Loi européenne sur les données (Data Act)
Contribution de Numeum

Dans la continuité de la stratégie européenne en matière de données lancée en février 2020, la Commission européenne a présenté le 23 février un règlement sur les données, aussi appelée « Data Act ».

Les données jouent aujourd'hui un rôle clé dans l'économie et la société et elles constituent un actif stratégique et économique pour les entreprises françaises. Leur traitement, y compris dans le cadre de transferts internationaux, est donc majeur pour le développement économique (intelligence artificielle, internet des objets, développement à l'international, etc.). Dans un contexte de plus en plus digitalisé et mondialisé, les échanges avec des pays situés en UE et hors UE sont devenus incontournables, que ce soit du fait de l'implantation ou de la présence de nos entreprises françaises à l'étranger ou de leurs activités dans plusieurs domaines de l'économie (santé, industrie, etc.).

Dans ce contexte, Numeum soutient les efforts de la Commission européenne pour identifier les leviers les plus adéquats pour le partage de données au sein de l'UE et leur transfert au niveau mondial, lever les obstacles règlementaires, et pour promouvoir des mécanismes de partage volontaire de données.

En complément de sa réponse à la consultation européenne de septembre 2021, Numeum a souhaité formuler dans ce document des éléments de contribution sur la base du texte publié le 23 février. Notre organisation souhaite poursuivre son implication vis-à-vis des travaux et des réflexions conduits par la Commission européenne, le Parlement et le Conseil dans le cadre de cette initiative.

A retenir

Clarifier le périmètre et les définitions : Il semble nécessaire que le champ d'application de la proposition, les définitions et la distinction entre les acteurs soient précisés. (1) Le champ d'application du Data Act manque de clarté et de précision au regard des définitions trop larges, plus particulièrement concernant la nature et les typologies de données concernées, avec le risque d'induire de l'insécurité juridique. (2) Les définitions des mots clés doivent être alignées entre les différents textes (RGPD, DGA, AI Act) et ne pas se contredire.

Comprendre la chaîne de valeur du partage de données : Il est nécessaire de comprendre le cheminement de la donnée et le statut de chaque acteur, notamment dans le cadre de chaînes complexes d'objets connectés et de services connexes, tels qu'observées dans le champ industriel.

Préciser les règles de portabilité des services de cloud : Nous accueillons favorablement l'idée de faciliter le changement de fournisseur pour les utilisateurs de ces services. Si le Data Act vise à corriger une asymétrie observée sur le marché européen entre clients/utilisateurs et fournisseurs de services, l'imprécision des termes ne semble pas à ce stade offrir de garanties suffisantes pour assurer la correction de cette asymétrie.

Assurer la cohérence règlementaire : Il conviendra d'assurer une cohérence entre les différents textes législatifs en cours et à venir (RGPD, Data Governance Act, AI Act, espaces européens de données, etc.).

Veiller à l'accompagnement des entreprises (notamment les plus petites) : Elles auront besoin de conseils et de processus simples et rationalisés pour être en mesure de répondre aux exigences. Des coûts de mise en conformité élevés pourraient être attendus.

1. Dispositions générales (champ d'application et définitions)

L'objectif initial de la proposition de règlement « Data Act » est d'exploiter pleinement le potentiel des données de l'Internet des objets (IoT) en faveur d'une économie des données, équitable et innovante. **Numeum se félicite des enjeux portés par ce texte qui permettra de stimuler le développement d'un marché des données concurrentiel, d'ouvrir des perspectives pour l'innovation fondée sur les données et de nouveaux services innovants dans ce secteur des objets connectés.**

Numeum est convaincu de l'importance et de la nécessité d'encourager l'utilisation généralisée des données de l'IoT. Ces données ne sont certes pas pleinement exploitées en raison d'un certain nombre de facteurs (techniques, juridiques et organisationnelles) mais des mécanismes d'échanges de données doivent être mis en place et surtout précisés en vue de stimuler les acteurs du marché, plutôt que d'élaborer des mécanismes contraignants. En effet, une approche volontaire permet d'obtenir des collaborations plus fructueuses tout en préservant les garde-fous nécessaires pour les entreprises souhaitant protéger leurs secrets commerciaux. Pour cela, des mesures au niveau européen apportant un soutien et des incitations aux entreprises pour le partage des données doivent être créées.

