N° 597

SÉNAT

SESSION ORDINAIRE DE 2022-2023

Enregistré à la Présidence du Sénat le 11 mai 2023

RAPPORT D'INFORMATION

FAIT

au nom de la commission des affaires européennes (1) sur la proposition de règlement du **Parlement européen** *et du* **Conseil** *fixant des* **règles harmonisées** *pour l'***équité** *de l'***accès** *aux* **données** *et de l'***utilisation** *des* **données** *(règlement sur les données) COM(2022) 68 final,*

Par Mme Florence BLATRIX CONTAT, M. André GATTOLIN
et Mme Catherine MORIN-DESAILLY,

Sénatrices et Sénateur

(1) Cette commission est composée de : M. Jean-François Rapin, *président ;* MM. Alain Cadec, Cyril Pellevat, André Reichardt, Didier Marie, Mme Gisèle Jourda, MM. Claude Kern, André Gattolin, Pierre Laurent, Mme Colette Mélot, M. Jacques Fernique, Mme Véronique Guillotin, *vice-présidents ;* M. François Calvet, Mme Marta de Cidrac, M. Jean-Yves Leconte, Mme Amel Gacquerre, *secrétaires ;* MM. Pascal Allizard, Jean-Michel Arnaud, Mme Florence Blatrix Contat, M. Philippe Bonnecarrère, Mme Valérie Boyer, MM. Jean-Pierre Corbisez, Pierre Cuypers, Christophe-André Frassa, Mme Joëlle Garriaud-Maylam, M. Daniel Gremillet, Mmes Pascale Gruny, Laurence Harribey, MM. Ludovic Haye, Jean-Michel Houllegatte, Patrice Joly, Mme Christine Lavarde, MM. Dominique de Legge, Pierre Louault, Victorin Lurel, Franck Menonville, Mme Catherine Morin-Desailly, MM. Louis-Jean de Nicolaÿ, Pierre Ouzoulias, Mmes Elsa Schalck, Patricia Schillinger.

S O M M A I R E

L'ESSENTIEL

UNE NOUVELLE ÉTAPE DANS LA CONSTRUCTION DU MARCHÉ EUROPÉEN DES DONNÉES

Avec la multiplication des **objets connectés**, dans le cadre du développement de l'internet des objets, le **volume des données** industrielles produites connaît depuis quelques années une **croissance exponentielle**[1]. Ces données, qui sont une composante centrale de l'économie numérique, sont **pourtant peu utilisées au sein de l'Union européenne**.

Cette **situation résulte de la combinaison de plusieurs éléments techniques**, en particulier la qualité et la fiabilité insuffisantes des données, des capacités limitées d'identification et d'analyse, l'absence d'interopérabilité et le coût d'interfaçage des systèmes et d'échange de données. En outre, ces données restent **concentrées entre les mains d'un nombre réduit d'acteurs** économiques en raison de l'asymétrie dans le pouvoir de négociation.

Pour accompagner **la mise en place d'un « espace européen des données »**, la Commission européenne a présenté le 23 février 2022 **un cadre harmonisé[2], destiné à faciliter l'accès à ces données et leur utilisation, et annoncé dans la stratégie européenne pour les données** qu'elle avait publiée en 2020.

UN CADRE EUROPEEN HARMONISÉ ET TRANSSECTORIEL EN MATIÈRE D'ACCÈS, D'UTILISATION ET DE PARTAGE DES DONNÉES GÉNÉRÉES PAR DES OBJETS CONNECTÉS ET DES SERVICES LIÉS

- **Un droit d'accès direct et gratuit aux données pour l'utilisateur**

L'accès aux données devra être simple et sécurisé, prévu dès la conception (by design). Des mesures de protection de la confidentialité des secrets d'affaires peuvent être convenues entre l'utilisateur de l'objet connecté et le détenteur des données mais elles ne doivent pas constituer un obstacle à l'accès aux données. En revanche, il est interdit à l'utilisateur de se servir des données pour mettre au point un produit concurrent.

L'utilisateur devra être informé de ses droits de manière claire et compréhensible, avant l'achat ou la location d'un objet connecté ou d'un service lié. En cas de difficulté, il pourra introduire une plainte auprès de l'autorité nationale compétente.

---

[1] *La Commission européenne évalue le nombre d'objets connectés à 8 milliards en 2019 et 13,8 milliards en 2024, le volume mondial de données à 33 zettaoctets en 2018 et 175 zettaoctets en 2025, la valeur de l'internet des objets à 5 000 milliards d'euros.*

[2] *Règlement sur les données (*Data Act), *COM(2022) 68 final.*

- **Un partage encadré des données avec un tiers désigné par l'utilisateur**

Les données dont la communication a été demandée par l'utilisateur devront être mises à sa disposition de manière équitable et transparente, cette mise à disposition pouvant être éventuellement assortie d'une compensation raisonnable. Les données ne peuvent être utilisées que pour la seule finalité prévue.

La liberté contractuelle des détenteurs des données est encadrée afin de prévenir l'introduction de clauses abusives en matière d'accès et d'utilisation des données. En cas de difficultés, les parties pourront saisir un organisme de règlement des litiges certifié.

- **Un droit d'accès aux données des autorités et organismes publics en cas de besoin exceptionnel de les utiliser**

L'exercice d'un tel droit est envisagé dans trois situations : une urgence publique, la prévention d'une telle urgence ou le rétablissement à la suite d'une telle urgence, enfin lorsque l'absence de données disponibles empêche l'organisme de s'acquitter d'une mission d'intérêt public prévue par la loi.

La demande d'accès doit être justifiée et précise (données concernées et durée d'utilisation), proportionnée au besoin et, « dans la mesure du possible », ne pas porter sur des données à caractère personnel. L'utilisation des données est encadrée mais certains partages peuvent être justifiés au regard de l'objet.

CLARIFIER ET COMPLÉTER LE PROJET EUROPÉEN POUR GARANTIR L'ACCES DES UTILISATEURS AUX DONNÉES

Pour **assurer l'effectivité des droits reconnus aux utilisateurs**, les rapporteurs de la commission des affaires européennes formulent plusieurs recommandations.

- **Préciser la définition des données concernées**

Afin de clarifier le périmètre des données concernées, il convient de préciser qu'il s'agit de données industrielles brutes, générées par l'utilisation d'un produit connecté ou de services liés.

- **Faciliter la lecture et la réutilisation des données par des mesures techniques**

Il paraît nécessaire de :

  - préciser que les formats de données doivent être compréhensibles, structurés, habituels et lisibles par la machine ;

- prévoir que les métadonnées nécessaires à l'interprétation des données doivent également être communiquées.

- **Assurer l'équilibre des relations entre l'utilisateur et le détenteur des données**
  - **identifier des clauses abusives** de nature à porter une atteinte injustifiée aux droits de l'utilisateur sur les données et les interdire ;
  - **préciser et encadrer le caractère raisonnable et non discriminatoire de la compensation** exigée pour la mise à disposition des données à un tiers afin de prévenir des abus.
- **Poser comme principe que la protection contractuelle des secrets d'affaires ne saurait conduire à limiter l'accès et l'utilisation des données**

Les rapporteurs considèrent toutefois qu'il devrait être admis que des impératifs de sécurité puissent exceptionnellement justifier un refus de transmettre des données.

- **Affirmer la primauté des règles de protection des données à caractère personnel** lorsque de telles données sont mêlées aux données générées
- **Encadrer l'accès des organismes et autorités publiques aux données**
  - **pour les cas où l'urgence est invoquée, préciser la nature de l'urgence ainsi que de ses conséquences ;**
  - **faire obligation à l'organisme public de justifier qu'il n'est pas en mesure d'obtenir rapidement les données concernées, y compris en les achetant ;**
  - **encadrer la portée de l'obligation de mise à disposition en l'absence d'urgence :**
    - l'utilisation des données doit être strictement limitée à l'objet de la mission ;
    - les droits et libertés des personnes doivent être préservés, en particulier lorsque l'anonymisation des données n'est pas possible.

ACCOMPAGNER ET SÉCURISER LES TRANSFERTS DE DONNÉES

La proposition de règlement s'attache à corriger certains obstacles juridiques et techniques au changement de fournisseur de services de traitement des données et d'interopérabilité des données. Elle organise par ailleurs une protection des données à caractère non personnel, afin d'empêcher certains transferts internationaux.

- **La réduction des obstacles commerciaux, techniques, contractuels et organisationnels au changement de fournisseur de services de traitement des données**

Dans un marché caractérisé par une très forte concentration (72% du marché européen est contrôlé par 3 fournisseurs américains) et des pratiques de verrouillage particulièrement efficaces, les utilisateurs ne parviennent pas à changer de fournisseur, ce qui entrave le développement de fournisseurs concurrents sur le marché européen.

Pour remédier à cette situation, la proposition de règlement impose un ensemble d'obligations au fournisseur initial, en particulier la limitation à 30 jours calendaires de la durée du préavis de résiliation du contrat, et l'indication dans le contrat des catégories de données et d'applications exportables.

Le fournisseur initial serait contraint de mettre en œuvre le portage des données, applications et autres actifs numériques et maintenir l'équivalence fonctionnelle du service dans l'environnement informatique des différents fournisseurs.

Enfin, les frais de sortie devraient être progressivement supprimés sous 3 ans.

- **Des exigences essentielles d'interopérabilité**

L'interopérabilité permet de combiner des données provenant de différentes sources à l'intérieur des secteurs et entre les secteurs. Elle est donc une condition nécessaire du partage des données, motif pour lequel la proposition de règlement impose un ensemble d'exigences essentielles d'interopérabilité des données aux exploitants d'espaces de données, aux services de traitement des données et en matière de contrats intelligents pour le partage des données.

- **La sécurisation des transferts internationaux de données**

Certains pays extra-européens se sont dotés de lois permettant à leurs juridictions, y compris répressives, ou à leurs administrations, d'obtenir un transfert direct de données à caractère non personnel situées en dehors de leur territoire, y compris dans l'Union. Or ces demandes de transfert peuvent ne pas être compatibles avec le droit européen ou avec le droit national, en particulier en matière de protection des droits fondamentaux de la personne (sécurité ou droit à un recours effectif) ou des

intérêts fondamentaux d'un État membre (sécurité ou défense nationales), ou encore avec la protection de secrets d'affaires ou de droits de propriété intellectuelle.

La proposition de règlement soumet les fournisseurs de services de traitement de données à l'obligation de prendre « toutes les mesures techniques, juridiques et organisationnelles raisonnables » afin d'empêcher le transfert hors du territoire européen de données à caractère non personnel qui y sont détenues ou l'accès d'États tiers à celles-ci. **En l'absence d'accord international**, il leur est en principe **interdit** de **procéder à un transfert de données** exigé par une décision ou un jugement d'un juridiction ou une décision d'une autorité administrative d'un pays tiers et de donner accès à ces données, **sauf si certaines conditions cumulatives**, qu'elle énumère, **sont réunies**.

COMPLÉTER LES OBLIGATIONS DES FOURNISSEURS DE SERVICES DE TRAITEMENT DES DONNÉES

Pour que l'exercice du droit de changer de fournisseur de services de traitement des données soit effectif, les rapporteurs de la commission des affaires européennes estiment indispensable de renforcer l'information du client et d'interdire certaines pratiques abusives.

- **Informer obligatoirement le client sur le possible changement de fournisseur**
  - information **préalable à l'acceptation de l'offre** d'un fournisseur de services de traitement des données **sur les conditions, coûts et modalités du changement de fournisseur** ;
  - information précise **sur les étapes techniques du processus de migration** ainsi que sur les diligences qu'il mettra en œuvre.
- **Interdire de refuser le changement de fournisseur au motif de la phase d'utilisation gratuite de ses services dont a bénéficié le client**
- **Supprimer rapidement les frais de sortie pour permettre d'atteindre l'objectif de rééquilibrage du marché de l'informatique en nuage.**

CONSTRUIRE UN HÉBERGEMENT SOUVERAIN POUR PROTÉGER CERTAINES DONNÉES

Une liste des données sensibles (dont les données de santé) et des données dont la divulgation est susceptible de porter atteinte à la sécurité nationale doit être établie.

Pour protéger ces données de l'application extraterritoriale de législations extra-européennes ou d'ingérences étrangères, il est indispensable que l'Union européennes et les États membres se dotent d'hébergements souverains.

METTRE EN PLACE UNE STRUCTURE DE COORDINATION INTRA-EUROPÉENNE

- **Un suivi à l'échelle nationale par des autorités dotées de pouvoirs d'investigation et de sanction**

La supervision de la mise en œuvre du règlement est confiée par la proposition de règlement européen à des autorités nationales entre lesquelles des mécanismes de coopération sont prévus.

Les États membre devront veiller à une coordination efficace entre les autorités qu'ils auront désignées pour superviser l'application du règlement et avec celles qui sont compétentes en matière de protection des données à caractère personnel.

- **La mise en place d'une structure permanente pour faciliter la coordination intra-européenne**

Sans aller jusqu'à désigner un contrôleur européen comme il en existe en matière de protection des données à caractère personnel, la mise en place d'une structure permanente de coordination réunissant des représentants des différentes autorités nationales concernées apparaît de nature à renforcer l'efficacité de la coordination intra-européenne.

Dans la suite de la stratégie européenne des données qu'elle a publiée en 2020, la Commission européenne a présenté le 23 février 2022, **une proposition de règlement européen sur les données**[1], qui **vise à faciliter la libre circulation des données dites industrielles, afin de permettre une répartition équitable de leur valeur entre les acteurs de l'économie des données.**

I. UN VOLET DE LA STRATÉGIE EUROPÉENNE POUR LES DONNÉES

Les données constituent **un atout stratégique potentiel pour l'Union européenne**. Leur utilisation et leur valorisation sont en effet une « composante centrale de l'économie numérique et une ressource essentielle pour assurer les transitions écologique et numérique »[2].

Depuis l'adoption, en 2016, du règlement général sur la protection des données à caractère personnel (RGPD)[3] puis, en 2018, du règlement sur la libre circulation des données à caractère non personnel[4], **la libre circulation des données au sein de l'UE est considérée comme une cinquième liberté** auprès des quatre libertés constitutives du marché unique européen que sont la libre circulation des biens, des personnes, des services et des capitaux, consacrées par l'Acte unique européen de 1986. Mais force est de constater **qu'un certain nombre de barrières limitent l'effectivité de cette libre circulation.**

Pour y remédier, la Commission européenne a publié, le 19 février 2020, une stratégie européenne pour les données[5], en vue de la mise en place et du développement d'un **« espace européen des données ».** Elle a annoncé à cet effet un ensemble de mesures, dont une législation sur les données pour développer l'accès aux données et permettre leur utilisation.

---

[1] *Proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (dit règlement sur les données* – Data Act*) - (COM(2022) 68 final).*

[2] *Exposé des motifs de la proposition de règlement.*

[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 95/46/CE. Son article 1er § 3 pose 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 ».*

[4] *Règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018, dont l'article 1er indique qu'il « vise à assurer le libre flux de données autres que les données à caractère personnel au sein de l'Union, en établissant des règles concernant les exigences de localisation des données, la disponibilité des données pour les autorités compétentes et le portage des données pour les utilisateurs professionnels ».*

[5] *Communication de la Commission au Parlement européen, au Conseil, au Comité Économique et Social Européen et au Comité des Régions- Une stratégie européenne pour les données – COM(2020)66 final.*

A. DES VOLUMES CONSIDÉRABLES DE DONNÉES SOUS-EXPLOITÉES

1. La croissance exponentielle de la production de données

Avec la multiplication des objets connectés, dans le cadre du développement de l'internet des objets (IdO - IoT), le volume de données industrielles produites connaît depuis quelques années une croissance exponentielle.

Quelques chiffres
Nombre d'objets connectés : 8 milliards en 2019 – 13,8 milliards en 2024
Volume mondial de données : 33 zettaoctets en 2018 – 175 zettaoctets en 2025
Valeur de l'internet des objets : 5 000 milliards d'euros en 2022.
Source : Commission européenne

2. Une sous-utilisation persistante

Comme l'a constaté la présidente de la Commission européenne lors de son discours sur l'état de l'Union 2020[1], en dépit de cette croissance de la production de données, la **part des données industrielles non utilisées en Europe** est **de l'ordre 80 %**.

