l'analyse de ces données. Ainsi, les données recueillies par les capteurs utilisés dans les exploitations agricoles modernes pourraient être exploitées pour créer une application permettant d'optimiser les récoltes,

[20] La libre circulation des données à caractère personnel est prévue par l'article 16 du traité sur le fonctionnement de l'Union européenne, les règles relatives à la libre circulation des données à caractère personnel sont énoncées dans la législation actuelle et en projet de l'Union en matière de protection des données. L'article 1er, paragraphe 3, du règlement général sur la protection des données dispose que: «La libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.»

[21] http://data.consilium.europa.eu/doc/document/ST-34-2016-INIT/fr/pdf

et les données produites par les capteurs installés sur les feux de circulation routière pourraient servir à mettre au point une application de gestion de la circulation ou d'optimisation des trajets.

Pour tirer un maximum de valeur de ce type de données, les acteurs du marché doivent avoir accès à des ensembles de données vastes et diversifiés. Toutefois, il sera difficile d'y parvenir si les producteurs des données n'y donnent pas accès et que les données sont par conséquent analysées de manière isolée. Les questions d'accès et de transfert en ce qui concerne les données brutes (c'est-à-dire ni traitées ni modifiées depuis leur enregistrement) produites par ces processus ou machines revêtent donc une importance capitale pour l'apparition d'une économie fondée sur les données et doivent faire l'objet d'une évaluation approfondie.

La question de l'accès aux données produites par les machines est en cours d'étude dans plusieurs secteurs, tels que les transports, les marchés de l'énergie, les environnements de vie intelligents et les soins de santé.

Avant d'examiner la situation actuelle en ce qui concerne l'accès aux données dans l'UE, il est important de préciser le type de données considérées dans ce contexte.

3.1. Type de données considérées

Généralement, les données peuvent être à caractère personnel ou non personnel. Par exemple, les données produites par des capteurs de température domestiques peuvent être à caractère personnel si elles sont liées à une personne physique vivante, alors que les données concernant l'humidité des sols sont à caractère non personnel. L'anonymisation permet de transformer les données à caractère personnel en données à caractère non personnel. Lorsque des données peuvent être considérées comme étant à caractère personnel[22], le cadre de la protection des données, en particulier le RGPD, sera applicable.

Les données produites par des machines sont générées sans intervention humaine directe, par des processus informatiques, des applications ou des services, ou par des capteurs qui traitent des informations reçues d'équipements, de logiciels ou de dispositifs virtuels ou réels.

Les données produites par des machines peuvent être à caractère personnel ou non personnel. Lorsqu'une donnée produite par une machine permet d'identifier une personne physique, elle est considérée comme une donnée à caractère personnel et est par conséquent soumise à toutes les règles relatives aux données à caractère personnel jusqu'à son anonymisation complète (par exemple, données de localisation des applications mobiles).

La libre circulation des données et les questions émergentes en matière d'accès et de transfert ont un dénominateur commun, à savoir que les entreprises et acteurs de l'économie fondée sur les données ont vocation à traiter des données à caractère personnel aussi bien que non personnel, et que les flux et les ensembles de données contiendront régulièrement les deux types de données. Toute mesure politique adoptée

[22] Selon la définition de l'article 4, paragraphe 1, du RGPD.

devra tenir compte de cette réalité économique et du cadre juridique relatif à la protection des données à caractère personnel, tout en respectant les droits fondamentaux de la personne.

3.2. Accès limité aux données

Pour pouvoir évaluer le problème qui commence à se faire jour, il faut d'abord analyser la manière dont les entreprises et les autres acteurs peuvent avoir accès aux ensembles de données vastes et diversifiées qui sont nécessaires dans l'économie fondée sur les données.