Toutefois, la portée et le champ d'application du Data Act ne sont pas clairement identifiés. Les définitions des données sont trop larges et pourraient engendrer des risques d'insécurité juridique. Il est également **difficile de déterminer à ce stade quelles sont les données couvertes par la proposition de règlement alors que l'objectif initial de la Commission était de se limiter aux données de l'IoT**.

Par ailleurs, Numeum souhaiterait obtenir une plus grande clarté sur la façon dont le Data Act s'articule et complète l'initiative de la Commission européenne pour créer des espaces communs de données dans des domaines stratégiques dans le cadre d'un grand marché unique des données (cf. au *Commission Staff Working Document on Common European Data Spaces* du 23 février 2022).

Mieux définir les parties prenantes dans l'émission et l'usage des données

Un flou demeure entre les différents textes concernant la définition précise des parties prenantes qui entourent la donnée rattachée aux objets connectés : « détenteur de l'IoT », « utilisateur de l'IoT », « data subject », « data holder », « data contrôler », etc.

A titre d'exemple, dans le cadre d'un dispositif médical utilisé en milieu hospitalier, la répartition de ces rôles respectifs n'est pas claire entre les parties prenantes qui sont, le fabricant, l'hôpital, le patient, Cette question est importante pour le partage des données mais également pour préciser les obligations de consentement qui les précèdent. Si nous prenons ici l'exemple de la e-santé, la question se pose également dans tous les autres secteurs de l'économie.

Clarifier le champ d'application des données

Les différentes notions et termes applicables au Data Act devront être clairement définies. Il est essentiel de délimiter les types de données concernées, le cas échéant, de les différencier entre les différents chapitres, en adoptant une taxonomie cohérente de part en part du projet. En l'état actuel, plutôt que clarifier, le texte risquerait de créer davantage d'ambiguïté et d'insécurité juridique tout en affaiblissant les protections des données et les secrets commerciaux des entreprises.

Or la lecture de cette proposition de règlement suscite des interrogations :

- Les dispositions concernent-elles les données brutes et/ou traitées, personnelles et/ou non personnelles, le statut de propriété, etc. ?

- Quelle est la définition de l'IoT ? Il conviendra impérativement de définir avec précision ce que recouvrera les notions d'IoT (les assistants vocaux entrent-ils dans le champ d'application du texte ?) et de contrats intelligents.
- Les définitions de « produit » et de « service connexe » ne semblent-elle pas plus larges que les données de l'IoT ?
- La multiplicité des sujets traités dans un même texte, avec des champs d'application différents en fonction des chapitres rend complexe la compréhension.
- La régulation doit également préciser ce qui en est des données industrielles et commerciales ?
- Données issues des machines-outils, systèmes embarqués professionnels, capteurs, etc.

Qu'il s'agisse des chapitres relatifs au partage de données en B2B, B2C ou B2G, la définition des données générées par les utilisateurs doit être basée sur les pratiques du secteur.

Il est nécessaire de **distinguer la donnée brut**e (résultat d'une mesure analogique isolée, non traitée, non contextualisée) **de la donnée traitée** (information interprétée et contextualisée au regard d'une finalité). En effet, dans ce dernier cas, la donnée est le résultat de la transformation de données brutes du fait d'un savoir-faire ou d'une expérience afin de répondre à un usage spécifique, ce qui nécessite un investissement initial (financier, technique ou humain) pour les entreprises. Seules les données brutes devraient être accessibles et faire l'objet de partage. Notons toutefois que ces dernières ont pour vocation d'être transformées en données traitées.

La définition de données visée à l'article 2 pourrait être complétée pour définir les données comme dans les considérants 14 et 17. Dans un souci de cohérence, il est **également nécessaire de préciser la notion de données visée dans le chapitre sur la portabilité du cloud.**

- Si les données brutes générées par un produit entrent dans le champ d'application, les informations dérivées ou déduites des données brutes ne devraient pas en faire partie.

- Le considérant 17 suggère que le règlement exige la capacité de l'utilisateur à avoir accès aux données brutes générées par le produit (mais pas aux informations déduites des données par un processus logiciel qui calcule des données dérivées) qui sont soumises aux droits de propriété intellectuelle.