Cette situation résulte de la combinaison de plusieurs facteurs.

a) Des obstacles techniques

Les données brutes générées par l'utilisation d'objets connectés ne peuvent être réutilisées que si elles présentent un **niveau de qualité et de fiabilité** suffisant. Tel n'est souvent pas le cas aujourd'hui, en raison par exemple de la médiocrité des connexions qui permettent de les recueillir ou de la fiabilité limitée de certains capteurs.

Au-delà des conditions techniques de recueil des données, le recours à des formats propriétaires par les grands opérateurs qui recueillent les données générées et l'absence de normes impératives en matière d'**interopérabilité** empêchent également l'utilisation de ces données.

Enfin, des analyses sont nécessaires pour identifier les objets et les données les plus pertinents. Des **capacités analytiques** doivent donc être développées pour traiter les volumes de données et en extraire des informations qualitatives et réellement exploitables.

---

[1] *Discours sur l'état de l'Union 2020 « Construire le monde dans lequel nous voulons ; vivre: une union pleine de vitalité dans un monde d'une grande fragilité », 16 septembre 2020.*

b) Des pratiques anticoncurrentielles agressives

La sous-utilisation des données s'explique aussi par le fait qu'elles sont **concentrées entre les mains d'un nombre réduit d'acteurs économiques,** en raison de l'asymétrie dans le pouvoir de négociation entre les différentes entreprises concourant à produire des données sur une chaîne de valeur.

Des déséquilibres en termes de pouvoir de marché permettent en effet aux principaux acteurs du numérique, – ces grandes plateformes, que le droit européen qualifie dorénavant de « contrôleurs d'accès » -, de concentrer les données et d'**imposer unilatéralement des conditions d'accès et d'utilisation de celles-ci** aux utilisateurs d'objets connectés qui produisent ces données et aux entreprises tierces avec lesquelles elles pourraient être partagées, par exemple à des fins de réparation de l'objet connecté.

c) Une faible confiance dans le partage des données

La faible confiance des utilisateurs et des entreprises dans le partage des données constitue également un obstacle important identifié par la Commission européenne[1].

B. UN ESPACE COMMUN DES DONNÉES EN CONSTRUCTION

Pour assurer le bon fonctionnement de l'espace européen des données qu'elle entend promouvoir, la Commission a prévu la mise en place de **règles communes** et de **mécanismes d'application** garantissant :

- la circulation des données à l'intérieur du marché unique et entre les secteurs, dans le plein respect des règles et valeurs européennes, en particulier la protection des données à caractère personnel ;
- une concurrence efficace sur le marché intérieur, en prévoyant des règles d'accès et d'utilisation des données « équitables, pratiques et fiables » ;
- des mécanismes de gouvernance des données « clairs et fiables » ;
- une approche des flux internationaux de données ouverte mais affirmée et fondée sur les valeurs européennes.
- Les actions qu'elle propose reposent sur **quatre piliers** :

[1] *Étude d'impact accompagnant la proposition de règlement sur la gouvernance des données, 25 novembre 2020.*

- des mesures horizontales (transsectorielles) pour l'accès aux données et leur utilisation, comportant en particulier un cadre pour la gouvernance des espaces européens communs de données et une législation sur les données facilitant le partage de celles-ci ;
- des investissements dans les données et le renforcement des capacités et des infrastructures européennes pour l'hébergement, le traitement et l'utilisation des données ainsi que leur interopérabilité ;
- le développement des compétences des particuliers en matière numérique, l'éducation générale aux données et le renforcement des capacités des PME ;
- le développement d'espaces européens communs des données dans des secteurs économiques stratégiques et des domaines d'intérêt public, en particulier les données relatives au pacte vert, en matière de santé, de mobilité, ou encore d'énergie.

Dans le cadre du premier pilier, pour accroître la disponibilité des données au sein de l'Union et en permettre la valorisation, afin que l'économie européenne puisse être davantage compétitive face aux grands acteurs internationaux du marché des données, la Commission a présenté **deux propositions législatives** destinées à clarifier et à renforcer les règles applicables en matière de partage des données au sein de l'Union. La première, qui sera applicable à compter du 23 septembre 2023, porte sur **les données du secteur public**[1], la seconde, – la proposition de règlement sur les données -, concerne **les données industrielles du secteur privé**.

C. UNE RÉPARTITION PLUS ÉQUITABLE DE LA VALEUR ENTRE LES ACTEURS DE L'ÉCONOMIE DES DONNÉES

Pour permettre une répartition plus équitable de la valeur entre les différents acteurs de l'économie des données, la proposition de règlement reconnaît aux utilisateurs d'objets connectés et de services liés des droits sur les données générées, impose des obligations aux entreprises qui détiennent les données, encadre l'utilisation de celles-ci et impose le respect de normes techniques harmonisées.

[1] *Voir annexe 1.*

1. Des données produites par des objets connectés et des services liés

Les objets connectés, qui peuvent être incorporés dans un bien immeuble, obtiennent, génèrent ou recueillent des données concernant leur utilisation ou leur environnement et les communiquent par l'intermédiaire d'un service de communication électronique (art. 2§2).

Sont considérés comme des services liés à ces objets, les services intégrés dans l'objet ou interconnectés avec celui-ci afin qu'il remplisse ses fonctions (art. 2§3), y compris les assistants virtuels (art. 2§4).

Trois catégories d'acteurs - personnes physiques ou morales-, sont concernées par l'accès et l'utilisation des données : **les utilisateurs, les détenteurs des données et les destinataires des données.**

Les « utilisateurs » d'objets connectés et de services liés possèdent ou louent ces objets.

Les « détenteurs de données » produites par les objets connectés et services liés ont l'obligation de les mettre à la disposition des utilisateurs qui en font la demande, de tiers destinataires désignés par l'utilisateur ou d'organismes publics en cas d'urgence publique ; il s'agit généralement du fabricant de l'objet connecté.

Les « destinataires de données, qui sont désignés par l'utilisateur en raison de leur activité commerciale, industrielle, artisanale ou libérale, ou en application d'une obligation légale ».

2. Des règles juridiques et techniques harmonisées

Le chapitre II de la proposition de règlement définit les droits des utilisateurs sur les données générées par leur utilisation d'objets connectés et de services liés, fixe des **règles harmonisées en matière d'accès, d'utilisation et de partage de ces données** entre entreprises et consommateurs (*BtoC* et *CtoB*) et interentreprises (*BtoB*). Le chapitre III définit les obligations des détenteurs des données ainsi tenus de rendre des données disponibles.

Le chapitre IV s'attache à limiter l'exploitation de leur position dominante par des acteurs qui entravent l'accès aux données, en **rééquilibrant le pouvoir de négociation** des micro, petites et moyennes entreprises dans les contrats de partage de données et en **écartant les grandes plateformes du bénéfice de ce partage**.

Le chapitre V prévoit un **accès encadré des organismes du secteur public** aux données détenues par le secteur privé, en particulier en situation d'urgence.

Le chapitre VI vise à **faciliter le changement de fournisseur de services de traitement de données** (*cloud*), que les très grands acteurs de l'informatique en nuage ont rendu en pratique impossible, tandis que le chapitre VII prévoit des **garanties en matière de transferts internationaux de données à caractère non personnel**.

Enfin, pour permettre la circulation des données et leur réutilisation, le chapitre VIII de la proposition définit des **exigences essentielles en matière d'interopérabilité** que doivent respecter les exploitants d'espaces de données, les services de traitement des données et les contrats intelligents pour le partage des données.

Un dernier chapitre (IX) confie **aux États membres**, qui devront désigner des autorités compétentes en la matière, **la responsabilité de la mise en œuvre du règlement**.

3. Des gains attendus importants pour l'économie européenne

La Commission estime que l'amélioration de l'utilisation des données dans l'Union permettrait **un gain de près de 2 % de PIB à l'horizon 2028 et la création de 2,2 millions d'emplois**[1].

Elle évalue les coûts d'entrée de la mise en conformité avec la proposition de règlement sur les données à environ 1 milliard d'euros, auxquels s'ajoutent un peu plus de 200 millions d'euros par an.

Quant au coût direct de traitement des données que les entreprises devront, dans certaines circonstances, mettre à la disposition d'organismes publics, il serait d'environ 20 millions d'euros par an.

II. UN CADRE POUR FACILITER L'ACCÈS AUX DONNÉES INDUSTRIELLES ET LEUR UTILISATION

La proposition de règlement sur les données définit des **règles harmonisées relatives à l'accès et à l'utilisation équitables des données**, « tout en préservant un haut degré de protection de la vie privée, de sécurité, de sûreté et d'éthique »[2].

---

[1] *L'étude d'impact prend appui sur des travaux conduits depuis 2017, en particulier par la Direction générale pour le marché intérieur, industrie, entrepreneuriat et PME (*DG GROW*).*

[2] *Ursula von der Leyen, « Une Union plus ambitieuse –Mon programme pour l'Europe. Orientations politiques pour la prochaines Commission européenne 2019-2024 », 16 juillet 2019.*

Afin d' assurer une cohérence entre les divers droits d'accès aux données qui sont d'ores et déjà développés pour des situations spécifiques et avec des règles et des conditions différentes, notamment dans les secteurs de l'énergie[1], des transports[2], des services de paiement[3], ou encore des données de santé[4], ces règles ont une **portée transsectorielle**.

Même si le règlement sur les données serait sans préjudice des obligations sectorielles existantes en matière d'accès aux données, ces législations européennes sectorielles devront être évaluées et, le cas échéant, alignées sur ce règlement[5], et, comme l'indique l'exposé des motifs de la proposition de règlement résolution, toute réglementation future en la matière devra lui être conforme.

A. DES DROITS POUR LES UTILISATEURS D'OBJETS CONNECTÉS ET DE SERVICES LIÉS SUR LES DONNÉES GÉNÉRÉES ET DES OBLIGATIONS À LA CHARGE DES DÉTENTEURS DES DONNÉES

La proposition de règlement reconnaît aux utilisateurs d'objets connectés un **droit d'accès direct gratuit aux données** générées par l'utilisation d'objets connectés et de services liés ainsi que **le droit de partager ces données avec un tiers afin que celui-ci puisse leur fournir un service en lien avec ces produits.** Ce droit d'accès ne serait toutefois pas opposable aux micro ou petites entreprises en raison de la charge technique et des coûts disproportionnés qui pourraient en résulter pour elles (art. 7).

Pour assurer l'effectivité de ces droits d'accès et de partage des données, la proposition de règlement en définit les modalités d'exercice, impose un ensemble d'obligations aux détenteurs des données et encadre les conventions de partage des données.

---

[1] *Règlement (UE) du Parlement européen et du Conseil du 5 juin 2019 sur le marché intérieur de l'électricité ; directive (UE) 2019/944 du Parlement européen et du Conseil du 5 juin 2019 concernant des règles communes pour le marché intérieur de l'électricité et modifiant le directive 2012/27/UE.*

[2] *Directive (UE) 2010/40/UE du Parlement européen et du Conseil du 7 juillet 2010 concernant le cadre pour le déploiement de systèmes de transport intelligents dans le domaine du transport routier et d'interfaces avec d'autres modes de transport ; règlement (CE) n° 549/2004 du Parlement européen et du Conseil de 10 mars 2004 fixant le cadre pour la réalisation du ciel unique européen.*

[3] *Directive (UE) 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (UE) n° 1093/2010, et abrogeant le directive 2007/64/CE.*

[4] *Proposition de règlement du Parlement européen et du Conseil relatif à l'espace européen des données de santé, COM(2022) 197 final.*

[5] *Par exemple la création de l'espace des données relatives au pacte vert qui devrait conduire à une extension du périmètre de la directive 2007/2/CE du Parlement européen et du Conseil du 14 mars 2007 établissant une infrastructure d'information géographique dans la Communauté européenne (dite INSPIRE).*

1. Les obligations des détenteurs des données

La proposition de règlement envisage de soumettre les détenteurs des données à un ensemble d'obligations juridiques et techniques pour que l'utilisateur puisse effectivement accéder aux données et les partager.

Même quand elles figurent dans des bases de données, ces données ne bénéficient en effet pas de la protection juridique *sui generis* prévue par l'article 7[1] de la directive 96/9/CE concernant les bases de données[2], ainsi que l'indique expressément la proposition de règlement (art. 35).

Si l'utilisateur estime que ses droits en matière d'accès et de partage des données ne sont pas respectés, il peut introduire une **plainte auprès de l'autorité nationale compétente** chargée de l'application et de l'exécution du règlement (art. 3§2, a, et 31).

a) L'information préalable de l'utilisateur

Avant l'achat ou la location d'un objet connecté ou d'un service lié, il est prévu que l'utilisateur soit informé de ses droits sur les données qui seront générées par l'utilisation de l'objet et des services liés. Des informations claires et compréhensibles doivent ainsi lui être fournies, en particulier sur la **nature et** le **volume des données susceptibles d'être générées**, l'**utilisation que le fournisseur fera de ces données** et à quelles **fins**, ainsi que les **modalités d'accès** à ces données (art. 3§2).

L'utilisateur est également informé par le fournisseur de l'objet connecté de la manière dont il peut demander que les données soient partagées avec un tiers.

b) Des données accessibles et sécurisées

Les données générées doivent être facilement accessibles par l'utilisateur, et ce, de manière sécurisée. La conception et la fabrication des produits devront donc désormais **intégrer ces contraintes dès la conception** (*by design*) (art. 3§1).

Si pour des raisons techniques, l'accès aux données n'est pas possible, le détenteur des données devra mettre celles-ci à la disposition de l'utilisateur par voie électronique, sur simple demande, dans les meilleurs délais et de manière gratuite (art. 4§1).

---

[1] *Ce droit limite l'extraction et/ou la réutilisation de la totalité ou d'une partie substantielle de la base de données.*

[2] *Directive du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données.*

c) La mise à disposition des données à un tiers à la demande de l'utilisateur, éventuellement assortie d'une compensation raisonnable

L'utilisateur a le droit de demander au détenteur des données de partager tout ou partie des données avec un tiers (art. 5§1). Toute clause contractuelle excluant l'exercice du droit de partage, y dérogeant ou en modifiant les effets, est inopposable à l'utilisateur (art. 12).

Afin de ne pas conforter le pouvoir de marché des grandes plateformes, il est prévu (art. 5§2) que ce tiers ne peut pas être un contrôleur d'accès désigné comme tel en application du règlement sur les marchés numériques[1].

Les données transférées doivent présenter un niveau de qualité identique à celui dont bénéficie l'utilisateur et leur mise à disposition doit être faite de manière « équitable et transparente » (art. 8).

Le détenteur des données peut demander une compensation « raisonnable » des coûts de mise à disposition (art. 9§1). Toutefois, lorsque le destinataire est une micro, petite ou moyenne entreprise, il est prévu que seuls peuvent être compensés les coûts directement liés à la mise à disposition (art. 9 §2).

Dans tous les cas, les modalités de calcul de la compensation doivent être transparentes et non-discriminatoires (art. 9§4).

2. Une protection contractuelle de la confidentialité des données

Si l'existence de secrets d'affaires ne saurait constituer un obstacle recevable à l'accès aux données, des **mesures visant à préserver leur confidentialité**, en particulier à l'égard des tiers, **peuvent être convenues** entre le détenteur des données et l'utilisateur (art. 4§3).

Afin d'éviter l'utilisation ou la divulgation non autorisées de données, leur détenteur peut en outre appliquer des mesures techniques et contractuelles de protection (art. 11).

Par ailleurs, dans la mesure où les données générées peuvent permettre d'identifier certains éléments de la méthodologie de recueil et de traitement mise en œuvre, il est **expressément interdit à l'utilisateur de s'en servir pour mettre au point un produit concurrent** de celui dont elles proviennent (art. 4§4).