Selon les éléments disponibles[23], les entreprises qui détiennent de grandes quantités de données ont généralement tendance à utiliser essentiellement des capacités d'analyse internes. Dans la plupart des cas, les données sont produites et analysées par la même entreprise et, même lorsque l'analyse est sous-traitée, les données pourraient ne pas être réutilisées. En outre, il arrive aussi que les fabricants, les entreprises proposant des services ou d'autres acteurs du marché qui détiennent des données produites par leurs machines ou leurs produits conservent ces données pour eux-mêmes, ce qui restreint potentiellement la réutilisation sur les marchés en aval. De nombreuses entreprises ne disposent pas d'interfaces de programmation d'application (API; interfaces précisant la façon dont différentes applications doivent interagir entre elles)[24] ou n'ont pas la possibilité d'en utiliser, alors que ces interfaces peuvent constituer des points d'entrée sûrs pour de nouvelles utilisations innovantes de données détenues par les entreprises.

Par conséquent, les échanges de données restent, dans l'ensemble, très limités. Des marchés de données commencent à apparaître, mais leur utilisation n'est pas très répandue. Il arrive que les entreprises ne disposent pas des outils et des compétences appropriés pour quantifier la valeur économique de leurs données et qu'elles craignent de perdre ou de compromettre leur avantage concurrentiel à partir du moment où leurs concurrents ont accès aux données.

3.3. Données brutes produites par des machines: situation juridique au niveau de l'UE et au niveau national

Les données brutes produites par des machines ne sont pas protégées par les droits de propriété intellectuelle existants puisqu'elles ne sont pas considérées comme étant le fruit d'une création intellectuelle et/ou comme présentant une quelconque originalité. Le droit *sui generis* prévu par la directive sur les bases de données (96/9/CE) — qui donne aux fabricants de bases de données le droit d'empêcher l'extraction et/ou la réutilisation de la totalité ou d'une partie substantielle du contenu d'une base de données n'accorde une protection que si l'obtention, la vérification ou la présentation de ce contenu attestent un investissement substantiel. La directive 2016/943/UE sur les secrets d'affaires, adoptée récemment, qui doit être transposée dans les législations nationales avant juin 2018,

23 IDC, European Data Market Study, premier rapport intermédiaire, 2016; Impact Assessment support study on emerging issues of data ownership, interoperability, (re)usability and access to data, and liability, premier rapport intermédiaire, 2016; DG Connect high-level conference, 17 octobre 2016

24 Par exemple, https://developer.lufthansa.com/; https://data.sncf.com/api; https://api.tfl.gov.uk/; https://dev.blablacar.com/

garantira la protection des secrets d'affaires contre l'obtention, l'utilisation et la divulgation illicites. Pour que des données puissent être considérées comme des «secrets d'affaires», elles doivent avoir fait l'objet de dispositions destinées à les garder secrètes car elles représentent le capital intellectuel de l'entreprise.

Il est prévu, dans le droit de différents États membres, que les données ne peuvent faire l'objet d'une action en justice que lorsqu'elles satisfont à des conditions particulières pour être considérées, par exemple, comme un droit de propriété intellectuelle, un droit protégeant une base de données ou un secret d'affaires. Toutefois, au niveau de l'UE, les données brutes produites par des machines en tant que telles ne satisferaient généralement pas aux conditions pertinentes.

Par conséquent, il n'existe pas actuellement, au niveau national ou au niveau de l'Union, de cadre politique complet relatif aux données brutes produites par des machines qui ne sont pas considérées comme des données à caractère personnel ou relatif aux conditions de leur exploitation et de leur négociabilité. Les solutions appliquées sont dans une large mesure de nature contractuelle. Il pourrait être suffisant d'avoir recours aux dispositions existantes du droit général des contrats et des instruments du droit de la concurrence disponibles dans l'Union. On pourrait également envisager de conclure des accords volontaires ou des accords-cadres couvrant certains secteurs. Toutefois, lorsque le pouvoir de négociation des différents acteurs du marché est inégal, les solutions fondées sur le marché risquent de ne pas suffire, à elles seules, pour garantir des résultats équitables et favorables à l'innovation, faciliter l'accès au marché de nouveaux venus et éviter les situations de blocage.

3.4. La situation en pratique

Dans certains cas, les fabricants ou les prestataires de services peuvent devenir les propriétaires «de fait» des données que leurs machines ou leurs processus génèrent, même si ces machines sont la propriété de l'utilisateur. Le contrôle «de fait» de ces données peut représenter un facteur de différenciation et un avantage concurrentiel pour les fabricants. Toutefois, cela peut être problématique car souvent le fabricant empêche l'utilisateur d'autoriser un tiers à utiliser les données.