Continuer à protéger les secrets d'affaires

La proposition prévoit la divulgation de secrets commerciaux aux utilisateurs, aux tiers et aux organismes publics dans des conditions permettant de préserver la confidentialité du secret commercial. Toutefois, elle n'indique pas comment les intérêts légitimes des détenteurs de données seraient protégés en cas d'utilisation illicite par des tiers ni comment le détenteur de données en aurait même connaissance. Il semble que la charge de la preuve de l'existence d'un tel abus incomberait au détenteur initial des données, ce qui pourrait être difficile en pratique.

- Les données couvertes par le secret des affaires devraient être exemptes de toute obligation de partage de données. **Il serait également opportun de clarifier explicitement qu'il n'y a aucune obligation de partager des secrets commerciaux.** Cela n'empêcherait pas les entreprises de partager des informations de manière confidentielle lorsque les garanties qu'elles jugent appropriées sont en place.
- En outre, il nous semble opportun de ne pas limiter le champ des données pouvant ne pas être divulguées en raison du seul secret des affaires, notion définie étroitement et surtout de manière différente dans les divers Etats Membres. Il convient d'y inclure les éléments relatifs à la **propriété intellectuelle et au savoir-faire**, les éléments rendant lisibles les **stratégies et les comportements des entreprises sur leur marché** aux fins d'éviter de biaiser le comportement

des concurrents et de garantir le libre-jeu de la concurrence basée sur les mérites et l'innovation, et enfin les éléments nécessaires à la **sécurité des systèmes d'information**.

De la nécessité de clarifier les définitions et le champ d'application

Le périmètre de la proposition de règlement étant couvert par les articles 1 et 2, ces articles devraient fournir des éléments suffisants pour mieux appréhender les périmètres des grandes thématiques abordées dans chaque chapitre de la proposition.

L'article 1(1) mentionne le partage de données en B2B/B2C/B2G mais ne fait aucune référence aux sections V à VII. De même, l'article 2 ne définit qu'approximativement mention de certaines notions importantes présentes dans les chapitres V et VII, notamment la nomenclature des données couvertes par le partage de données. Les termes définis à l'article 2 laissent une large place à l'interprétation, ce qui nuirait à la sécurité juridique du texte. En outre, les considérants les faisant résonner avec des concepts présents dans d'autres législations (tel que le RGPD) sans s'appuyer sur les définitions que ces autres législations ont adopté, une clarification est nécessaire pour assurer une meilleure lisibilité de la norme, une plus grande sécurité juridiques.

Détenteur de données (data holder)

A titre d'exemple, la définition du détenteur de données considère que « *le contrôle de la conception technique ou des services connexes* » crée la capacité de mettre des données à disposition. Cette formulation ne semble pas saisir que la conception technique du produit peut entraver ou limiter la portée d'un service connexe. Lorsque le produit et les services connexes sont conçus par des entités différentes, la capacité de rendre les données disponibles est incertaine et pourrait s'avérer impossible pour le fournisseur de services connexes qui est lui-même lié par la capacité du produit dans lequel il est intégré. Il est nécessaire de prendre en considération qu'un produit peut inclure divers services connexes, provenant de divers fournisseurs (parfois concurrents), choisis à la discrétion du concepteur du produit ou de son utilisateur (lorsqu'il s'agit d'une entreprise). Les produits de l'IoT industriel doivent être intégrés dans un environnement logiciel susceptible d'évoluer en permanence, qui comprend divers fournisseurs, dont le concepteur peut ne pas connaître tous les fournisseurs de manière exhaustive.

Il convient par conséquent de mieux définir qui a le contrôle des données et de préciser le concept de détenteur de données (*data holder*).

- Un acteur qui développe et commercialise un logiciel utilisé par un client dans un dispositif IoT est-il considéré comme un détenteur de données ? A titre d'exemple, un développeur de logiciels à usage général n'a pas le droit d'accéder aux données générées par l'utilisation d'un dispositif IoT.

- Ici, la manière dont un détenteur de données doit s'assurer que les données d'un utilisateur sont conservées en sécurité par un tiers n'est pas claire.