[1] Règlement (UE) 2022/1925 du Parlement européen et du Conseil du 14 septembre 2022 relatif aux marchés contestables et équitables dans le secteur numérique et modifiant les directives (UE) 2019/1937 et (UE) 2020/1828 (règlement sur les marchés numériques – *Digital Market Act* ou *DMA*).

3. L'utilisation des données pour la seule finalité prévue dans la demande de partage

La mise à disposition des données se fait aux fins et conditions convenues avec l'utilisateur pour la fourniture d'un service ou prévues par une législation spécifique.

En conséquence, dès lors que les données mises à disposition ne sont plus nécessaires à la finalité convenue (ou prévue par la législation spécifique), le tiers bénéficiaire doit les supprimer (art. 6§1).

Il est en outre interdit au tiers bénéficiaire de les transmettre à un autre tiers, sauf à ce que cela soit nécessaire pour la fourniture du service demandé par l'utilisateur, ou de les utiliser pour mettre au point un produit concurrent (art. 6§2, c).

Il est également formellement interdit au tiers bénéficiaire de se servir de ces données pour manipuler l'utilisateur ou à des fins de profilage (art. 6§2, a et b).

En cas de difficultés, les parties peuvent saisir un **organisme de règlement des litiges certifié**, dont la mise en place est prévue dans chaque État membre. Cet organisme devra prendre une décision sous 90 jours mais cette décision n'est contraignante pour les parties que si celles-ci ont expressément accepté son caractère contraignant avant le début de la procédure de règlement (art. 11).

4. Une protection contre les clauses contractuelles abusives en matière d'accès et d'utilisation des données

Afin que les détenteurs de données ne puissent pas imposer aux micro, petites ou moyennes entreprises des conditions abusives en matière d'accès aux données, d'utilisation de celles-ci, de responsabilité ou de voies de recours, qui les empêcheraient d'exercer leur activité, le chapitre IV (art. 13) encadre la liberté contractuelle des entreprises.

La Commission entend ainsi **corriger des déséquilibres contractuels avérés** alors que 99 % des entreprises pourvoyeuses de données et 98,8 % des entreprises utilisatrices de données dans l'Union européenne sont des micro, petites et moyennes entreprises[1].

[1] *Il résulte du rapport d'étude finale de l'outil de surveillance du marché européen des données intitulé* Faits et chiffres clés, premières conclusion, paysage des données et histoires quantifiée-, *que 85 % des emplois créés ces dernières années dans le domaine des données l'ont été par ces entreprises.*

Une clause est considérée abusive si elle est « d'une nature telle que son utilisation s'écarte fortement des bonnes pratiques commerciales en matière d'accès aux données et d'utilisation de celles-ci, et qu'elle est contraire à la bonne foi et à la loyauté ». C'est ainsi que, lorsqu'elles ont été **imposées unilatéralement**, **trois clauses sont considérées comme abusives à raison de leur objet ou de leur effet et cinq autres sont réputées l'être.** Celui qui a pris l'initiative d'une telle clause ne peut alors l'opposer que s'il démontre le caractère négocié de celle-ci.

Pour faciliter l'élaboration de ces contrats et aider les parties à les rédiger et à les négocier de manière équilibrée, il est prévu que des **clauses types** seront élaborées par la Commission (art. 34).

5. La mise des données à la disposition d'organismes du secteur public

La proposition de règlement prévoit que les organismes du secteur public et des institutions, organes ou organismes de l'Union sont en droit d'utiliser des données détenues par des entreprises en raison d'un « besoin exceptionnel » (art. 14).

Les détenteurs des données doivent alors mettre les données demandées à disposition dans les meilleurs délais (art. 18), sauf si celles-ci ne sont pas disponibles ou lorsque la demande de mise à disposition ne respecte pas les exigences définies (art. 17).

Il est précisé que cette obligation est sans préjudice des autres obligations de mise à disposition de données prévues par le droit national ou le droit européen[1].

Il est par ailleurs expressément interdit de faire usage des données ainsi mises à disposition à des fins de prévention et de détection d'infractions, d'enquêtes ou de poursuites.

Le non-respect de cette obligation - dont sont exemptées les micro et petites entreprises -, est passible de sanctions (art. 33).

a) Justifier d'un besoin exceptionnel

Trois situations sont considérées comme constitutives d'un besoin exceptionnel d'utiliser des données (art. 15) :

- lorsque les données sont nécessaires pour réagir à une urgence publique ;

[1] *Voir* supra.

- lorsqu'elles sont nécessaires pour prévenir une telle urgence ou contribuer au rétablissement à la suite d'une telle urgence : la demande de données doit alors avoir une durée et une portée limitées ;

- lorsque l'absence de données disponibles empêche l'organisme de s'acquitter d'une mission d'intérêt public prévue par la loi et que :
    - soit il ne lui a pas été possible d'obtenir ces données par d'autres moyens (achat, obligation de mise à disposition) et que l'adoption d'une nouvelle législation ne permet pas que les données soient disponibles en temps utile ;
    - soit l'obtention des données selon la procédure prévue par la proposition de règlement réduirait substantiellement la charge administrative pour les détenteurs des données.

La demande adressée au détenteur des données doit indiquer précisément les données demandées, **démontrer le besoin exceptionnel** pour lequel elles sont demandées et **expliquer l'utilisation prévue** des données et la **durée** de cette utilisation (art. 17§1). Cette demande est publiée en ligne dans les meilleurs délais (art. 17§2, f).

La demande doit être proportionnée au besoin en termes de granularité, de volume et de fréquence d'accès, et il est recommandé qu'elle ne porte **pas, « dans la mesure du possible »,** sur **des données à caractère personnel** (art. 17§2, d), sauf si celles-ci peuvent être anonymisées.

Quant à la divulgation de secrets d'affaires, elle ne peut être imposée que lorsqu'elle est strictement nécessaire pour atteindre la finalité de la demande (art. 19§2).

b) Des données qui ne peuvent être utilisées qu'aux fins pour lesquelles elles ont été demandées

Les données ainsi obtenues ne sont utilisées que d'une « manière compatible » avec la finalité pour laquelle elles ont été demandées (art. 19§1, a)[1]. Elles doivent en conséquence être détruites lorsqu'elles ne sont plus nécessaires à la finalité indiquée (art. 19§1 c).

Ces données, qui peuvent être commercialement sensibles, **ne peuvent être considérées comme des données publiques ouvertes disponibles pour une réutilisation[2]**.

---

[1] *Et non pas, comme en cas de partage de données avec un tiers, aux seules fins pour lesquels ce partage est effectué.*

[2] *Dans le cadre prévu par la directive (UE) 2019/1024 du Parlement européen et du Conseil du 20 juin 2019 concernant les données ouvertes et la réutilisation des données du secteur public.*

En revanche, elles peuvent être **partagées** avec d'autres organismes publics, ou un tiers en cas d'externalisation de leur traitement, pour répondre aux besoins ayant justifié la demande de mise à disposition (art. 17§4).

Ces données peuvent également être **échangées** dans le cadre de la coopération transfrontière et ne sont alors pas utilisées d'une manière « incompatible avec la finalité pour laquelle elles ont été demandées » (art. 22), sous le contrôle de l'autorité compétente de l'État membre (art. 31).

Il est par ailleurs prévu que ces données puissent être partagées avec des organismes de **recherche** ou des instituts de statistique **dans le cadre de besoins exceptionnels** (art. 21). Le détenteur des données en est alors informé.

c) Une compensation possible sauf en cas d'urgence publique

Sauf lorsqu'elle est demandée pour répondre à une urgence publique, il est prévu (art. 20) que le détenteur des données peut demander une compensation des coûts techniques, organisationnels et d'adaptation (y compris l'anonymisation) occasionnés par la mise à disposition.

B. DES CLARIFICATIONS ET DES COMPLÉMENTS SONT NÉCESSAIRES

Les objectifs poursuivis par la proposition de règlement en matière d'accès et d'utilisation des données apparaissent pertinents et la mise en place d'une législation européenne horizontale définissant des règles harmonisées à ces effets est bienvenue. Il est toutefois indispensable de veiller à son articulation avec les régimes européens sectoriels existants et à venir, par exemple en matière de données de santé.

Pour renforcer l'efficacité du cadre proposé, plusieurs précisions et compléments devraient en outre lui être apportés.

1. Préciser quelles sont les données visées

La proposition de règlement définit les données comme « toute représentation numérique d'actes, de faits ou d'informations et toute compilation de ces actes, faits ou informations, notamment sous la forme d'enregistrements sonores, visuels ou audiovisuels » (art. 2§1), tandis que son article premier indique que les données qu'elle vise sont celles qui sont générées par l'utilisation d'un produit ou d'un service lié.

Sans que cela soit explicité, il en résulte qu'il s'agit de données industrielles brutes, non modifiées, non interprétées, ni ajoutées, émanant de la source primaire que constitue l'objet connecté ou un service lié à celui-ci,

dont les caractéristiques sont liées à cette source et qui n'ont été soumises à aucun traitement ou autre manipulation[1].

Afin de définir plus clairement la nature des données et le caractère connecté de leur source, il paraît nécessaire de préciser qu'il s'agit de données industrielles brutes résultant directement de l'utilisation d'un objet connecté ou de services liés.

2. Affirmer la primauté des règles de protection des données à caractère personnel

L'utilisation d'un produit ou d'un service lié, en particulier par une personne physique, peut générer des données se rapportant à cette personne identifiée ou identifiable. Ainsi que l'évoque le considérant n° 30 de la proposition de règlement, **des données se rapportant à la personne concernée et des données non personnelles peuvent se trouver inextricablement liées dans un ensemble de données.** Le considérant précise qu'en pareil cas, le traitement de ces données est soumis au RGPD, comme le prévoit d'ailleurs l'article 2§2 du règlement du 14 novembre 2018 relatif au libre flux des données à caractère non personnel.

Dans la mesure où l'objet connecté n'est pas exclusivement utilisé par son seul propriétaire ou loueur mais par les membres du foyer ou les salariés d'une entreprise (qui utilisent par exemple des véhicules connectés mis à leur disposition), le considérant précise également que, lorsque les données générées par l'utilisation de tels produits et services ne sont pas produites par l'utilisateur, celui-ci devrait être considéré comme « responsable du traitement des données » au sens de l'article 6§1 du RGPD. Le propriétaire de l'objet connecté ou son loueur doit alors disposer à ce titre d'une « base juridique » pour le traitement des données et respecter les obligations lui incombant en cette qualité.

Dans la suite d'une **recommandation du Comité européen de la protection des données et du Contrôleur européen de la protection des données,** figurant dans leur avis conjoint du 4 mai 2022 sur la proposition de règlement, il est indiqué, à l'article 1er§3 de la proposition de règlement, que celui-ci est « sans préjudice de l'applicabilité du droit de l'Union sur la protection des données à caractère personnel »[2].

---

[1] *Ces données quantitatives sont fiables si l'objet qui les a produites a été convenablement étalonné et si le processus de collecte n'est pas biaisé.*

[2] *Soit principalement :*

- *la directive 2002/58/CE du 12 juillet 2002 « vie privée et communications électroniques » (prochainement remplacée par un règlement éponyme) ;*
- *le Règlement général sur la protection des données (RGPD) du 27 avril 2016 ;*
- *la directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de*

Toujours en cas de partage des données avec des tiers, l'article 6§2 (b) **interdit l'utilisation** par le tiers des données qu'il reçoit **à des fins de profilage** de personnes physiques au sens du RGPD, sauf à ce qu'une telle utilisation soit nécessaire pour fournir le service demandé par l'utilisateur.

Ces précisions sur les interactions entre les textes européens applicables en matière de protection des données à caractère personnel, en particulier le RGPD, ainsi que les compétences reconnues en la matière aux autorités de contrôle indépendantes sont bienvenues[1] mais les rapporteurs de la commission des affaires européennes considèrent que la primauté des règles européennes de protection des données à caractère personnel, quelle que soit la situation, devrait être expressément affirmée.

Afin de prévenir toute incertitude pour les données à caractère personnel figurant parmi les données recueillies, la primauté des règles européennes de protection des données à caractère personnel sur celles de la proposition de règlement sur les données doit être rappelée.

3. Renforcer la protection des droits des utilisateurs sur les données

La proposition de règlement reconnaît à l'utilisateur un droit d'accès « aisé, sécurisé et direct » aux données produites par l'utilisation d'objets connectés et de services liés. Il impose, pour faciliter la mise en œuvre de ce droit, que cet accès soit techniquement prévu dès la conception de l'objet connecté.

Encore faut-il que ces données soient compréhensibles pour l'utilisateur et qu'il puisse facilement les utiliser.

Afin de permettre un accès effectif de l'utilisateur aux données générées par l'utilisation d'objets connectés et de services liés et une réutilisation facile de ces données, le format des données doit être compréhensible, structuré, habituel et lisible, et les métadonnées nécessaires à leur interprétation doivent également être communiquées à l'utilisateur.

---

détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données ;

- *le règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données du 23 octobre 2018.*

[1] *Les rapporteurs ont notamment pu échanger sur ce point avec des représentants de la Cnil.*

Une information préalable de l'utilisateur est prévue par la proposition de règlement, en particulier sur les données qui seront générées par l'utilisation de l'objet connecté et des services liés, les modalités d'accès à celles-ci et les conditions de leur ouverture à un tiers, en particulier lorsque ces données relèvent pour partie de secrets d'affaires.

Dans le même esprit, des limites sont également posées à l'utilisation des données par leur détenteur, y compris pour évaluer la situation économique, les actifs ou les méthodes de production de celui-ci.

Pour conforter la protection de l'utilisateur contre des limitations injustifiées de ses droits sur les données, l'identification de clauses de nature à porter une atteinte injustifiée aux droits de l'utilisateur sur les données qu'il génère pourrait être utilement engagée et les clauses abusives ainsi identifiées devraient être privées d'effets.

4. Faciliter le partage des données avec des tiers

Au vu des objectifs de partage de la valeur et d'ouverture des données aux micro, petites et moyennes entreprises mis en avant par la Commission face au pouvoir de marché des détenteurs des données, **l'interdiction de partager ces donnés avec des contrôleurs d'accès apparaît justifiée**.

S'agissant de la dispense de l'obligation de mise à disposition des données prévue pour les micro et petites entreprises, elle peut être admise en raison des coûts induits par la mise en conformité à laquelle ces entreprises devraient procéder. Il toutefois est prévu que les micro et petites entreprises qui ont des entreprises partenaires ou des entreprises liées ne puissent pas prétendre au bénéfice de cette dispense.

Les rapporteurs estiment, dans le même esprit, que les micro et petites entreprises ayant un lien avec un fabricant de produits connectés ou un fournisseur de services liés devraient également être écartées du bénéfice de cette dispense.

La dispense de l'obligation de mise à disposition des données prévue pour les micro et petites entreprises ne doit pas pouvoir bénéficier à celles d'entre elles qui ont un lien avec un fabricant de produits connectés ou un fournisseur de services liés.

Au-delà, et plus généralement, le fait que le volume de données générées par les objets connectés et les services liés qu'elles mettent à disposition ne soit pas pris en compte pour définir le périmètre des entreprises considérées comme de trop petits acteurs pour être soumises à certaines obligations en lien avec le numérique mérite un examen attentif, dans un secteur où le nombre de salariés peut être très réduit mais l'activité en matière de données importante.

Enfin, il est admis que la mise à disposition des données peut être facturée dès lors que la compensation est raisonnable et non discriminatoire, le détenteur des données devant alors en fournir les bases de calcul.

Afin de prévenir des abus au détriment des bénéficiaires du partage des données, des critères permettant de considérer qu'une compensation est « raisonnable et non discriminatoire » doivent être définis.

5. Assurer une protection contractuelle équilibrée des secrets d'affaires et prendre en compte les impératifs de sécurité

Dans certains cas, les données peuvent être susceptibles de révéler des informations sur la méthodologie mise en œuvre par leur détenteur. Des mesures techniques et opérationnelles peuvent alors être prévues d'un commun accord entre l'utilisateur et le détenteur des données. Des mesures peuvent également être convenues entre le détenteur de celles-ci et le tiers bénéficiaire.