Les différents acteurs qui exercent un contrôle sur les données, selon les particularités des marchés, peuvent donc tirer avantage des lacunes du cadre réglementaire ou de l'insécurité juridique décrite ci-dessus, en imposant aux utilisateurs des clauses contractuelles abusives ou en ayant recours à des moyens techniques tels que des formats propriétaires ou le cryptage. Si plusieurs États membres ont étendu aux transactions entre entreprises le champ d'application de la directive concernant les clauses abusives dans les contrats conclus avec les consommateurs, ce n'est pas le cas de tous. De ce fait, des utilisateurs et des entreprises pourraient, par exemple, se retrouver «prisonniers» d'accords exclusifs d'exploitation de données. Il est possible que des systèmes volontaires de partage de données apparaissent, mais la négociation de contrats de ce type pourrait entraîner des coûts de transaction élevés pour les parties les plus faibles, lorsque la négociation est déséquilibrée ou en raison des coûts considérables liés au recours à des experts juridiques.

3.5. Un futur cadre réglementaire de l'UE en matière d'accès aux données

Certains États membres étudient actuellement la question de l'accès aux données produites par les machines, un aspect qu'ils pourraient décider de réglementer eux-mêmes. Une absence de coordination risque de créer un morcellement et nuirait au développement de l'économie fondée sur les données dans l'UE ainsi qu'au fonctionnement des services de données et technologies transfrontaliers dans le marché intérieur.

La Commission entend donc engager un dialogue avec les États membres et les autres parties prenantes afin d'étudier la possibilité d'un futur cadre réglementaire de l'UE relatif à l'accès aux données. Selon elle, ce dialogue devrait s'articuler autour des moyens les plus efficaces de parvenir aux objectifs suivants:

- **Améliorer l'accès aux données anonymes produites par des machines:** le partage, la réutilisation et l'agrégation font des données produites par des machines une source de création de valeur, d'innovation et de diversité des modèles d'entreprise[25].

- **Faciliter et encourager le partage de ces données**: toute éventuelle solution future devrait encourager l'accès effectif aux données, en tenant compte, par exemple, des différences potentielles dans le rapport de forces entre les acteurs du marché.

- **Protéger les investissements et les actifs:** toute éventuelle solution future devrait aussi tenir compte des intérêts légitimes des acteurs du marché qui investissent dans le développement de produits, garantir un juste retour sur leurs investissements et contribuer ainsi à l'innovation. Elle devrait, dans le même temps, assurer une répartition équitable des avantages entre les détenteurs de données[26], les responsables du traitement et les fournisseurs d'application dans les chaînes de valeur.

- **Éviter la divulgation de données confidentielles:** il faudrait que les solutions futures envisagées atténuent les risques de divulgation de données confidentielles, notamment aux concurrents existants ou potentiels. Elles devraient aussi, à cet égard, permettre une classification correcte des données avant que la possibilité de partager ou non certaines données ne soit évaluée.

- **Limiter les blocages:** il convient de tenir compte du déséquilibre entre le pouvoir de négociation des entreprises et celui des particuliers. Il faut éviter les situations de blocage, notamment pour les PME, les start-ups et les particuliers.

Dans le cadre de ses dialogues avec les parties prenantes, la Commission entend examiner les possibilités suivantes, caractérisées par différents niveaux d'intervention, pour régler le problème de l'accès aux données produites par des machines:

---

[25] Lorsqu'il s'agit de données à caractère personnel, c'est le RGPD qui s'applique.

[26] L'entité qui gère et conserve, dans la pratique, les données produites par les machines.

- **Orientations concernant la manière d'inciter les entreprises à partager les données:** pour atténuer les effets des divergences entre réglementations nationales et procurer une sécurité juridique accrue aux entreprises, la Commission pourrait formuler des orientations sur la manière d'aborder les droits au contrôle des données à caractère non personnel dans les contrats. Ces orientations seront fondées sur la législation existante et notamment sur les exigences de transparence et d'équité fixées par la législation de l'UE dans le domaine du marketing et de la protection des consommateurs, la directive sur les secrets d'affaires et la législation sur le droit d'auteur, en particulier la directive sur les bases de données. La Commission compte lancer une évaluation de la directive sur les bases de données en 2017.