- Le même type de critères devrait s'appliquer aux données personnelles et non personnelles. A la lecture du texte, il semble que le concept de data holder soit défini différemment selon si l'on se réfère à l'article 2(6) ou aux considérants 21 et 24.
    - L'article 2(6) expose que, lorsqu'il s'agit du traitement de données non personnelles, toute entité ayant la capacité technique de fournir des données est considérée comme un détenteur de données.

    - Le considérant 21 définit la notion de détenteur de donnés de manière très extensive puisqu'il expose qu'un fournisseur de services cloud qui stocke les données générées par des dispositifs IoT serait également assimilé à un détenteur de données, et serait donc tenu de partager des données non personnelles relatives à ses clients (le

fabriquant de dispositifs IoT – la plupart du temps) avec des tiers. Cela va à l'encontre des dispositions contractuelles et techniques des fournisseurs de services cloud, selon lesquelles les données ne sont pas partagées, sauf sur instruction explicite du client. Toute exception à ce principe nuirait grandement à la confiance dans le secteur.

- A l'inverse, le considérant 24 donne une définition beaucoup plus restrictive puisqu'il expose que lorsqu'il s'agit de traitement de données personnelles, le détenteur de données devrait être un responsable de traitement (*data controller*) en vertu du RGPD.

- Il convient de se demander **comment doit s'apprécier le statut de détenteur de données dans le cadre de chaînes complexes d'objets connectés et de services connexes**, tels qu'ils se développent dans le champ industriel. En effet, des objets connectés peuvent tout à la fois :
  - Récupérer des données collectées par d'autre objets connectés situés en amont,
  - En collecter par eux-mêmes,
  - Les transformer,
  - Les communiquer à d'autres objets connectés en aval.

  Ces objets peuvent tous comporter des services connexes déployés par des producteurs d'objets différents. Ils peuvent également comporter des services connexes fournis par des opérateurs différents.

Services connexes (related services)

- La définition des services connexes reste très large et n'aborde pas la délimitation des responsabilités entre les parties prenantes de la chaîne de valeur qui sont les mieux placées pour donner accès aux données. En particulier, la définition des services connexes est assez large et pourrait potentiellement inclure des services de traitement des données (par exemple, des services IoT ou d'IA) pour lesquels les utilisateurs du cloud ont également un droit d'accès en vertu du chapitre V sur la portabilité du cloud. Il existe un risque évident de chevauchement et de redondance entre ces dispositions qui visent à atteindre le même objectif. Etant donné que la plupart des services connexes des appareils connectés sont et seront davantage basés sur le cloud, cela soulève la question de savoir si les services connexes devraient être retirés du champ d'application du Data Act afin de garantir une meilleure sécurité juridique.

- En outre, dans le cadre de chaine complexe d'objets connectés et de services connexes, tels qu'ils se développent dans le champ industriel, la question de l'identification de ce qu'est un service connexe est difficile, et le partage de données IoT dans ce cadre comporte un risque très élevé de communication de données appartenant à des tiers. Dans le cadre des services cloud B2B, les fournisseurs n'étant pas en mesure de contrôler, analyser, modifier les données communiquées par leurs clients, il leur est impossible de déterminer si une donnée appartient bien à l'utilisateur désigné et non à un tiers (de type sous-traitant ou fournisseur de l'utilisateur).

Services de traitement de données

En ce qui concerne les définitions applicables aux dispositions des chapitres 6 et 8, les nouvelles références aux « services de traitement de données », au « type de service » et à « l'équivalence fonctionnelle » devraient également être plus clairement délimitées et définies. En effet, cette terminologie risque de créer une confusion avec le concept de « processeurs de données » introduit dans le RGPD, et la variété croissante de différents acteurs impliqués dans le développement et la fourniture de services cloud.

Produit et équipement terminal

Il serait également nécessaire de clarifier **comment la notion de « produit » du Data Act s'articule avec la notion d' « équipement terminal »** qui délimite le champ d'application de la directive sur le traitement des données personnelles dans le secteur des communications électroniques (Directive e-Privacy). L'équipement terminal est défini comme « tout équipement qui est connecté directement ou indirectement à l'interface d'un réseau public de télécommunications pour transmettre, traiter ou recevoir des informations ». Bon nombre de produits au sens du Data Act pourraient donc être soumis aux prescriptions très restrictives de la Directive e-Privacy qui limite considérablement les conditions de traitement des données relatives aux équipements terminaux.