Le cadre contractuel de protection de secrets d'affaires susceptibles d'être révélés par des données brutes en cas de demande d'accès et de transmission de celles-ci doit être équilibré et **ne pas excéder les exigences de protection de tels secrets**.

Toutefois, lors des auditions auxquelles ils ont procédé, l'attention des rapporteurs a été attirée sur les risques attachés à la communication de certaines données brutes qui peuvent révéler des informations sur le fonctionnement des objets connectés et mettre ainsi en péril leur sécurité.

La protection de secrets d'affaires ne saurait justifier un refus de communiquer les données à l'utilisateur, l'empêcher de les utiliser ou de les partager avec un tiers dans les conditions prévues par le règlement. Toutefois, un refus de transmettre les données doit pouvoir être opposé si le détenteur démontre que la divulgation de secret d'affaires est de nature à avoir des conséquences dommageables sérieuses, en particulier au regard de la sécurité de l'objet.

6. Encadrer l'accès aux données par des autorités publiques

Le dispositif proposé en matière de mise à disposition d'organismes publics de données en raison d'un besoin exceptionnel est présenté par la Commission comme constituant « un cadre proportionné, limité et prévisible », qui tient compte des contraintes des détenteurs des données et garantit la sécurité juridique (considérant n° 61). Les rapporteurs jugent toutefois indispensable de le préciser afin de **ne pas imposer des obligations injustifiées ou excessives aux entreprises qui détiennent les données concernées**.

a) Préciser la nature des situations exceptionnelles visées

Un besoin exceptionnel d'utiliser les données est réputé exister en cas d'urgence publique. Celle-ci est définie comme « une situation exceptionnelle ayant une incidence négative sur la population de l'Union, d'un État membre ou d'une partie de celui-ci, entraînant un risque de répercussions graves et durables sur les conditions de vie ou la stabilité économique, ou la détérioration substantielle d'actifs économiques dans l'Union ou dans les états concernés » (art. 2 (10)).

La définition de la nature de l'urgence et ses conséquences apparait particulièrement large. Afin de ne pas donner une portée excessive à l'obligation de mise à disposition, les rapporteurs préconisent que l'urgence et ses conséquences soient précisées.

Une définition précise de la nature de l'urgence (santé, catastrophe naturelle, catastrophes majeures d'origine humaine, cyberattaques) ainsi que de ses conséquences (y compris sur la stabilité économique ou des actifs économiques majeurs) permettrait de mieux encadrer le déclenchement de l'obligation de mise à disposition de données et sa portée.

Afin de ne pas permettre un recours injustifié à la mise à disposition contrainte de données détenues par des entreprises privées, l'accent doit être mis sur l'obligation pour l'organisme public demandeur de justifier qu'il n'est pas en mesure d'obtenir rapidement les données concernées, y compris en les achetant.

b) Encadrer la portée de l'obligation de mise à disposition en l'absence d'urgence

Il est prévu, même en l'absence d'urgence, qu'une mise à disposition de données peut également être imposée, faute de données disponibles, pour permettre à un organisme public de s'acquitter d'une mission spécifique d'intérêt public.

En l'absence de définition de la notion de mission spécifique d'intérêt public, les rapporteurs considèrent que la portée de l'obligation d'ouverture de données alors qu'il n'y a pas d'urgence doit être plus précisément encadrée afin de ne pas abusivement priver des entreprises des bénéfices qu'elles peuvent retirer des bases de données qu'elles ont constituées.

L'utilisation des données mises à disposition d'un organisme public pour lui permettre de s'acquitter d'une mission spécifique d'intérêt public doit être strictement limitée à l'objet de cette mission.

Elle doit en outre veiller au respect des droits et libertés des personnes, en particulier lorsqu'il s'agit de données à caractère personnel qui ne peuvent pas être anonymisées.

III. ACCOMPAGNER LA LIBRE CIRCULATION DES DONNÉES TOUT EN ASSURANT LA PROTECTION DE CERTAINES D'ENTRE ELLES

La liberté de circulation des données étant loin d'être effective, la proposition de règlement s'attache à corriger certains obstacles juridiques et techniques identifiés en matière de changement de fournisseur de services de traitement des données et d'interopérabilité.

Elle organise en outre une protection des données à caractère non personnel afin d'empêcher certains transferts internationaux de données.

A. DONNER UNE PORTÉE EFFECTIVE À LA POSSIBILITÉ DE CHANGER DE FOURNISSEUR DE SERVICES DE TRAITEMENT DES DONNÉES

Le service de traitement des données « permet la gestion à la demande et un large accès à distance à un ensemble modulable et variable de ressources informatiques pouvant être partagées de nature centralisée, distribuée ou fortement distribuée » (art. 2 (12)). Il est constitué de trois couches.

***Les trois couches du* cloud**

IaaS (*infrastructures as a Service*) : ressources informatiques brutes proposées par le prestataire de services, utilisées pour virtualiser une infrastructure ou pour des projets exigeants en ressources (*machine learning*, *big data*, hébergement etc.)

PaaS (*Plateform as a Service*) : plateforme accessible en ligne qui permet aux utilisateurs de créer des applications et des logiciels sans devoir en assurer la maintenance

SaaS (*Software as a Service*) : logiciel fonctionnant sur une infrastructure *cloud* dont l'utilisateur paie la licence sans s'occuper ni du stockage des données ni de l'entretien du matériel physique.

1. Un marché caractérisé par une très forte concentration

Le marché de l'informatique en nuage (*cloud*) est fortement concentré et les pratiques de verrouillage mises en place par ses très grands acteurs empêchent les utilisateurs de changer de fournisseurs et, par voie de conséquence, le développement de nouveaux fournisseurs de services de traitement des données sur le marché européen.

a) Un marché particulièrement concentré

Le marché des services de traitement de données est caractérisé par une très forte concentration. 90% du marché mondial est en effet détenu par trois fournisseurs américains (AWS, Microsoft Azure et Google Cloud), et un chinois (Alibaba), et 72% du marché européen par les trois mêmes fournisseurs américains (Microsoft Azure, AWS et Google Cloud).

Cette situation de **domination se renforce continuellement**. En effet, même si leur activité a connu une croissance significative au cours des dernières années, la part de marché des acteurs européens tend à régresser. **L'industrie européenne du *cloud* a** ainsi **vu ses parts de marché diminuer de moitié en l'espace de 5 ans (27 % en 2017, 13 % en 2022).**

*b) Des pratiques avérées de verrouillage (*lock in*)*

Les très grands acteurs du marché des services de traitement de données (*hyperscalers*) renforcent leur position dominante en multipliant des pratiques techniques, juridiques ou financières visant à verrouiller le marché et empêchent ainsi les utilisateurs de changer de fournisseur ou de recourir à plusieurs fournisseurs (*multicloud*).

Sur un plan **technique**, on relève en particulier le recours à des **formats propriétaires** et l'**absence d'interopérabilité** des données, qui empêchent les services de l'utilisateur de fonctionner dans un environnement *cloud* différent de celui du fournisseur d'origine, ou encore les **fonctionnalités dégradées** d'une application SaaS quand elle est utilisée dans un *cloud* (IaaS) non fourni par son fournisseur de SaaS.

Des moyens **juridiques** sont également utilisés comme l'absence de dispositifs permettant ou prévoyant la transition entre fournisseurs de services de *cloud* ou le recours au *multicloud*. C'est ainsi que les **contrats de long terme** ne comportent souvent **pas de clause de sortie anticipée pour motif légitime**, pas plus qu'ils ne prévoient la **réversibilité**, la **portabilité, ou l'interopérabilité** des données.

Sur un plan **financier**, il apparaît que le coût affiché des transferts de données est particulièrement élevé, ce qui dissuade le client de changer de fournisseur. Le montant des **frais de sortie** imposés (*egrees fees*) est ainsi généralement déconnecté du cout réel de transfert des données.

Par ailleurs, **des avantages** sont **utilisés comme produits d'appels** pour attirer puis retenir le client. Les grands opérateurs distribuent en effet très largement des *credits cloud* qui permettent une utilisation gratuite de leurs services pendant un à deux ans afin de les tester, attirant ainsi les utilisateurs à un stade précoce de leur développement. À l'issue de la période d'essai gratuit, les utilisateurs doivent basculer dans un mode payant pour conserver leur service *cloud* ou s'acquitter de frais de sortie élevés pour changer de fournisseur.

On constate également des **abus de position de marché**. Les *hyperscalers* convertissent ainsi leur position forte au sein d'une couche de leur service de traitement des données en une position dominante au sein d'autres couches, par exemple :

- en empêchant le client d'utiliser un logiciel majeur qu'il propose dans leur *cloud* dans un service proposé par un concurrent ;
- en augmentant les coûts de licence lorsque le logiciel est utilisé dans un autre environnement de traitement des données ;
- en appliquant des mesures de représailles, - par exemple des audits abusifs -, lorsqu'un client tente de changer de fournisseur, de renégocier son contrat ou même d'adopter une stratégie *multicloud* incluant pourtant son fournisseur initial ;
- en pratiquant la vente liée ;
- en proposant des groupements de logiciels incluant leurs services à des prix inférieurs à ceux de la concurrence.

Cette industrie étant relativement récente, la situation concurrentielle n'est pas encore pleinement appréhendée par les pouvoirs publics. Des enquêtes ont toutefois été ouvertes par des autorités de concurrence, notamment en France, au Royaume-Uni et aux Pays-Bas.

L'étude de marché publiée en septembre 2022 par l'Autorité de la concurrence néerlandaise a ainsi constaté que les principaux fournisseurs de services de traitement de données **cherchent désormais à devenir des « guichets uniques »** pour les utilisateurs, ce qui empêche d'autres acteurs de proposer des solutions alternatives.

En outre, la récente législation européenne sur les marchés numériques (*DMA*) et la proposition de règlement sur les données traduisent une volonté croissante des autorités et des pouvoirs publics de se saisir du sujet et d'agir en faveur d'un meilleur fonctionnement concurrentiel du marché des fournisseurs de services de traitement des données.

2. Une ambition forte : supprimer les obstacles au changement de fournisseur

Le chapitre VI de la proposition de règlement entend supprimer les obstacles commerciaux, techniques, contractuels et organisationnels aux changements de fournisseur de services de traitements de données qui permettent aux *hyperscaler*s de verrouiller le marché de l'informatique en nuage.

a) Des obligations imposées au fournisseur initial pour permettre le changement

Le fournisseur initial de services de traitement des données serait désormais soumis à un ensemble d'obligations (art. 23) :

- **permettre au client de résilier le contrat** couvrant le service après un préavis dont la durée ne peut excéder 30 jours calendaires ;
- ne pas l'empêcher de conclure de nouveaux accords avec un autre fournisseur de services de même nature ;
- mettre en œuvre le **portage des données, applications et autres actifs numériques** vers un autre fournisseur de services de traitement de données, à la demande du client ;
- **maintenir l'équivalence fonctionnelle** du service dans l'environnement informatique des différents fournisseurs de services de traitement de données couvrant le même service.

La proposition de règlement détaille en outre certains aspects du cadre juridique, y compris contractuel, et technique (art. 26) du changement de fournisseur.

b) Un changement préparé

Afin de les rendre pleinement opposables, la proposition de règlement prévoit que les droits du client et les obligations du fournisseur de services de traitement de données doivent être clairement énoncés dans un **contrat écrit**, comportant des **clauses permettant** au client **de changer de fournisseur ou de transférer** vers un système sur place les données, applications et actifs numériques qu'il a directement ou indirectement générés.

Afin de préparer un tel changement, le contrat doit en particulier comporter une **spécification exhaustive de toutes les catégories de données et d'applications exportable**s, dont une liste *a minima* est établie (art. 24§1, b) et prévoir un **délai d'extraction** des données à la fin de la période transitoire (art. 24§1, c).

Durant cette période, le fournisseur initial doit apporter son **aide** dans le processus de migration et assurer la pleine **continuité** dans la fourniture des fonctions et services.

c) L'interdiction à terme de facturer des frais de changement

La proposition de règlement interdit dorénavant au fournisseur initial de facturer des frais au client pour le changement de fournisseur (art. 25). La suppression de ces frais ne s'appliquerait toutefois que **progressivemen**t et **à horizon de trois ans**. D'ici là, leur montant ne pourrait pas excéder les coûts directement liés au changement supportés par le fournisseur (art. 25).

3. Il faut appuyer les perspectives de développement d'offres concurrentielles

Les mesures proposées apparaissent de nature à permettre aux clients de pouvoir changer de fournisseur de services de traitement des données lorsqu'ils le souhaitent.

Les rapporteurs de la commission des affaires européennes estiment toutefois que certains compléments pourraient y être utilement apportés afin que le client soit pleinement informé en la matière. Surtout, le calendrier de mise en œuvre du cadre proposé leur paraît devoir être fortement accéléré pour permettre d'atteindre l'objectif de rééquilibrage du marché de l'informatique en nuage.

a) Renforcer l'information du client

Pour que le droit de changer de fournisseur soit effectif, la proposition de règlement définit certaines des clauses qui doivent figurer dans les contrats définissant les relations entre le client et le fournisseur.

Les rapporteurs préconisent de prévoir également une information du client sur les modalités d'exercice de ce droit avant qu'il décide de recourir aux services d'un fournisseur de services de traitement des données, afin qu'il soit informé de ce droit ainsi que des conditions, coûts et modalités de changement de fournisseur.

Préalablement à l'acceptation de son offre, le fournisseur de services de traitement des données doit informer le client des conditions, coûts et modalités de changement de fournisseur.

En raison de la complexité technique de la mise en œuvre du transfert des données et applications et de la période transitoire en cas de changement de fournisseur de services de traitement des données, la proposition de règlement prévoit un accompagnement et une information du client. Les rapporteurs estiment que le contenu et l'objet de cette information devraient être précisés.

Lorsqu'un client demande à changer de fournisseur de services de traitement des données, le fournisseur initial doit lui donner une information précise sur les étapes techniques du processus de migration ainsi que sur les diligences qu'il mettra en œuvre.

Certaines **pratiques** très généralisées devraient par ailleurs être **interdites**. Ainsi en est-il **en particulier des techniques d'appel** qui consistent à proposer une phase d'utilisation gratuite des services à l'issue de laquelle le client ne peut demander à changer de fournisseur.

Le fournisseur de services de traitement des données ne doit pas pouvoir empêcher un client de changer de fournisseur au motif que celui-ci aurait bénéficié d'une phase d'utilisation gratuite de ses services.

b) Prévoir une mise en œuvre rapide de la suppression des frais de sortie

Les rapporteurs de la commission des affaires européennes considèrent excessive la durée du délai - trois ans - prévu par la proposition de règlement pendant lequel serait mise en œuvre progressivement la suppression des frais facturés par le fournisseur initial au client qui décide de recourir à un autre fournisseur de services de traitement des données : une telle durée est de nature à retarder les demandes de changement de fournisseur.

En effet, elle **pénaliserait le développement des nouveaux acteurs, en particulier européens** et briderait la concurrence, confortant ainsi la position dominante des *hyperscalers* sur ce marché, au détriment des utilisateurs.

Le délai de trois ans pendant lequel les fournisseurs initiaux de services de traitement des données doivent progressivement supprimer les frais de sortie en cas de demande de changement de fournisseur empêchera les fournisseurs de services européens de développer leur présence sur le marché intérieur et pénalisera les utilisateurs.

B. DES EXIGENCES ESSENTIELLES EN MATIÈRE D'INTERROPÉRABILITÉ

Pour que des systèmes informatiques puissent interagir avec d'autres produits ou systèmes, il faut qu'ils soient en mesure de fonctionner sans restriction d'accès ou de mise en œuvre.

Dans un contexte de numérisation croissante de l'économie, l'interopérabilité, c'est-à-dire « la capacité d'au moins deux espaces de données ou réseaux de communication, systèmes, produits, applications ou composants d'échanger et d'utiliser des données afin de remplir leurs fonctions »[1], est donc **cruciale pour le bon fonctionnement de l'économie**. Elle **permet en effet de combiner des données provenant de différentes sources à l'intérieur des secteurs et entre les secteurs.**

Le frein majeur à une interopérabilité optimale est l'utilisation de formats dit propriétaires, dont seuls les concepteurs ont les clefs, et l'absence de protocoles de communication. Des règles de cohérence des données et d'interfaces librement utilisables ont été développées mais elles ne sont pas contraignantes[2].