- **Stimuler le développement de solutions techniques pour la fiabilité de l'identification et de l'échange de données:** la traçabilité et l'identification claire des sources de données sont des conditions préalables à un contrôle effectif des données sur le marché. Pour établir la confiance dans le système, il peut être nécessaire de définir des protocoles fiables et éventuellement normalisés pour l'identification continue des sources de données. Les interfaces de programmation d'application (API) peuvent aussi favoriser la création d'un écosystème de développeurs d'applications et d'algorithmes intéressés par les données détenues par les entreprises. Ces API peuvent aider les entreprises et les pouvoirs publics à identifier les différents types de réutilisation des données qu'elles détiennent et à en tirer profit. Il serait ainsi possible d'envisager une utilisation plus large d'API ouvertes, normalisées et bien documentées, grâce à des orientations techniques, y compris le recensement et la diffusion des meilleures pratiques à appliquer par les entreprises et les organismes du secteur public. Les options possibles seraient la mise à disposition de données dans des formats lisibles en machine et la fourniture des métadonnées associées.

- **Règles contractuelles par défaut**: ces règles par défaut pourraient consister en une solution équilibrée de référence pour les contrats portant sur les données, compte dûment tenu du bilan de qualité, actuellement en cours, de la directive concernant les clauses abusives dans les contrats. Elles pourraient être assorties d'un contrôle du caractère abusif des relations contractuelles interentreprises[27] qui permettrait d'invalider les clauses contractuelles qui s'écartent trop des règles par défaut. Elles pourraient également être complétées par une série de clauses contractuelles types conçues par les parties prenantes. Cette approche pourrait permettre d'aplanir les obstacles juridiques pour les petites entreprises et de réduire le déséquilibre entre les positions de négociation, tout en laissant une liberté contractuelle non négligeable.

- **Accès dans l'intérêt public et à des fins scientifiques:** il serait possible d'accorder aux pouvoirs publics l'accès aux données lorsque c'est dans l'«intérêt général» et que cela permettrait d'améliorer considérablement le fonctionnement du secteur public, par exemple dans le cas de l'accès des offices statistiques à des données commerciales, ou de l'optimisation des systèmes de gestion de la

[27]. En ce qui concerne le caractère abusif, le seuil de référence devrait être différent pour les contrats entre entreprises et ceux entre entreprises et consommateurs, de manière à tenir compte de la liberté contractuelle plus importante que laissent les relations entre entreprises.

circulation s'appuyant sur les données en temps réel provenant des voitures particulières. Accorder aux pouvoirs publics l'accès aux données contribuerait par exemple à alléger la charge des rapports statistiques qui pèse sur les opérateurs économiques. De la même manière, l'accès aux données provenant de différentes sources, ainsi que la possibilité de les combiner, sont essentiels à la recherche scientifique dans des domaines tels que les sciences médicales, sociales et environnementales.

- **Droit du producteur de données:** il serait possible d'accorder au «producteur de données», c'est-à-dire le propriétaire ou l'utilisateur à long terme du dispositif (le locataire), un droit d'utiliser et d'autoriser l'utilisation de données à caractère non personnel. Une telle approche aurait pour but de clarifier la situation et d'offrir un choix plus étendu au producteur de données, en donnant aux utilisateurs la possibilité d'utiliser leurs données, ce qui contribuerait à libérer les données produites par des machines. Il faudrait cependant préciser expressément les exceptions pertinentes, notamment en ce qui concerne la fourniture d'accès non exclusif aux données par le fabricant ou par les pouvoirs publics, par exemple pour des motifs liés à l'environnement ou à la gestion de la circulation. Pour ce qui est des données à caractère personnel, la personne concernée conserve le droit de retirer son consentement à tout moment après avoir autorisé l'utilisation. Avant que la réutilisation des données à caractère personnel soit autorisée par l'autre partie, ces données devraient impérativement être rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. En effet, le RGPD continue de s'appliquer à toutes les données à caractère personnel (qu'il s'agisse de données produites par des machines ou autres) jusqu'à l'anonymisation de ces données.