Assurer la cohérence avec les législations en cours

La manière dont le texte pourrait s'articuler avec la législation et les réglementations existantes exige une approche cohérente aux fins d'assurer une homogénéité des notions juridiques et une plus grande sécurité juridique. Voici quelques exemples de législations pour lesquelles des chevauchements pourraient être observés :

Règlement général pour la protection des données (RGPD)

- Les exigences de partage semblent aller au-delà des exigences de portabilité du RGPD en demandant aux fournisseurs de rendre le contenu non personnel récupérable. Les exigences de partage des données non personnelles conduisent à un champ d'application infini, impossible à concevoir.

- Étant donné que les détenteurs de données ont l'obligation de donner accès aux données des clients, il n'est pas clair comment les données non personnelles peuvent être liées à un utilisateur spécifique sans être classées comme données personnelles et comment le Data Act fonctionnerait en conjonction avec le RGPD.

- L'obligation de rendre les données générées par l'utilisation de produits ou de services connexes accessibles de l'art. 3 (2) en particulier (d-f et h) crée une charge considérable, en particulier (d-f et h). De telles obligations d'information semblent également être considérées comme excessives au regard des dispositions des articles 13 et 14 du RGPD.

Data Governance Act (DGA)

Il pourrait y avoir un décalage entre la mention des données commerciales confidentielles dans le DGA et le Data Act, ainsi que dans des légilations sectorielles tel qu'en matière bancaire (cf DORA). Le DGA a introduit une catégorie d'intermédiaires « neutres » de données. Ils pourraient, dans le Data Act, être concernés par les modalités du partage de données générées par des produits entre utilisateur final et partie tiers.

Espaces européens de données

Le Data Act pourrait imposer un cadre horizontal en matière d'interopérabilité entre les différents Data Spaces, qui devraient disposer de leurs propres dispositions. Le concept n'apparait pas dans les dispositions relatives au partage de données mais dans celles relatives à l'interopérabilité (article 28) sans aucune definition ou précision dans les considérants.

Règlement européen sur l'IA (AI Act)

- Parallèlement au Data Act, la Commission européenne a proposé un règlement pour l'établissement de règles harmonisées en matière d'IA, le AI Act. Dans sa rédaction actuelle, le Data Act ne permettra pas l'accès aux données qui est absolument indispensable dans le cadre de la conformité avec les obligations du futur AI Act.

- L'accès aux données est crucial pour le respect des futures obligations du AI Act (représentativité des data sets, lutte contre les biais, exactitude et complétude des data sets…). En l'état, le champ d'application limité du Data Act et les restrictions quant à l'utilisation des données ne semblent pas cohérentes avec les obligations du futur AI Act et l'ambition de l'UE sur l'intelligence artificielle.

- L'accès aux données et le profilage sont des éléments indispensables pour l'entrainement efficace des modèles algorithmiques. Tel que présenté dans le Data Act, l'impossibilité pour les tiers de réutiliser les données à des fins de profilage ou de les mettre à disposition d'autres organisations aura pour effet de limiter la possibilité pour les acteurs économiques d'utiliser les données afin d'entrainer des algorithmes d'IA.

2. Partage de données en B2B et B2C

Les articles sur le partage de donnée (articles 3 à 7) semblent construits d'une manière qui ne prend pas pleinement en compte la façon dont les entreprises déploient les objets IoT pour leurs activités économiques.

Les produits IoT dans les processus B2B ne sont généralement pas isolés. Ils font partie d'un réseau complexe en constante évolution de produits IoT sophistiqués (ex : robots), et les données générées par leur utilisation pourraient passer par un très grand nombre de solutions logicielles déployées par de nombreux fournisseurs différents et modifiées de temps en temps pour optimiser le fonctionnement des entreprises. Comme indiqué précédemment, cette complexité propre au B2B exige des **définitions claires des services connexes, des données, du détenteur des données et des destinataires des données.** Elle exige également une clarification des droits et obligations.

Accès de l'utilisateurs aux données

- Concernant **l'accès de l'utilisateur aux données,** l'article 3 ne clarifie pas suffisamment les obligations entre le fournisseur de produits et le(s) fournisseur(s) de services connexes. La question de savoir si le fournisseur de services/produits a l'intention d'utiliser lui-même les données pourrait être précisée par une définition plus étroite des données. Toutes les données générées par l'IoT ne sont pas pertinentes pour l'utilisateur et peuvent avoir une valeur sensible pour le fournisseur, comme la qualité du service dans un environnement IoT complexe.