La proposition de règlement impose désormais aux exploitants d'espaces de données, de mécanismes de partage de données et des services dans ces domaines le respect d'un ensemble d'**exigences essentielles d'interopérabilité des données** (art. 28).

Selon une logique similaire, elle définit des exigences essentielles **en matière d'interopérabilité des services de traitement des données** (art. 29) et **en matière de contrats intelligents pour le partage des données** (art. 30), domaines dans lesquels il n'existe pas de normes harmonisées, ou de normes suffisantes en matière d'interopérabilité.

Pour assurer le respect de ces exigences essentielles et favoriser l'**harmonisation des normes afférentes**, la proposition de règlement prévoit que la Commission européenne peut adopter des **actes délégués** pour préciser ces conditions techniques, demander à des organisations européennes de normalisation d'élaborer des normes harmonisées qui satisfont à ces exigences ou encore adopter des **lignes directrices** établissant des spécifications d'interopérabilité pour les services visés.

L'objet des normes harmonisées en matière d'interopérabilité des espaces de données et de mécanismes de partage de données que la Commission européenne est chargée de définir doivent être d'ores et déjà précisés et leur processus d'élaboration détaillé, en particulier le recours à des organismes de normalisation et le rôle des parties prenantes.

---

[1] *Définition figurant à l'article 2§19 de la proposition de règlement*

[2] *Voir notamment l'annexe II du règlement (UE) n° 1025/2021 du Parlement européen et du Conseil du 25 octobre 2012 relatif à la normalisation européenne.*

C. SÉCURISER LES TRANSFERTS INTERNATIONAUX DE DONNÉES À CARACTÈRE NON PERSONNEL

Certains pays extra-européens se sont dotés de lois permettant à leurs juridictions, y compris répressives, ou à leurs administrations, d'obtenir un transfert direct de données à caractère non personnel situées en dehors de leur territoire, y compris dans l'Union. Or ces **demandes de transfert** peuvent ne **pas** être **compatibles avec le droit européen ou avec le droit national, en particulier en matière de protection des droits fondamentaux de la personne** (sécurité ou droit à un recours effectif) ou **des intérêts fondamentaux d'un État membre en matière de sécurité ou de défense nationales**, ou encore être incompatibles avec **la protection de secrets d'affaires ou de droits de propriété intellectuelle**.

1. Des garanties de protection des données détenues sur le territoire européen

La proposition de règlement (art. 27) prévoit des garanties spécifiques de protection des données à caractère non personnel lorsque la demande de transfert de données situées sur le territoire européen n'est pas compatible avec le droit européen ou le droit national d'un État membre.

Dans une telle situation, elle soumet **les fournisseurs de services de traitement de données** à l'**obligation** de prendre « toutes les mesures techniques, juridiques et organisationnelles raisonnables » **afin d'empêcher le transfert hors du territoire européen** de données à caractère non personnel qui y sont détenues ou l'accès de l'État tiers à celles-ci.

Après avoir posé qu'**en l'absence d'accord international**, les fournisseurs de services de traitement de données à caractère non personnel **ne doivent pas procéder à un transfert** de données exigé par une décision ou un jugement d'un juridiction ou une décision d'une autorité administrative d'un pays tiers ni donner accès à ces données, elle autorise **toutefois** de tels transferts ou ouvertures de données **lorsque certaines conditions cumulatives sont respectées** (jugement motivé et proportionnel, examen par un juge de l'objection motivée du destinataire, prise en compte des intérêts juridiques du détenteur des données) (art. 27§3).

Le fournisseur de services de traitement de données peut solliciter l'**avis des autorités nationales compétentes** afin de déterminer si ces conditions sont satisfaites.

Il est enfin prévu que le comité européen de l'innovation dans le domaine des données, mis en place en application du règlement sur la gouvernance des données (*DGA*), assiste la Commission dans l'élaboration de **lignes directrices** sur ce sujet.

2. Il est indispensable de mettre en place des hébergements souverains pour certaines données européennes

La mise en place d'hébergements souverains pour les données n'est pas abordée dans la proposition de règlement. Pourtant, elle s'inscrit dans la suite logique de l'encadrement des transferts internationaux de données qui préoccupe légitimement les entreprises et les citoyens européens[1]. Elle constitue d'ailleurs une **préoccupation forte du Sénat**, qui s'est à plusieurs reprises penché sur le sujet[2].

C'est pourquoi les rapporteurs de la commission des affaires européennes préconisent que soit établie une liste des données sensibles (dont les données de santé) et des données dont la divulgation est susceptible de porter atteinte à la sécurité nationale. Un hébergement souverain est en effet nécessaire pour ces données afin de les protéger contre des applications extraterritoriales de législations extra-européennes ou d'intrusions malveillantes.

Ils soulignent en outre que le caractère souverain exige que le service soit fourni par une **entreprise européenne dans laquelle les participations étrangères cumulées, directes ou indirectes**, ne puissent être que **marginales**.

Une liste des données sensibles (dont les données de santé) et des données dont la divulgation est susceptible de porter atteinte à la sécurité nationale doit être établie et un hébergement souverain mis en place pour les protéger contre des applications extraterritoriales de législations extra-européennes ou d'intrusions malveillantes.

IV. UNE SUPERVISION CONFIÉE À DES AUTORITÉS NATIONALES

La mise en œuvre et l'application du règlement est confiée à des autorités nationales compétentes, qui devront agir en coordination avec les autorités compétentes en matière de protection des données à caractère personnel et les autorités sectorielles.

---

[1] *Notamment en France à la suite du choix par l'État de Microsoft pour l'hébergement des données médicales des Français (* Health Data Hub *).*

[2] *Voir notamment le rapport d'information du Sénat n°678 (2020-2021 du 10 juin 2021* La cybersécurité des entreprises - Prévenir et guérir : quels remèdes contre les cyber virus ?*, présenté par MM. Sébastien Meurat et Rémi Cardon, au nom de la délégation aux entreprises.*

A. UNE SUPERVISION ORGANISÉE À L'ÉCHELLE NATIONALE

Les missions et pouvoirs des autorités que les États membres devront désigner devront être clairement définis par les États membres et inclure un ensemble d'éléments (art. 31§3) en matière :

- d'information des utilisateurs ;
- de traitement des réclamations ;
- de suivi du respect des obligations prévues par le règlement (en particulier la réalisation d'enquêtes, y compris sur le respect de la suppression des frais de sortie en cas de changement de fournisseur de services de traitement des données) ;
- de sanctions (y compris la possibilité d'engager des procédures judiciaires) ;
- de coopération avec les autorités compétentes des autres États membres.

Un volet répressif devra également être prévu, comportant des sanctions administratives (financières), éventuellement assorties d'astreintes, et des amendes.

Pour plus d'efficacité, le pouvoir des autorités nationales de contrôle de prononcer des injonctions éventuellement assorties d'astreintes en cas de persistance d'un comportement constituant un manquement aux obligations prévues par le règlement pourrait utilement être complété par la possibilité d'imposer des remèdes aux professionnels défaillants.

B. UNE ARTICULATION DIFFICILE ENTRE LES DIFFÉRENTES AUTORITÉS NATIONALES CONCERNÉES

La désignation des autorités nationales compétentes sera complexe, dans la mesure où **les données visées** par la proposition de règlement **peuvent contenir certaines données à caractère personnel**. Or, le recueil et l'utilisation de celles-ci sont soumis à des règles européennes spécifiques, sous le contrôle des autorités indépendantes nationales créées à cet effet.

Il en est de même, comme le rappelle la proposition de règlement, pour les données sectorielles qui relèvent de la compétence d'autorités nationales sectorielles.

Ainsi que l'a souligné la CNIL (Commission nationale de l'informatique et des libertés) lors de son audition par les rapporteurs, les États membres devront organiser avec précision les modalités de coopération entre ces différentes autorités, dans le respect de leurs attributions respectives, particulièrement s'ils décident que l'autorité indépendante nationale chargée de veiller à la protection des données à caractère personnel

n'est pas compétente pour contrôler l'application du règlement sur les données.

C. PRÉVOIR LA MISE EN PLACE D'UNE STRUCTURE DE COORDINATION INTRA-EUROPÉENNE

Dans la mesure où le règlement sera applicable à des données produites au sein du marché intérieur et que celles-ci peuvent en principe librement circuler dans l'espace européen, la proposition de règlement prévoit des obligations d'échanges d'informations et de coopération entre les autorités nationales de contrôle qui seront désignées par les États membres pour assurer la supervision de sa mise en œuvre.

Afin de faciliter la coopération et la coordination entre les autorités nationales de contrôle, y compris les autorités compétentes en matière de protection des données à caractère personnel, les rapporteurs sont favorables à la mise en place d'un cadre d'échanges formalisé.

Pour renforcer l'efficacité de la coopération intra européenne en matière de données qu'appelle une mise en œuvre efficace et coordonnée du règlement sur les données, il apparaît nécessaire de prévoir la mise en place d'une structure de coordination, réunissant des représentants des autorités nationales de contrôle concernées.

CONCLUSION

Les rapporteurs de la commission des affaires européennes partagent les objectifs de la proposition de règlement européen sur les données, qui leur paraît pouvoir être complétée et précisée sur plusieurs points afin d'en renforcer l'effectivité.

Ils attirent l'attention sur la nécessité d'une articulation pertinente entre ouverture et sécurité des données, pour assurer la protection des données sensibles et des données dont la divulgation est susceptible de porter atteinte à la sécurité nationale, et appellent à la mise en place rapide d'un hébergement souverain.

EXAMEN EN COMMISSION

La commission des affaires européennes s'est réunie le jeudi 11 mai 2023, sous la présidence de M. Jean-François Rapin, président, pour l'examen du présent rapport.

M. Jean-François Rapin, président. – Mes chers collègues, les technologies numériques tiennent une place désormais centrale dans nos vies quotidiennes et transforment profondément l'économie et la société. Leur développement ouvre de formidables perspectives, mais favorise également des comportements préjudiciables. Il crée en outre des tensions, dans un univers interconnecté mondialisé, dominé par de très grands acteurs, le plus souvent américains ou chinois.

L'Union européenne (UE) s'attelle à construire une régulation du numérique dans le marché intérieur, pour protéger ses citoyens et ses valeurs et pour assurer le respect des règles de concurrence. Elle a ainsi récemment adopté plusieurs législations importantes, dont le règlement relatif aux marchés contestables et équitables dans le secteur numérique. Cette législation sur les marchés numériques, le *Digital Markets Act* (DMA), vise à rétablir la concurrence mise à mal sur le marché intérieur par les pratiques abusives des grandes plateformes qualifiées de « contrôleurs d'accès », en encadrant leurs comportements de domination et d'éviction.

Afin que ne soit pas praticable en ligne ce qui est interdit hors ligne, l'Union européenne a également adopté une législation sur les services numériques, le *Digital Services Act* (DSA), qui encadre les activités des plateformes afin de lutter contre la haine en ligne, la manipulation, la désinformation ou la vente de produits contrefaits.

Nous avons déjà eu l'occasion d'étudier ces textes européens et d'adopter des résolutions pour en renforcer la portée et l'efficacité. D'ailleurs, le Sénat examinera bientôt le projet de loi déposé hier par le Gouvernement pour assurer leur transposition en droit national.

En complément du DMA et du DSA, la Commission européenne a aussi présenté, le 19 février 2020, deux stratégies européennes : l'une dédiée à l'intelligence artificielle (IA), l'autre aux données. Dernièrement, en mars, c'est l'intelligence artificielle qui a mobilisé notre commission, afin de contribuer à ce que son déploiement sur notre continent respecte les valeurs européennes.

L'objet de notre réunion de ce jour est d'aborder l'autre volet : le sujet des données, souvent qualifiées d'« or noir » à l'ère numérique. Mme Blatrix Contat, Mme Morin-Desailly et M. Gattolin vont nous présenter la stratégie européenne en la matière et, plus spécialement, leur rapport sur la proposition de règlement européen sur les données, le *Data Act*.

Mme Florence Blatrix Contat, rapporteure. – Nous allons effectivement vous présenter aujourd'hui le volet législatif de la stratégie européenne pour les données visant à réduire les obstacles de différentes natures auxquels se heurte la construction en cours du partage des données au sein de l'UE.

La Commission a identifié un certain nombre de barrières qui empêchent la libre circulation effective des données au sein de l'Union, au premier rang desquelles la faible confiance dans le partage des données. Elle a également constaté que des pratiques de verrouillage empêchent les personnes, physiques ou morales, d'exercer pleinement leurs droits à accéder aux données générées par l'utilisation d'objets connectés et de services numériques liés, à en suivre l'utilisation et à en permettre la réutilisation dans les écosystèmes numériques. En effet, des déséquilibres en termes de pouvoir de marché permettent aux contrôleurs d'accès de concentrer les données et d'imposer unilatéralement des conditions d'accès et d'utilisation qui en empêchent le partage.

La Commission a en outre constaté que la réutilisation des données se heurte à des obstacles techniques significatifs en raison de difficultés d'interopérabilité et de qualité des données, en l'absence de normes impératives en la matière. Elle a par ailleurs identifié des problématiques liées à la disponibilité des données, en particulier des données du secteur public, et à la collecte de données dans l'intérêt commun.

Enfin, elle n'a pu que constater que la souveraineté européenne sur les données n'est pas assurée. En raison du rôle marginal des fournisseurs européens de *cloud*, les fournisseurs étrangers opérant dans l'UE jouent un rôle prédominant, alors même qu'ils sont soumis à la législation applicable aux États tiers, avec les risques en résultant en matière de protection des données et de cybersécurité.

Pour remédier à ces insuffisances, la Commission a publié une stratégie européenne pour les données, destinée à mettre en place un espace européen des données, dont les règles communes et les mécanismes d'application doivent tout à la fois garantir les points suivants : la circulation des données à l'intérieur du marché unique et entre les secteurs, dans le respect des règles et valeurs européennes, en particulier la protection des données à caractère personnel – fil rouge du texte – ; une concurrence efficace sur le marché intérieur, en prévoyant des règles d'accès et d'utilisation des données équitables, pratiques et fiables ; des mécanismes de gouvernance des données clairs et fiables ; enfin, une approche ouverte des flux internationaux de données, mais affirmée et fondée sur les valeurs européennes.

Les actions proposées par la Commission reposent sur quatre piliers : des mesures horizontales trans-sectorielles pour l'accès aux données et leur utilisation ; des investissements dans les données et le renforcement des capacités et des infrastructures européennes pour l'hébergement, le traitement et l'utilisation des données ainsi que leur interopérabilité ; le développement des compétences en matière numérique ; le développement d'espaces européens communs des données dans des secteurs économiques stratégiques et des domaines d'intérêt public, en particulier les données relatives au pacte vert, en matière de santé, de mobilité, ou encore d'énergie.

Après le récent règlement sur la gouvernance des données, dit *Data Governance Act*, qui est destiné à faciliter la réutilisation des données du secteur public, et qui sera applicable à compter du 24 septembre prochain, la proposition de règlement sur les données, dite *Data Act*, sur laquelle nous nous penchons aujourd'hui, s'inscrit dans le premier pilier. En effet, elle définit un cadre juridique et technique horizontal pour permettre une répartition plus équitable de la valeur des données industrielles entre les acteurs de l'économie des données.

Les données concernées sont les données produites par l'utilisation d'objets connectés et de services liés. Point important : il s'agit donc de données primaires, non traitées, ce qui devrait d'ailleurs être plus clairement précisé dans le texte, comme nous le préconisons dans la proposition de résolution que nous vous soumettrons. Le volume de ces données connaît depuis quelques années un développement exponentiel en raison du nombre croissant d'objets connectés : 8 milliards d'objets en 2019, 13,8 milliards attendus en 2024. Or ces données, qualifiées d'industrielles, sont peu exploitées en Europe. Lors de son discours de 2020 sur l'état de l'Union, la présidente de la Commission européenne a ainsi précisé que 80 % d'entre elles ne sont pas utilisées. D'où le grand intérêt de ce texte.