- **Accès moyennant rémunération:** il serait possible d'établir, pour les détenteurs de données tels que les fabricants, les prestataires de services ou des tiers, un cadre potentiellement fondé sur certains principes clés, telles que des conditions équitables, raisonnables et non discriminatoires (cadre «FRAND»), afin qu'ils puissent donner accès, moyennant rémunération, aux données qu'ils détiennent après anonymisation de ces dernières. Il convient de tenir compte des intérêts légitimes en cause ainsi que la nécessité de protéger les secrets d'affaires. Pour tenir compte des particularités de chaque secteur, il serait aussi possible d'envisager des régimes d'accès différents en fonction des secteurs et/ou modèles économiques. Par exemple, dans certains cas, la solution de l'accès ouvert (total ou partiel) aux données pourrait être privilégiée, à la fois pour les entreprises et pour la société.

La Commission consultera les parties prenantes sur les aspects évoqués ci-dessus, en vue de recueillir davantage d'éléments sur le fonctionnement des marchés de données par secteur et d'étudier les solutions possibles. Il est essentiel, dans ce contexte, d'engager un vaste débat au niveau macro pour examiner les solutions possibles et éviter les effets secondaires indésirables susceptibles de freiner l'innovation ou d'entraver la concurrence. En outre, des discussions sectorielles seront organisées avec les parties prenantes concernées de la chaîne de valeur des données.

4. RESPONSABILITE

Un autre problème qui se pose a trait à l'application, dans l'économie fondée sur les données, des règles actuellement en vigueur en matière de responsabilité pour ce qui est des produits et services fondés sur des technologies émergentes, telles que l'internet des objets, les usines du futur et les systèmes connectés autonomes. L'internet des objets est un réseau en expansion rapide, constitué d'objets du quotidien, tels que des montres, des voitures ou des thermostats, qui sont connectés à l'internet. Les systèmes connectés autonomes, tels que les véhicules sans chauffeur, agissent indépendamment de toute action humaine et sont capables de comprendre et d'interpréter leur environnement. Ces technologies émergentes utilisent des capteurs qui leur fournissent les nombreux types de données souvent nécessaires au fonctionnement du produit ou du service.

Toutes ces innovations sont susceptibles de contribuer à améliorer la sécurité et la qualité de vie mais on ne peut évidemment pas exclure la possibilité d'erreurs de conception, de dysfonctionnement ou de manipulation des dispositifs. Cela peut être dû à la transmission de données erronées par un capteur, par exemple en raison de défauts logiciels, de problèmes de connectivité ou d'utilisation incorrecte de l'appareil. Du fait de la nature de ces systèmes, il peut être difficile de déterminer l'origine exacte d'un problème qui cause des dommages, ce qui amène à se demander comment garantir la sécurité de ces systèmes pour les utilisateurs de manière à minimiser la survenue de dommages et, si des dommages se produisent, comment déterminer le responsable.

Il est donc capital, pour favoriser l'avènement d'une économie fondée sur les données, de donner des certitudes aux utilisateurs et aux fabricants en ce qui concerne leur responsabilité potentielle.

4.1. Règles de l'UE relatives à la responsabilité

En droit civil, on distingue généralement deux types de responsabilité civile: *la* responsabilité contractuelle, qui prévoit que la responsabilité des dommages causés découle de la relation contractuelle entre les parties; et la responsabilité extracontractuelle[28], où la responsabilité est établie hors contrat. La responsabilité du fait des produits défectueux constitue un des principaux exemples de responsabilité extracontractuelle. Au niveau de l'UE, la directive sur la responsabilité du fait des produits défectueux (85/374/CEE) établit le principe de la responsabilité objective, c'est-à-dire la responsabilité sans faute: lorsqu'un dommage est causé à un consommateur par un produit défectueux, le fabricant peut être responsable même s'il n'a commis ni négligence ni faute. Toutefois, l'application des dispositions de cette directive[29] peut être difficile ou source de confusion dans le contexte de l'internet des objets et des systèmes connectés autonomes (par exemple en robotique), pour les raisons suivantes: les caractéristiques de ces systèmes, par exemple une chaîne de valeur de produits ou services complexe, avec des interdépendances entre fournisseurs, fabricants et autres tiers; des incertitudes concernant la nature juridique des dispositifs de l'internet des

[28] Les règles de l'UE en matière de responsabilité ne concernent que la responsabilité extracontractuelle.

[29] D'autres actes législatifs relatifs à la sécurité des produits, tels que la directive sur les équipements radioélectriques (2014/53/UE), les règlements sur les dispositifs médicaux, la directive «Machines» (2006/42/CE) et la directive relative à la sécurité générale des produits (2001/95/CE) font référence à la responsabilité objective des fabricants en cas de produits défectueux.

objets, à savoir s'il s'agit de produits, de services ou de produits accompagnant la vente d'un service; et le caractère autonome de ces technologies.

La Commission a lancé un vaste exercice d'évaluation de l'application de la directive sur la responsabilité du fait des produits défectueux, visant à évaluer son fonctionnement global et à déterminer si ses règles, établies pour un environnement très différent, restent appropriées dans le contexte de technologies émergentes telles que l'internet des objets et les systèmes connectés autonomes.

4.2. Mesures envisageables

L'objectif de la Commission est d'améliorer la sécurité juridique en matière de responsabilité dans le contexte des technologies émergentes et, partant, de créer des conditions favorables à l'innovation. Outre le statu quo[30], différentes approches sont envisageables, à savoir:

- **Approches fondées sur la production de risques et la gestion des risques**: selon ce type d'approche, la responsabilité pourrait être imputée aux acteurs du marché qui génèrent un risque majeur pour d'autres ou aux acteurs qui sont les mieux placés pour réduire au minimum ce risque ou l'éviter.

- **Régimes d'assurance volontaire ou obligatoire**: les approches décrites ci-dessus pourraient également être complétées par des régimes d'assurance qui dédommageraient les parties ayant subi le préjudice (c'est-à-dire les consommateurs). Ces régimes devraient garantir la protection juridique des investissements effectués par des entreprises tout en offrant aux victimes une compensation équitable ou une assurance appropriée en cas de préjudice.

Ils devraient tenir compte des actions des utilisateurs de la technologie en cause et définir plus précisément le rôle de ces derniers.

La Commission consultera les parties prenantes en ce qui concerne le caractère adéquat des règles existantes de l'UE en matière de responsabilité dans le contexte de l'internet des objets et des systèmes connectés autonomes, et sur la façon de surmonter les difficultés qui se présentent actuellement pour l'imputation de cette responsabilité. Une consultation publique relative à l'évaluation globale de l'application de la directive sur la responsabilité du fait des produits défectueux est également menée en parallèle. La Commission en évaluera les résultats et examinera les futures actions possibles.

5. PORTABILITE, INTEROPERABILITE ET NORMES

Parmi les autres problématiques émergentes dans l'économie fondée sur les données figurent la portabilité des données à caractère non personnel, l'interopérabilité des services pour permettre l'échange des données et l'adoption de normes appropriées pour la mise en œuvre d'une véritable portabilité.

[30] La Commission pourrait publier des orientations sur l'application des règles de l'UE en matière de responsabilité dans le domaine de l'internet des objets et de la robotique.

5.1. Portabilité des données à caractère non personnel

La portabilité des données permet aux consommateurs et aux entreprises de transférer facilement leurs données d'un système à un autre. Dans l'économie fondée sur les données, elle est généralement associée à un faible coût de changement de fournisseur et, partant, à des obstacles à l'entrée peu élevés. Le RGPD conférera aux individus le droit de recevoir les données à caractère personnel fournies au prestataire de services dans un format structuré, couramment utilisé, lisible par machine et interopérable, et de les transmettre à un autre responsable du traitement[31].