M. André Gattolin, rapporteur. – Le *Data Act* prévoit un droit d'accès et de partage encadré. Il reconnaît aux utilisateurs des objets connectés des droits sur les données produites par leur utilisation de ces objets et de services liés. Il fixe des règles harmonisées en matière d'accès, d'utilisation et de partage de ces données entre entreprises et consommateurs et interentreprises. Enfin, il définit les obligations des détenteurs des données tenus de rendre des données disponibles.

Nous avons donc affaire à trois protagonistes : l'utilisateur de l'objet connecté et de services liés, qui peut être une personne physique – un consommateur –, ou une personne morale – une entreprise – ; le détenteur des données produites par cet objet, qui en est généralement le fabricant ; le destinataire des données, entreprise tierce désignée par l'utilisateur en raison de son activité, afin qu'il puisse utiliser les données à des fins précises, notamment de réparation de l'objet connecté.

L'utilisateur de l'objet connecté se voit reconnaître un double droit sur les données générées par son utilisation de l'objet connecté et des services liés : un droit d'accès gratuit et un droit d'utilisation, y compris pour les partager avec des tiers.

La proposition de règlement précise la portée du droit d'accès de l'utilisateur aux données, y compris en termes de qualité des données. Elle prévoit des mesures pour en faciliter la mise en œuvre, en particulier l'obligation de prévoir l'accès aux données dès la conception, dit *by design*, et d'assurer la protection de la confidentialité et de la sécurité des données.

Le partage des données avec un tiers désigné par l'utilisateur est également encadré : les données transférées doivent présenter un niveau de qualité identique ; une compensation raisonnable des coûts de mise à disposition peut être facturée ; l'utilisation des données est limitée aux fins et conditions convenues avec l'utilisateur, pour la fourniture d'un service ; profilage et manipulation des données sont prohibés. Un dispositif de règlement des conflits est prévu en cas de litige.

Enfin, il est proposé de corriger les déséquilibres contractuels constatés en rééquilibrant le pouvoir de négociation des micro, petites et moyennes entreprises dans les contrats de partage de données et en écartant les grandes plateformes du bénéfice de ce partage.

Plusieurs points doivent être précisés. Nous proposons tout d'abord d'affirmer fermement la primauté des règles de protection des données à caractère personnel, en particulier du règlement général sur la protection des données (RGPD) et de la directive sur la protection de la vie privée dans le secteur des communications électroniques. De telles données à caractère personnel peuvent en effet être mêlées aux données dont nous parlons.

Une attention toute particulière doit en outre être portée aux situations dans lesquelles les données sont celles non pas de l'utilisateur titulaire, mais, par exemple, d'un salarié ou d'un membre tiers du foyer.

Deuxième point d'attention : il faut assurer l'effectivité des droits des utilisateurs sur les données. Cela suppose en particulier que le format des données soit compréhensible, structuré, habituel et lisible par la machine et que les métadonnées nécessaires à leur interprétation soient communiquées. Nous proposons de rendre obligatoire le respect de ces exigences techniques.

Dans un souci d'équilibre de la relation contractuelle entre l'utilisateur et le détenteur des données, nous préconisons par ailleurs que soient identifiées des clauses abusives afin de les priver d'effet.

S'agissant du partage des données avec des tiers, il nous semble pertinent de maintenir l'exclusion proposée des grandes plateformes dites « contrôleurs d'accès » en raison de leur pouvoir de marché excessif. Je signale toutefois que ce point est contesté par certaines entreprises, au nom de la cohérence du fonctionnement des chaînes de valeur.

Afin d'équilibrer les accords de partage conclus entre le détenteur des données et le tiers utilisateur, il est prévu de rendre inopposables un ensemble de clauses considérées comme abusives, ce qui, là encore, nous paraît pertinent. La compensation des coûts de mise à disposition des données devrait toutefois être mieux encadrée.

Venons-en maintenant à un sujet particulièrement sensible : la protection des secrets d'affaires. Qui dit protection ne dit pas refus de communiquer des données pour ce motif – le texte ne l'autorise pas –, mais interdiction de les utiliser à des fins concurrentielles – ce qui est prévu –, et mise en place de mesures de protection, en particulier contractuelles, ce qui est également prévu. Encore faudrait-il que ces mesures n'excèdent pas les besoins légitimes d'assurer cette protection.

Nous vous proposons malgré tout de considérer que, dans certains cas exceptionnels, la protection de secrets d'affaires puisse justifier un refus de transmettre les données. Notre attention a ainsi été attirée sur la possibilité de déduire de données brutes des éléments clés sur les dispositifs de sécurité inclus dans le produit connecté – c'est notamment le cas dans le domaine de l'aviation. Pour justifier un refus en pareil cas, le détenteur des données devrait démontrer que leur divulgation est de nature à avoir des conséquences dommageables graves, y compris au regard de la sécurité.

J'en viens à un point particulier : l'accès d'autorités publiques nationales et européennes à des données en cas d'urgence publique. Un chapitre du *Data Act* est consacré à la mise à disposition de ces autorités de données détenues par le secteur privé, en cas de besoin exceptionnel.

Trois situations sont considérées comme constitutives d'un tel besoin exceptionnel : lorsque les données sont nécessaires pour réagir à une urgence publique ; lorsqu'elles sont nécessaires pour prévenir une telle urgence ou contribuer au rétablissement à la suite d'une telle urgence ; lorsque l'absence de données disponibles empêche l'organisme de s'acquitter d'une mission d'intérêt public prévue par la loi et qu'il ne lui a pas été possible d'obtenir ces données par d'autres voies.

Je ferai plusieurs observations. Tout d'abord, l'urgence publique est définie comme une situation exceptionnelle qui a des conséquences négatives pour la population de l'Union, d'un État membre ou d'une partie de celui-ci, entraînant un risque de répercussions graves et durables sur les conditions de vie, la stabilité économique ou la situation d'actifs économiques. Nous vous proposons de demander que la nature de l'urgence soit précisée en indiquant expressément quelles sont les circonstances

visées : santé, catastrophe, cyberattaque, par exemple. Les conséquences de la situation exceptionnelle justifiant l'exercice de ce droit d'utilisation des données doivent également être précisées. Il est ainsi préférable de parler d'atteinte à la stabilité financière ou à des actifs économiques majeurs, plutôt que de faire référence à la « stabilité économique » ou la « situation d'actifs économiques ».

La troisième situation visée par la proposition de règlement – l'absence de données disponibles empêchant l'organisme de s'acquitter d'une mission d'intérêt public – est recevable, mais il nous semble qu'elle doit être plus précisément encadrée, qu'il s'agisse de la durée et de la portée de la mise à disposition des données, de la démonstration de l'impossibilité de trouver ces données et de l'obligation de ne les utiliser que pour les seules finalités de la demande, dans le strict respect des droits et libertés des personnes.

Mme Catherine Morin-Desailly, rapporteure. – Le second objectif du texte est de permettre une mobilité effective et sécurisée des données.

Trois dimensions de cette mobilité sont ainsi traitées : le changement de fournisseur de services de traitement des données, autrement dit de *cloud* ; la définition des conditions techniques permettant cette mobilité, autrement dit la portabilité et l'interopérabilité des données ; enfin la sécurisation des flux internationaux de données.

S'agissant de la mise en œuvre du droit de changer de fournisseur de *cloud*, la proposition de règlement s'attaque à une vraie difficulté. Le marché de l'informatique en nuage est fortement concentré : 72 % du marché européen est ainsi contrôlé par trois fournisseurs américains, Microsoft Azure, AWS et Google Cloud, ce qui laisse peu de place aux fournisseurs européens, dont la part relative tend à régresser rapidement. La raison en est un fort lobbying de ces trois acteurs et un déficit de politique industrielle volontariste pour accompagner le développement du *cloud* européen.

Ces acteurs dominants, dits *hyperscalers*, ont recours à des pratiques de verrouillage qui empêchent les utilisateurs de changer de fournisseurs et, par voie de conséquence, le développement de concurrents. Ces pratiques sont techniques, juridiques et financières, en particulier le recours à des formats propriétaires et la facturation de frais de sorties très élevés. Les personnes auditionnées ont particulièrement insisté sur ce point.

On constate également des abus de position de marché. Ces très grands acteurs convertissent ainsi leur position forte au sein d'une couche du *cloud* – câbles, *data centers*, serveurs ou logiciels de traitement – en une position dominante au sein d'autres couches, par exemple en recourant à la vente liée, ou en appliquant des mesures de représailles. Vous trouverez des détails à ce sujet dans notre rapport d'information.

Pour supprimer les obstacles commerciaux, techniques, contractuels et organisationnels au changement de fournisseur de services de traitements de données, le chapitre VI de la proposition de règlement soumet le fournisseur initial de services de traitement des données à un ensemble d'obligations et met en place un cadre de préparation et d'accompagnement du changement. Enfin, il prévoit une interdiction progressive de facturer des frais de changement à horizon de trois ans.

Les mesures proposées permettront aux clients de pouvoir changer de fournisseur de services de traitement des données lorsqu'ils le souhaitent. Certains compléments pourraient toutefois y être utilement apportés, afin que le client soit pleinement informé en la matière, y compris avant l'acceptation de l'offre de service. Il devrait également être précisément informé sur les étapes du processus de migration et les diligences à mettre en œuvre.

Par ailleurs, il conviendrait d'interdire au fournisseur de services de traitement des données d'empêcher un client de changer de fournisseur au motif qu'il aurait bénéficié d'une phase d'utilisation gratuite de ses services. Peut-on même admettre ces pratiques de gratuité, forme de *dumping* ? Telle est la question que nous nous sommes aussi posée.

Quant au délai de mise en œuvre de la suppression des frais de sortie – trois ans –, il nous paraît difficilement acceptable, sauf à anéantir toutes velléités concurrentielles sur le marché intérieur.

Venons-en maintenant à l'interopérabilité. La combinaison de données provenant de différentes sources à l'intérieur des secteurs et entre les secteurs ne peut être mise en œuvre si les espaces de données ne sont pas interopérables. Le frein majeur à une interopérabilité optimale est l'utilisation de formats dits propriétaires et l'absence de protocoles de communication.

La proposition de règlement impose aux exploitants – d'espaces de données, de mécanismes de partage de données et des services dans ces domaines – un ensemble d'exigences essentielles en matière d'interopérabilité des données et d'interopérabilité des services de traitement des données, ainsi qu'en matière de contrats intelligents pour le partage des données, autant de domaines dans lesquels il n'existe pas de normes harmonisées, ou de normes suffisantes en la matière. Il est prévu que des normes harmonisées soient publiées. Sans doute serait-il utile de préciser d'ores et déjà l'objet de ces normes et leur processus d'élaboration, en particulier le rôle des parties prenantes.

J'en viens à la sécurité des données en cas de transferts internationaux, dernier point crucial traité par la proposition de règlement, en raison de l'application extraterritoriale de leurs lois par des États tiers sur des données européennes, en méconnaissance du droit européen ou du droit national, en particulier en matière de protection des droits fondamentaux de

la personne, des intérêts fondamentaux d'un État membre pour des raisons tenant à la sécurité ou la défense nationales, aux secrets d'affaires ou aux droits de propriété intellectuelle.

En l'absence d'accord international – le régime de transferts de données entre l'Union européenne et les États-Unis, dit *Privacy Shield*, a été invalidé – , la proposition de règlement prévoit des garanties spécifiques de protection des données, et soumet les fournisseurs de services de traitement de données à l'obligation de prendre « toutes les mesures techniques, juridiques et organisationnelles raisonnables » afin d'empêcher le transfert hors du territoire européen de données à caractère non personnel qui y sont détenues ou l'accès d'un État tiers à celles-ci.

Il s'agit indiscutablement d'une démarche positive. Mais rappelons que, étant donné la législation américaine, incluant le *Foreign Intelligence Surveillance Act* (FISA) et le *Cloud Act*, nous aurons beau voter toutes les législations possibles, dès que nous aurons affaire à un fournisseur de la *Big Tech*, le transfert des données sera rendu obligatoire. Il nous semble donc tout aussi indispensable d'établir une liste de données sensibles et de données dont la divulgation est susceptible de porter atteinte à la sécurité nationale que de doter l'Europe d'infrastructures souveraines sécurisées, qui ne soient pas contrôlées par des capitaux étrangers.

J'en viens au dernier sujet : la supervision de la mise en œuvre du règlement. Elle est organisée au niveau national et doit être confiée à des autorités dotées de pouvoirs de surveillance, d'injonction, astreinte et de sanctions. Ces pouvoirs pourraient être utilement complétés par la possibilité d'imposer des remèdes aux professionnels défaillants. Par ailleurs, dès lors que des données à caractère personnel sont en cause, une attention particulière devra être portée à l'articulation entre ces autorités chargées de superviser l'application du règlement sur les données et celles qui sont en charge de la protection de ces données personnelles. Enfin, pour renforcer l'efficacité de la coopération intra-européenne en matière de données, qui est nécessaire à une mise en œuvre efficace et coordonnée du règlement, la mise en place d'une structure de coordination, réunissant des représentants des autorités nationales de contrôle concernées nous paraît s'imposer.

Voilà l'ensemble de nos préconisations, rassemblées dans la proposition de résolution européenne que nous vous soumettons.

Pour conclure, je précise que, dans le projet de loi sur le numérique que le Gouvernement vient de déposer sur le bureau du Sénat à l'initiative du ministre Jean-Noël Barrot, est présente par anticipation la question des fournisseurs de services de traitement de données, notamment de l'interopérabilité et du transfert des données.

M. Jean-François Rapin, président. – Je vous remercie pour votre grande expertise, sur des sujets certes austères, mais dont le retentissement sera considérable. La transposition à venir que constitue le texte du ministre Barrot devra s'inspirer de vos travaux, dont j'ai rappelé l'importance.

M. André Reichardt. – La proposition de règlement est essentielle, et votre proposition de résolution l'est tout autant. J'y souscris pleinement.

Cependant, l'alinéa 29 ne devrait-il pas plutôt indiquer que le service de communication électronique est exclu du champ d'application de la proposition de règlement ? Cela serait plus clair et plus simple que la rédaction proposée.

Par ailleurs, vous me semblez trop prudents, à l'alinéa 46, sur le renforcement de la protection des droits de l'utilisateur. Ne devrions-nous pas préconiser l'interdiction de certaines clauses, plutôt que demander à examiner l'opportunité d'une telle interdiction ? Selon moi, les clauses abusives devraient être considérées comme non écrites.

Mme Catherine Morin-Desailly, rapporteure. – Nous avons privilégié cette formulation parce qu'il faut d'abord identifier de telles clauses, ce qui reste à faire.

M. André Reichardt. – Enfin, dès lors qu'on autorise les autorités publiques nationales et européennes à accéder aux données en cas d'urgence, il faut préciser la nature de celle-ci. Ainsi, à l'alinéa 68, ne faudrait-il pas définir des éléments quantitatifs, s'agissant de la temporalité de l'urgence et de ses conséquences ? En particulier, à quoi renvoie la notion d'« actifs économiques majeurs » ? Il faut encadrer au maximum l'accès à ces données. L'urgence doit être objective.

M. Jean-François Rapin, président. – Il y a l'urgence liée au numérique, mais aussi celle qui relève d'un état de catastrophe.

M. Didier Marie. – En cas de crise majeure, l'urgence est appréciée par l'État membre et pas par la Commission européenne. La proposition de règlement est une simple couche d'harmonisation. Mais la définition de l'urgence n'est pas harmonisée au niveau européen.

Mme Florence Blatrix Contat, rapporteure. – L'urgence est déjà encadrée par la proposition de règlement et les compléments que nous proposons d'y apporter. Peut-on aller au-delà ? Par définition, on ne peut pas prévoir tous les cas d'urgence.

M. André Gattolin, rapporteur. – On n'aurait pas imaginé la pandémie avant 2019…

Mme Pascale Gruny. – N'oublions pas l'effet sur la recherche d'un trop grand verrouillage de l'accès aux données.