En ce qui concerne les données à caractère non personnel, cependant, il n'existe actuellement aucune obligation de garantir ne serait-ce qu'un niveau minimal de portabilité des données, même pour des services en ligne dont l'utilisation est largement répandue tels que ceux des hébergeurs dans le nuage. Cela tient en partie au fait que les exigences applicables à la mise en œuvre de la portabilité des données peuvent être techniquement contraignantes et coûteuses, étant donné que différents fournisseurs du même service peuvent stocker des données de manière différente.

Une véritable portabilité des données à caractère non personnel devait aussi tenir compte de considérations plus générales en matière de gouvernance des données ayant trait à la transparence pour les utilisateurs, à la gestion de l'accès et à l'interopérabilité pour relier entre elles différentes plateformes de manière à stimuler l'innovation.

5.2. Interopérabilité

Les questions de portabilité des données sont souvent étroitement liées à l'interopérabilité des données, qui permet l'échange de données sans discontinuité entre de multiples services numériques et est facilitée par l'existence de spécifications techniques appropriées. La directive relative aux informations du secteur public et les documents d'orientation correspondants (y compris le cadre d'interopérabilité européen) soulignent combien il est important de disposer de métadonnées riches, normalisées et conformes à des vocabulaires établis pour faciliter la recherche et l'interopérabilité. La directive établissant une infrastructure d'information géographique dans la Communauté européenne (INSPIRE), ainsi que les règlements et orientations qui en découlent en ce qui concerne l'interopérabilité et les données et services de données géographiques, y compris les données d'observation fournies par des capteurs, sont actuellement applicables aux données géographiques du secteur public[32].

Dans le cas de plateformes en ligne, ces données facilitent non seulement le passage d'une plateforme à l'autre, mais aussi l'utilisation simultanée de plusieurs plateformes (dite «multihébergement», ainsi que la généralisation de l'échange de données entre plateformes, qui a le potentiel de renforcer l'innovation dans l'économie numérique.

[31] Article 20

[32] Les données produites par des machines sont des «données géographiques» dans la mesure où les capteurs transmettent généralement aussi leur position (localisation) directe ou indirecte en même temps que les valeurs mesurées.

5.3. Normes

Pour mettre en œuvre une véritable portabilité en respectant la neutralité technologique, il faut adopter des normes techniques appropriées afin de soutenir des politiques de portabilité efficaces. La Commission s'est engagée[33] à soutenir les normes appropriées afin d'améliorer l'interopérabilité, la portabilité et la sécurité des services d'informatique en nuage par une meilleure intégration des travaux des communautés «open source» dans le processus d'élaboration des normes au niveau européen. On peut citer, à titre d'exemple, la spécification TOSCA relative aux applications en nuage, destinée à améliorer la portabilité et la gestion opérationnelle des services et applications en nuage[34], et les spécifications et orientations techniques des règlements d'exécution INSPIRE[35].

5.4. Mesures envisageables

Pour régler les problèmes décrits ci-dessus, on peut envisager les mesures suivantes:

- **Élaborer des clauses contractuelles recommandées permettant de faciliter le changement de prestataire de services**: la portabilité des données et le changement de prestataire de services étant interdépendants, il pourrait être envisagé d'élaborer des clauses contractuelles type obligeant le prestataire de services à mettre en œuvre la portabilité des données des clients.

- **Introduire d'autres droits dans le domaine de la portabilité des données**: il serait possible d'introduire d'autres droits dans le domaine de la portabilité des données à caractère non personnel en se fondant sur le droit à la portabilité des données prévu par le RGPD et sur les règles proposées en matière de contrat de fourniture de contenu numérique, notamment pour couvrir les situations des relations interentreprises, tout en tenant dûment compte des résultats du bilan de qualité en cours sur les principaux instruments législatifs de l'UE dans le domaine du marketing et de la protection des consommateurs[36].

- **Tests sectoriels sur les normes**: des initiatives expérimentales sectorielles pourraient être envisagées pour mettre au point une approche solide des règles de portabilité codifiées par des normes. Elles pourraient, par exemple, prendre la forme d'une collaboration entre diverses parties prenantes dont les organismes de normalisation, les entreprises, la communauté technique et les pouvoirs publics.

La Commission consultera les parties prenantes sur ces sujets et déterminera par la suite s'il y a lieu de prendre des mesures supplémentaires, éventuellement sous la forme des actions évoquées ci-dessus, exécutées ensemble ou isolément.

[33] COM (2016) 176 final Priorités pour la normalisation en matière de TIC dans le marché unique numérique

[34] https://www.oasis-open.org/committees/tosca

[35] Législation INSPIRE: http://inspire.ec.europa.eu/inspire-legislation/26

[36] http://ec.europa.eu/consumers/consumer_rights/review/index_en.htm

6. EXPERIMENTATION ET ESSAIS

L'expérimentation joue un rôle important dans l'étude des nouveaux problèmes qui se poseront dans le contexte de l'économie fondée sur les données. La possibilité d'utiliser le financement d'Horizon 2020 pour soutenir ce type d'essais et d'expériences sera examinée.

Avant de parvenir à des conclusions sur l'applicabilité de solutions possibles pour l'accès aux données et la responsabilité, il convient d'organiser un essai spécifique pour mettre ces solutions à l'épreuve en situation réelle, en partenariat avec les parties prenantes. Il faut trouver une solution européenne qui repose sur la coopération et l'expérimentation entre les États membres.

Certains projets en matière de mobilité coopérative, connectée et automatisée[37] pourraient se prêter à une telle expérimentation, compte tenu de leur dimension transfrontalière.

Des projets visant à mettre au point des systèmes coopératifs et à promouvoir des niveaux d'automation supérieurs sont déjà en cours dans plusieurs États membres [38]. Ces projets permettent à des véhicules de se connecter entre eux et avec des éléments de l'infrastructure routière tels que les feux de signalisation et les panneaux routiers. En outre, la Commission entend collaborer avec un groupe d'États membres intéressés pour créer un cadre juridique d'essais en vue de mener des expériences fondées sur des règles harmonisées en matière d'accès aux données et de responsabilité. Pour permettre l'accès à un volume de données suffisamment élevé, les essais devraient être fondés sur la 5G, qui fonctionnera en coexistence continue avec les technologies déjà déployées, selon un principe de complémentarité[39].

Une autre expérience intéressante se déroulera dans le domaine géospatial, avec l'apparition d'un nouvel écosystème de données autour de Copernicus, le programme européen d'observation de la Terre qui est aussi le troisième plus grand fournisseur de données au monde. La Commission met actuellement au point des solutions en vue d'encourager le développement d'applications fondées sur le programme Copernicus et d'autres données géographiques, portant notamment sur les questions d'accès aux données, d'interopérabilité et de prévisibilité.

7. CONCLUSION

Pour créer une économie fondée sur les données, l'UE doit se doter d'un cadre politique permettant l'utilisation des données dans toute la chaîne de valeur à des fins scientifiques, sociétales et industrielles. À cette fin, la Commission va engager un vaste dialogue avec les parties prenantes sur les questions évoquées dans la présente communication. La première étape de ce dialogue consiste en une consultation publique. Les questions de l'accès aux données et de la responsabilité feront également l'objet

[37] Voir COM (2016) 766 du 30.11.2016.

[38] Voir COM(2016) 766, «Une stratégie européenne relative aux systèmes de transport intelligents coopératifs».

[39] Voir COM(2016) 588, «Un plan d'action pour la 5G en Europe».

d’expériences en situation réelle dans le domaine de la mobilité coopérative, connectée et automatisée.

En ce qui concerne la libre circulation des données, la Commission continuera à travailler sur ce sujet conformément à l’approche exposée ci-dessus, afin de mettre pleinement en œuvre le principe de la libre circulation des données au sein de l’UE, notamment, s’il y a lieu, en donnant la priorité aux mesures visant à faire appliquer la législation. Elle continuera aussi à suivre l’évolution de la situation et à recueillir davantage d’éléments et envisagera, si nécessaire, de prendre d’autres initiatives sur la libre circulation des données.

En fonction des résultats de son dialogue avec les parties prenantes, la Commission décidera également si des mesures supplémentaires sont nécessaires sur les nouveaux problèmes qui se posent et proposera des solutions en conséquence. À cet égard, l’expérimentation en situation réelle pourrait avoir un rôle à jouer.