M. André Reichardt. – Cela étant, je salue votre travail, soutenu et détaillé. Il est d'autant plus nécessaire au regard du contenu du projet de loi visant à sécuriser et réguler l'espace numérique présenté hier en conseil des ministres.

M. Jean-François Rapin, président. – Nous ne devons pas prêter le flanc aux critiques sur le respect de la subsidiarité. À chaque État membre de définir l'état d'urgence. Pouvons-nous demander plus d'harmonisation en ce domaine ? Je n'en suis pas certain.

M. André Reichardt. – Ce n'est pas ce que je propose : il s'agit plutôt de définir un cadre temporel de l'urgence, quitte à avoir des variantes de délais au sein de ce cadre, d'un État à l'autre.

M. Jean-François Rapin, président. – À qui s'en remettre, alors, pour une telle définition ? Au Conseil ?

Mme Catherine Morin-Desailly, rapporteure. – J'observe que la notion d'urgence présentait les mêmes difficultés de définition pour l'instrument d'urgence pour le marché intérieur. Peut-être y a-t-il d'ailleurs une articulation à trouver avec ce texte, ainsi qu'avec tous les textes sectoriels prévoyant des situations d'urgence, comme en matière de santé. Je ne suis pas certaine qu'on puisse aller plus loin en l'état.

En revanche, il faut distinguer les urgences concernant tout le marché intérieur, et celles qui frappent un État membre seulement. Dans ce dernier cas, la définition relève de la compétence nationale. On peut envisager l'obligation harmonisée de fixer une durée à l'urgence, mais aller au-delà risquerait de porter atteinte au principe de subsidiarité.

M. André Gattolin, rapporteur. – Peut-être pourrions-nous, à l'alinéa 68, mentionner parmi les exemples la notion d'une crise majeure. En outre, la proposition de règlement prévoit l'accès aux données pour prévenir –et non seulement traiter- une situation d'urgence. Le risque lié aux régimes d'exception me semble surtout important sur ce point.

Mme Catherine Morin-Desailly, rapporteure. – Selon le *c* du 1 de l'article 17 de la proposition de règlement, la durée d'utilisation des données doit être précisée. La répétition, même si elle est à la base de la pédagogie, est-elle bien nécessaire ?

M. André Reichardt. – Chat échaudé craint l'eau froide : nous voyons bien comment la deuxième vague pandémique, en France, avait conduit notre ministre de la santé à prolonger l'état d'urgence sanitaire, sous le prétexte effrayant d'une charge virale mille fois plus grande. L'autorité nationale peut prendre tout type de décision.

M. Jean-François Rapin, président. – Je ne vois pas l'autorité européenne s'y substituer.

M. André Reichardt. – Tout à fait, mais il s'agit de créer un garde-fou pour les autorités publiques, nationales comme européennes. Il faut selon moi préciser la notion d'urgence.

M. Jean-François Rapin, président. – À nouveau, j'alerte sur la nécessité de respecter le principe de subsidiarité.

M. André Gattolin, rapporteur. – Lors d'un déplacement sur place en septembre 2020, avec Jean Bizet et Jean-Yves Leconte, nous avions constaté que les décisions d'urgence prises en Hongrie ont annihilé la capacité des collectivités locales, notamment la mairie de Budapest, à exécuter leur budget, empêchant l'opposition à Viktor Orban de démontrer sa capacité à agir. Le recours à l'état d'urgence varie singulièrement d'un pays à l'autre.

Mme Catherine Morin-Desailly, rapporteure. – Nous n'avons pas vocation à définir l'urgence. Nous pourrions toutefois compléter l'alinéa 68 par les mots : « et que sa durée soit encadrée. »

M. André Gattolin, rapporteur. – Il faut en effet que la durée de telles mesures soit limitée.

M. André Reichardt. – Très bien.

Il en est ainsi décidé.

Mme Pascale Gruny. – Avec Laurence Harribey et Patricia Schillinger, nous travaillons actuellement sur la régulation en matière de données de santé. La protection des données de santé est fondamentale, mais celles-ci sont essentielles à la recherche. Tout en comprenant André Reichardt, je souligne l'importance de ne pas bloquer l'accès à ces données.

Mme Florence Blatrix Contat, rapporteure. – L'utilisation des données à des fins de recherche est déjà prévue dans le texte, et ce même en dehors de situation d'urgences.

M. Jean-François Rapin, président. – Nous sommes malheureusement très en retard sur les données de santé. Chaque application de santé prévoit des clauses d'acceptation par l'utilisateur du transfert de ses données, hors de tout contrôle…

Mme Catherine Morin-Desailly, rapporteure. – En principe, ces données sont anonymisées, mais les données françaises sont gérées par des acteurs extra européens. C'est pourquoi nous demandons que soit établie une liste des données sensibles. La Commission nationale de l'informatique et des libertés (Cnil) recommande d'ailleurs de trouver rapidement des solutions souveraines, qui sont à notre portée.

Mme Pascale Gruny. – La commission des affaires sociales travaille aussi sur ce sujet. La plateforme européenne attend la mise en œuvre de la plateforme française.

L'anonymisation est associée au numéro d'inscription au répertoire (NIR, ou numéro de sécurité sociale), qui permet donc de retrouver la personne concernée. On risque de perdre l'anonymat. Les personnes auditionnées nous confirment qu'on ne pourra jamais se protéger de toutes les attaques conduites par des *hackers*.

M. Jean-François Rapin, président. – J'ajoute que le Sénat est attaqué depuis plusieurs jours. Soyez prudents… Vendredi, notre site était d'ailleurs inaccessible.

Mme Catherine Morin-Desailly, rapporteure. – André Reichardt demandait à préciser l'alinéa 29. Votre proposition de remplacer les mots : « n'est pas un service numérique lié à un objet connecté relevant » par les mots : « est exclu du champ » ne pose pas de souci. Appelons un chat un chat.

Il en est ainsi décidé.

M. Pierre Ouzoulias. – Je me réjouis que la commission des affaires européennes du Sénat soit pilote sur ces sujets complexes et irrigue les travaux des autres commissions. Après six ans, nous ne connaissons toujours pas la position du Gouvernement en la matière. Nous votons, deux à trois fois par an, des lois rendues obsolètes par les directives et règlements européens. Ainsi, le 12 juillet 2022, à l'occasion de l'examen du projet de loi portant diverses dispositions d'adaptation au droit de l'Union européenne en matière de prévention de la diffusion de contenus à caractère terroriste en ligne, le Gouvernement m'avait assuré que les prochains règlements européens ne remettraient pas en cause le texte que nous votions. Tel n'a pas été le cas, et le projet de loi qui vient d'être déposé ne fait que prolonger cette incompréhension.

Je tiens beaucoup à votre mention de l'interopérabilité dans la proposition de résolution. Les citoyens doivent avoir une alternative lorsque leurs réseaux sociaux et *clouds* ne sont pas conformes à leurs valeurs. Or, aujourd'hui, nous en sommes prisonniers, car nous ne pouvons retirer nos données de ces opérateurs.

Enfin, nous ne pouvons faire l'économie d'une politique industrielle et d'investissements massifs.

M. André Gattolin, rapporteur. – Nous le disons depuis dix ans !

Mme Catherine Morin-Desailly, rapporteure. – Considérez-vous normal que les fournisseurs de service d'informatique en nuage continuent à formuler des offres gratuites, jusqu'à un certain seuil, pour appâter et enserrer le client ? Il est difficile de sortir de ce qui s'apparente à du *dumping*.

M. André Gattolin. – L'internet s'est fondé sur le mythe de la gratuité. Les entreprises se rétribuent sur les données, la publicité ou l'abonnement, voire, en position dominante, sur l'ensemble des vecteurs. La gratuité, en elle-même, pose problème dans un système concurrentiel dès

lors qu'elle emprisonne le client. Lors de son audition, OVHcloud, nous a rappelé que cette technique d'enfermement l'empêche de prospérer dans les secteurs où il est le plus concurrentiel. La suppression progressive, sur trois ans, des frais de changement d'opérateur émane sans doute du *lobby* des grands groupes internet à Bruxelles.

J'ai demandé à la Commission européenne qui étaient réellement les membres de DIGITALEUROPE : à de rares exceptions près, comme Dassault Systèmes, ils étaient à 90 % américains. Désormais, les Chinois, avec TikTok et Huawei, y sont présents en force. Alors que, depuis la directive sur le commerce électronique, on refuse les barrières pour ne pas gêner le développement d'un internet européen, avec notamment le principe de non-responsabilité des hébergeurs, on n'a fait que renforcer les opérateurs internationaux sur le marché européen.

Cependant, il ne fait pas de doute que la Commission est sous pression. Ainsi, lors des travaux sur la directive Vie privée et communications électroniques, les trente principaux cabinets d'avocats spécialisés dans le droit du numérique à Bruxelles étaient déjà sous contrat avec Google ou ce qui deviendrait Meta. Nous sommes juridiquement désarmés. La production du droit est en cours de « désouverainisation ».

Mme Catherine Morin-Desailly, rapporteure. – Seuls les Gafam – Google, Apple, Facebook, Amazon, Microsoft – peuvent proposer des offres véritablement gratuites. Ils captent les marchés par anticipation, notamment *via* l'Éducation nationale : c'est une concurrence déloyale au *cloud* européen. Je vous rappelle aussi que nos marchés sont ouverts aux quatre vents, quand ceux des États-Unis nous sont fermés. Sans symétrie, nous continuerons à scier la branche, déjà bien fragile, sur laquelle nous sommes assis.

M. Jean-François Rapin, président. – Le sujet émergent est celui des objets connectés. Un échelon est franchi avec la voiture autonome. On vous impose un opérateur, en général un Gafam, lors de l'achat du véhicule. Ainsi, un compte Google est requis pour faire fonctionner l'Austral de Renault. Nous sommes rattrapés par la patrouille, hors de toute réglementation.

Mme Catherine Morin-Desailly, rapporteure. – C'est tout l'enjeu des systèmes propriétaires.

M. André Gattolin. – Je souligne qu'il y a un défaut de vision globale en raison de l'emboîtement des législations européennes. Il est impératif de veiller à leur articulation..

La commission adopte la proposition de résolution européenne, ainsi modifiée, disponible en ligne sur le site du Sénat, ainsi que l'avis politique qui en reprend les termes et qui sera adressé à la Commission européenne et au Parlement européen, et autorise la publication du rapport d'information.

PROPOSITION DE RÉSOLUTION EUROPÉENNE

Le Sénat,

Vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Programme de travail de la Commission pour 2020 - Une Union plus ambitieuse », COM(2020) 37 final,

Vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, « Une stratégie européenne pour les données » du 19 février 2020, COM(2020) 66 final,

Vu la résolution du Parlement européen du 25 mars 2021 sur une stratégie européenne pour les données /2217(INI), (2021/C 494/04),

Vu la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques),

Vu la proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (directive vie privée et communications électroniques), COM/2017/010 final,

Vu le 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 95/46/CE (règlement général sur la protection des données - RGPD),

Vu la directive (UE) 2016/943 du Parlement européen et du Conseil du 8 juin 2016 sur la protection des savoir-faire et des informations commerciales non divulgués (secrets d'affaires) contre l'obtention, l'utilisation et la divulgation illicites,

Vu le règlement (UE) 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne,

Vu la directive (UE) 2018/1972 du Parlement européen et du Conseil du 11 décembre 2018 établissant le code des communications électroniques européen,

Vu le règlement (UE) 2022/868 du Parlement européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (règlement sur la gouvernance des données),

Vu la proposition de règlement du Parlement européen et du Conseil fixant des règles harmonisées pour l'équité de l'accès aux données et de l'utilisation des données (règlement sur les données) COM(2022) 68 final,

Des objectifs pertinents

Considérant que la présence généralisée d'objets connectés dans les sphères privées et publiques produit de très nombreuses données dont la croissance est exponentielle ;

Considérant que ces données ouvrent des perspectives particulièrement prometteuses pour stimuler l'innovation dans de nombreux secteurs ;

Considérant que les utilisateurs des objets connectés et des services liés n'ont généralement pas accès, pour des raisons techniques et commerciales, aux données produites par l'utilisation de ces objets et services ;

Considérant que ces données sont souvent utilisées par leurs détenteurs à d'autres fins que celles qui en justifient le recueil et ce sans que les utilisateurs en soient pleinement informés ;

Considérant que les grands acteurs du numérique tendent à empêcher les micro, petites et moyennes entreprises d'accéder aux données dans des conditions satisfaisantes alors que ces données leur permettraient de développer de nouveaux services, dans un cadre concurrentiel équilibré ;

Soutient le principe de la mise en place d'une législation européenne horizontale définissant des règles harmonisées pour un accès équitable aux données produites par l'utilisation d'objets connectés et de services liés, et prévoyant des processus de règlement des litiges ;

Approuve en particulier l'objectif de transparence en matière de recueil de ces données et la reconnaissance de droits effectifs aux consommateurs et aux entreprises sur les données qu'ils produisent en utilisant des objets connectés et des services liés ;

Soutient également l'objectif d'un partage choisi de ces données avec des tiers, dans un cadre contractuel équilibré qui permet au tiers bénéficiaire de ne pas être soumis à des exigences excessives par le détenteur des données ;

Est également favorable à l'adoption de règles permettant de procéder effectivement à un changement de fournisseur de services de traitement des données et à l'encadrement des transferts internationaux de données à caractère non personnel ;

Estime toutefois que, pour atteindre ses objectifs, la proposition de règlement doit être précisée et complétée sur plusieurs points ;

Attire l'attention sur la nécessaire articulation de cette législation transversale avec les régimes sectoriels existants et à venir, par exemple en matière de données de santé ;

Souhaite, qu'au-delà de la reconnaissance des droits des consommateurs sur les données générées par les objets connectés et les services liés qu'ils utilisent, les règles européennes en matière de protection des consommateurs fassent l'objet d'une évaluation générale de leur pertinence dans un environnement de plus en plus numérique et que des adaptions et compléments y soient apportés afin d'assurer une meilleure protection des consommateurs en ligne ;

Préciser le champ d'application du règlement

Considérant que la proposition de règlement concerne les données « générées par l'utilisation d'un produit, y compris incorporé dans un bien immeuble, ou d'un service lié » ;

Préconise qu'il soit indiqué explicitement qu'il s'agit de produits connectés, et, que les données concernées sont des données brutes, non modifiées ni ajoutées, résultant directement de l'utilisation de ces objets ou de services liés ;

Demande qu'il soit en outre précisé que le service de communication électronique, qui est régi par des textes spécifiques, est exclu de champ d'application de la proposition de règlement ;

Veiller à la primauté des règles de protection des données à caractère personnel

Considérant que les données recueillies par des objets connectés et des services liés peuvent inclure des données à caractère personnel ;

Considérant que le recueil et l'utilisation de telles données sont encadrés par plusieurs textes européens dont le RGPD et la directive vie privée et communications électroniques ;

Préconise qu'il soit précisé que la définition des données à caractère personnel susceptibles d'être présentes dans les données recueillies par des objets connectés et des services liés est celle du RGPD ;

Estime préférable qu'il soit expressément indiqué que, pour les données à caractère personnel figurant parmi les données recueillies, les règles européennes applicables en matière de données à caractère personnel prévalent en toute hypothèse sur les dispositions de la proposition de règlement, sous le contrôle de l'autorité nationale de protection des données compétente ;

Considérant que l'utilisateur de l'objet connecté peut ne pas être la personne dont des données à caractère personnel sont recueillies ;

Souligne qu'il convient d'être particulièrement vigilant en pareil cas et que le détenteur des données doit veiller à ce que la transmission de ces données à l'utilisateur soit effectuée dans le strict respect du RGPD ;

Renforcer la protection des droits des utilisateurs sur les données produites par l'utilisation d'objets connectés et de services liés

Considérant qu'il est proposé de reconnaître à l'utilisateur d'un objet connecté et de services liés un droit d'accès aisé, sécurisé et direct sur les données produites par l'utilisation qu'il fait de l'objet et des services liés ;

Considérant que cet accès devra être prévu techniquement dès la conception de l'objet connecté ;

Demande, pour que l'accessibilité soit effective, qu'il soit exigé que le format des données soit compréhensible, structuré, habituel et lisible par la machine, et que les métadonnées nécessaires à leur interprétation soient communiquées à l'utilisateur ;

Estime qu'il devrait également être précisé que, lorsqu'elles ne sont pas directement accessibles, les données doivent être mises à la disposition de l'utilisateur sans délai indu et présenter une qualité technique équivalente en termes de réutilisation, de sécurité et de format ;

Considérant que la proposition de règlement prévoit que l'utilisateur soit informé, préalablement à l'acquisition de l'objet connecté et des services liés, des données que leur utilisation produira, des modalités d'accès à ces données, de l'utilisation qui en sera faite et de leur éventuelle ouverture à un tiers ou encore du droit d'introduire une plainte auprès de l'autorité compétente ;

Considérant qu'elle prévoit également que l'utilisateur soit préalablement informé, le cas échéant, de l'existence de secrets d'affaires et de droits de propriété intellectuelle et de leurs conséquences pour l'exercice de son droit d'utiliser et de partager ces données avec un tiers ;

Considérant qu'il est prévu que le détenteur des données ne puisse utiliser celles-ci que dans le cadre d'un accord contractuel conclu avec l'utilisateur du produit connecté et des services liés ;

Considérant que la proposition de règlement prévoit qu'il est expressément interdit au détenteur des données d'utiliser celles-ci pour évaluer la situation économique, les actifs ou les méthodes de production de l'utilisateur ;

Préconise que soient identifiées des clauses qui porteraient une atteinte injustifiée aux droits de l'utilisateur en matière d'utilisation et de partage des données et que soit examinée l'opportunité de les interdire et de les priver d'effet ;

Faciliter le partage des données avec des tiers

Considérant que l'utilisateur d'un objet connecté ou de services liés est en droit de demander au détenteur des données ainsi générées que celles-ci soient mises à la disposition d'un tiers ;

Considérant que la proposition de règlement prévoit que les contrôleurs d'accès soient exclus du bénéfice, direct ou indirect, d'un tel partage de données ;

Estime que cette exclusion est justifiée au regard du pouvoir de marché excessif de ces opérateurs ;

Considérant que la proposition de règlement prévoit que les micro et petites entreprises ne soient pas soumises à l'obligation de mise à disposition des données sauf si elles ont des entreprises partenaires ou des entreprises liées ;

Estime que les micro et petites entreprises ayant un lien avec un fabricant de produits connectés ou un fournisseur de services liés devraient également être soumises à cette obligation ;

Invite à l'ouverture d'une réflexion sur la pertinence de l'application des seuils de droit commun en termes de chiffres d'affaires, de bilan et de nombre de salariés pour qualifier ces entreprises, et sur l'opportunité de prendre en compte à cet effet le nombre de données générées par les objets connectés et services liés qu'elles mettent à disposition ;

Considérant que la proposition de règlement prévoit que le détenteur des données qui met celles-ci à la disposition d'un tiers veille à leur qualité et à leur sécurité ;

Considérant que la proposition de règlement prévoit que les conditions de cette mise à disposition convenues entre le détenteur des données et un tiers bénéficiaire doivent être équitables, raisonnables, non discrétionnaires et transparentes ;

Approuve le fait que certaines clauses qui réduisent l'accès de PME aux données et la possibilité de les utiliser soient prohibées et considérées comme inopposables;

Considérant que la proposition de règlement prévoit d'autoriser que la mise à disposition des données fasse l'objet d'une compensation raisonnable et non discriminatoire à la charge du tiers bénéficiaire dont le détenteur des données doit fournir les bases de calcul ;

Demande que, pour prévenir les risques d'abus, la marge qui peut être facturée au tiers bénéficiaire soit plus précisément encadrée que par la seule exigence d'un caractère raisonnable et non discriminatoire ;

Veiller à une protection équilibrée des secrets d'affaires et prendre en compte les impératifs de sécurité

Considérant que la proposition de règlement prévoit que le détenteur des données et l'utilisateur du produit connecté et de services liés doivent s'accorder sur les mesures techniques et opérationnelles à mettre en place pour assurer la protection des secrets d'affaires avant l'ouverture des données ;

Considérant qu'elle indique que de de telles mesures doivent également être prévues en cas de partage des données avec un tiers ;

Considérant que la proposition de règlement interdit expressément à l'utilisateur et au tiers bénéficiaire d'utiliser les données recueillies pour développer des produits concurrents ;

Souligne que le cadre contractuel de protection de secrets d'affaires susceptibles d'être révélés par des données brutes en cas de demande d'accès et de transmission de celles-ci doit être équilibré et ne pas excéder les exigences de protection de tels secrets ;

Estime toutefois que la protection des secrets d'affaires doit pouvoir exceptionnellement justifier un refus de transmettre les données, y compris à l'utilisateur, si le détenteur des données démontre que leur divulgation est de nature à avoir des conséquences dommageables sérieuses, y compris au regard de la sécurité ;

Encadrer l'accès d'autorités publiques nationales et européennes à des données en cas d'urgence publique

Considérant qu'aux termes de la proposition de règlement, les détenteurs de données pourraient être dans l'obligation, en cas d'urgence publique, de mettre des données générées par l'utilisation d'objets connectés et de services liés à la disposition d'un organisme public national ou de l'Union européenne démontrant un besoin exceptionnel d'utiliser ces données pour faire face à une urgence, prévenir une telle urgence ou pour contribuer au rétablissement à la suite d'une telle urgence ;

Considérant que l'urgence publique est définie par la proposition de règlement comme « une situation exceptionnelle ayant une incidence négative sur la population de l'Union, d'un État membre ou d'une partie de celui-ci, entraînant un risque de répercussions graves et durables sur les conditions de vie ou la stabilité économique, ou la détérioration substantielle d'actifs économiques dans l'Union ou dans les États concernés » ;

Souhaite que soient précisées la nature de l'urgence, pour viser expressément diverses circonstances (santé, catastrophe naturelle, catastrophe majeure d'origine humaine, cyberattaque), ses conséquences (y compris sur la stabilité financière ou des actifs économiques majeurs) et que sa durée soit encadrée ;

Estime que l'obligation d'ouverture des données hors cas d'urgence publique, lorsque l'absence de données disponibles empêche l'organisme ou l'institution publics de s'acquitter d'une mission spécifique d'intérêt public, doit être précisément encadrée, en particulier sa durée et sa portée, afin de ne pas priver abusivement des entreprises des bénéfices qu'elles peuvent légitimement retirer de l'exploitation des bases de données qu'elles ont constituées ;

Souligne que cette mise à disposition ne doit être requise que si les autorités publiques concernées justifient qu'elles ne sont pas en mesure d'obtenir rapidement ces données par d'autres moyens ;

Demande qu'il soit précisé que les organismes publics ne peuvent utiliser les données que pour la seule finalité de la demande, et dans le strict respect des droits et libertés des personnes, en particulier lorsqu'il s'agit de données à caractère personnel qui ne peuvent être anonymisées ;

Renforcer l'effectivité du droit de changer de fournisseur de services de traitement des données

Considérant que les principaux fournisseurs de services de traitement actifs en Europe sont de très grandes entreprises étrangères qui exercent une position dominante sur le marché intérieur et ont développé des pratiques pour empêcher leurs utilisateurs d'utiliser d'autres logiciels que ceux qu'elles proposent et de se tourner vers d'autres fournisseurs ;

Considérant que la proposition de règlement entend supprimer les obstacles commerciaux, techniques et contractuels au changement efficace de fournisseur de services de traitement des données ;

Demande que le fournisseur de services de traitement des données soit tenu de communiquer, préalablement à l'acceptation de l'offre de traitement des données, des informations précises sur les conditions, coûts et modalités de changement de fournisseur;

Souhaite qu'il soit expressément indiqué que le transfert des données ne doit pas pouvoir être refusé ou retardé lorsque le client a bénéficié d'une offre d'utilisation gratuite des services de traitement des données ;

Estime que la complexité technique de ce transfert et de la période transitoire ainsi que l'impératif de continuité du service exigent une information précise du client sur les étapes techniques du processus de changement de fournisseur et les droits et obligations des différentes parties ;

Considérant qu'il est prévu que la suppression progressive des frais de changement de fournisseur s'étale sur trois ans à compter de l'entrée en vigueur du règlement ;

Estime qu'en raison de sa durée un tel délai est de nature à empêcher les fournisseurs de services européens de développer leur présence sur le marché intérieur qui est de plus en plus dominé par de grands acteurs étranger ;

Veiller au respect des valeurs et des intérêts européens dans les flux internationaux de données

Considérant que les transferts internationaux de données ne doivent pas exposer les données à un risque d'être rendues accessibles à des autorités étrangères qui ne seraient pas liées aux États européens par un accord international assurant la protection des données à caractère personnel, de la propriété intellectuelle, des secrets d'affaires, des engagements de confidentialité et des données commercialement sensibles ;

Considérant que la proposition de règlement fait obligation aux fournisseurs de services de traitement de données de vérifier la licéité de toute demande d'accès ou de transfert de données non personnelles émanant d'une autorité étrangère, de s'assurer de sa proportionnalité et de l'existence d'une possibilité de contestation devant une juridiction compétente du pays tiers ;

Considérant qu'il est prévu que le fournisseur destinataire d'une telle demande doit consulter les autorités ou organismes compétents notamment lorsqu'il estime que la décision peut concerner des données commercialement sensibles ou porter atteinte aux intérêts de l'Union, ou de ses États membres en matière de sécurité nationale ou de défense ;

Considérant que la proposition de règlement impose aux fournisseurs de prendre toutes les mesures techniques, juridiques et organisationnelles raisonnables, y compris des accords contractuels, afin d'empêcher l'accès aux données et leur transfert à des autorités d'États tiers qui ne seraient pas liés par un tel accord dès lors que cet accès ou ce transfert serait contraire au droit de l'Union ou d'un État membre ;

Approuve la définition de règles dictées par le souci d'assurer le respect des valeurs et des intérêts européens dans les flux internationaux de données ;

Demande que soit établie une liste des données sensibles (dont les données de santé) et des données dont la divulgation est susceptible de porter atteinte à la sécurité nationale, pour lesquelles un hébergement souverain est nécessaire afin de les protéger d'une application extraterritoriale de législations extra-européennes ;

Souligne que le caractère souverain exige en particulier que le service soit fourni par une entreprise européenne dans laquelle les participations étrangères cumulées, directes ou indirectes, ne peuvent être que marginales ;

Développer des normes en matière de portabilité et d'interopérabilité des données

Considérant que l'interopérabilité des données et leur portabilité sont nécessaires pour pouvoir échanger et utiliser les données d'espaces et de systèmes de données distincts ;

Considérant qu'il est prévu que des actes d'exécution seront pris par la Commission pour définir des règles harmonisées en la matière ;

Invite à préciser plus avant l'objet de ces normes harmonisées d'interopérabilité et de portabilité des données et à en détailler le processus d'élaboration, en particulier le rôle des États membres et des organismes de normalisation ;

Veiller à l'efficacité de la supervision de la mise en œuvre du règlement

Considérant que les États membres doivent désigner les autorités nationales compétentes pour suivre la mise en œuvre du règlement, traiter les réclamations et infliger des sanctions en cas de manquement ;

Attire l'attention sur la nécessaire coordination au sein des États membres entre les différentes autorités nationales, en particulier les autorités compétentes en matière de protection des données à caractère personnel ;

Préconise que les autorités nationales compétentes soient dotées de la possibilité d'imposer des remèdes en cas de non-respect des obligations prévues par le règlement ;

Demande qu'une structure de coordination intra-européenne soit mise en place pour faciliter la mise en œuvre du règlement.

Invite le Gouvernement à faire valoir cette position dans les négociations

ANNEXE

Le règlement sur la gouvernance européenne des données[1] pour faciliter la réutilisation des données du secteur public

Un plus grand nombre de données détenues par le secteur public seront éligibles au droit de réutilisation à compter du 24 septembre 2023, y compris des données protégées par la confidentialité commerciale, le secret statistique, les droits de propriété intellectuelle de tiers et certaines données à caractère personnel, pour que celles-ci servent, *in fine*, à améliorer la productivité et à stimuler l'innovation.

Pour faciliter la réutilisation de ces données, une obligation d'assistance du demandeur est prévue, chaque État membre devant créer un point d'information unique destiné à fournir aux réutilisateurs potentiels des informations sur les données détenues par les autorités publiques. Un point d'information unique sera également mis en place au niveau européen par la Commission. Pour permettre une disponibilité maximale de ces données détenues par les organismes publics, il est interdit aux organismes publics de conclure des accords d'exclusivité de réutilisation des données par un, sauf exceptions liées à l'intérêt public.

Le règlement crée par ailleurs un nouveau modèle commercial encadré : le service d'intermédiation de données qui vise à « établir des relations commerciales à des fins de partage de données entre un nombre indéterminé de personnes concernées et de détenteurs de données, d'une part, et d'utilisateurs de données, d'autre part, par des moyens techniques, juridiques ou autres, y compris aux fins de l'exercice des droits des personnes concernées en ce qui concerne les données à caractère personnel ». Afin de garantir leur neutralité, et renforcer ainsi la confiance dans le partage des données, ces intermédiaires ne devront pas exercer une autre activité et l'accès à leurs services, leurs conditions ainsi que les prix pratiqués devront respecter des principes d'équité, de transparence et de non-discrimination. Les personnes souhaitant exercer une telle activité devront le notifier à l'autorité nationale compétente, qui les autorisera à l'exercer et à utiliser le label de « Prestataire de services d'intermédiation de données reconnu dans l'Union ».

Enfin, l'altruisme en matière de données[2] est encouragé et encadré : les entités qui mettent à disposition des données doivent ainsi répondre à un

---

[1] *Règlement (UE) 2022/868 du Parlement Européen et du Conseil du 30 mai 2022 portant sur la gouvernance européenne des données et modifiant le règlement (UE) 2018/1724 (*Data Governance Act*).*

[2] *Il est défini comme le « partage volontaire de données fondé sur le consentement donné par les personnes concernées au traitement de données à caractère personnel les concernant, ou l'autorisation accordée par des détenteurs de données pour l'utilisation de leurs données à caractère non personnel sans demander ni recevoir de contrepartie qui aille au-delà de la compensation des coûts qu'ils supportent lorsqu'ils mettent à disposition leurs données, pour des objectifs d'intérêt général prévus par le droit national » (art. 2).*

ensemble de conditions telles qu'exercer leurs activités dans un but non lucratif et être juridiquement distinctes de toute entité exerçant des activités à but lucratif, afin, là encore, de renforcer la confiance dans le partage des données.

LISTE DES PERSONNES ENTENDUES

Services de l'État

Secrétariat général aux affaires européennes (SGAE)

M. Benoit CATZARAS, secrétaire général adjoint

Mme Christine CABUZEL-DUVALLON, adjointe au chef du bureau marché intérieur : industrie – recherche et innovation – numérique et espace

Mme Constance DELER, cheffe du bureau Parlement

Direction générale des entreprises (ministère de l'économie et des finances)

M. Pierre SERRA, service de l'économie numérique, économie de la donnée et régulation du *cloud*

Autorité de régulation

Commission nationale de l'informatique et des libertés (CNIL)

M. Bertrand PAILHES, directeur des technologies et de l'innovation

Mme Najma BICHARA, juriste au service des affaires européennes et internationales

Mme Chirine BERRICHI, chargée des relations avec le Parlement

Syndicats professionnels

Digitaleurope

M. Julien CHASSERIAU, *senior manager for IA and Data Policy*

Mme Béatrice ERICSON, *officer for privacy and security policy*

Organisations non gouvernementales (ONG)

Bureau européen des unions de consommateurs (BEUC)

Mme Mayant Fernandez Perez, *senior Digital Policy Officer*

Entreprises

OVHcloud

Mme Solange VIEGAS DOS REIS, directrice juridique

Mme Blandine EGGRICKX, responsable des affaires publiques