- L'article 4(6) interdit à un détenteur de données d'utiliser les données pour obtenir des informations sur la situation économique de l'utilisateur.

- L'article 5(5) interdit au détenteur des données d'utiliser des données non personnelles pour obtenir des informations sur la situation d'un tiers, mais ne prévoit pas d'interdiction similaire pour le tiers qui recevra un volume indéterminé de données susceptibles de l'aider à obtenir des informations du détenteur des données. De même, l'article 6(e) interdit l'utilisation de données pour se faire concurrence sur un marché, mais pas l'utilisation de données pour développer des capacités internes contre son fournisseur.

Réutilisation des données par des tiers

- L'article 6(2)b exclut de son champ d'application bon nombre d'activités qui sont au cœur de l'Internet ouvert, en particulier les **activités liées au marketing et à la publicité**. Cet article prévoit que les tiers recevant les données ne peuvent pas réutiliser celles-ci à des fins de profilage des individus tel que défini par l'article 4(4) du RGPD, à moins que ce profilage ne soit nécessaire pour la fourniture du service.

    - L'utilisation des données par le tiers serait limitée à la fourniture du service, en excluant toute possibilité de mieux connaître les clients pour leur proposer de nouveaux produits ou services (et ce en conformité avec les dispositions du RGPD).

    - Cette exclusion pourrait créer un obstacle significatif à l'innovation dans le domaine des objets connectés et des services accessoires et avoir pour effet de décourager le tiers d'investir dans la fourniture de services reposant sur l'accès aux données générées par l'utilisation des produits.

    - Cette disposition semble également contraire à l'article 5 du RGPD qui définit les bases légales permettant aux organisations de traiter les données personnelles en tant que responsables de traitement. Cet article prévoit une série de bases légales, chacune assortie de garanties pour la protection des utilisateurs : consentement de l'individu ; traitement rendu nécessaire pour l'exécution du contrat ; intérêt public ; conformité à une obligation légale ou l'intérêt légitime du responsable de traitement.
      A ce titre, le Data Act devrait être aligné avec cette disposition en permettant la réutilisation des données par le tiers destinataire, à condition qu'elle repose sur une des bases légales du RGPD. Cette approche serait cohérente avec l'article 20 du RGPD sur le droit à la portabilité des individus.

- La même réflexion s'applique à l'article 6(2)c du Data Act qui interdit au tiers de mettre les données reçues à disposition d'une autre organisation sous une forme brute, agrégée ou dérivée, empêchant toute réutilisation des données en dépit d'une base légale valide. Cette redaction ne semble pas permettre la réutilisation des données sous une forme anonymisée, ou pseudonymisée, ni même l'utilisation de tout autre technique permettant de protéger les données personnelles des individus.

- Ces restrictions d'utilisation des données semblent contraires à la volonté initiale du Data Act de ne pas contredire les dispositions du RGPD et à l'objectif de partage de données.

3. Encourager le partage des données volontaire et guidé par des principes

Offrir un cadre propice au développement des petites et moyennes entreprises

Nous accueillons favorablement le modèle européen d'accords volontaires de partage de données visant à améliorer la sécurité juridique, en particulier pour les PME, et nous encourageons le législateur à faire référence aux modèles, normes et pratiques existants qui alimentent déjà des modèles de partage de données qui fonctionnent bien.

L'article 13 porte sur les clauses contractuelles abusives imposées unilatéralement à une micro, petite ou moyenne entreprise. Les petites et moyennes entreprises bénéficieront d'une protection particulière contractuelle : toute clause relative à un échange de données, dans la cadre du Data Act, qui serait jugée en leur défaveur serait déclarée caduque en cas de conflit. **En effet, les plus petites entreprises ne sont souvent pas en mesure de négocier des accords équilibrés de partage de données avec**

les acteurs du marché qui leur sont supérieurs. Bien que la liberté contractuelle reste le principe, le texte encadre plus strictement ces clauses contractuelles abusives.

Accroître la confiance dans le partage de données

Comme le souligne la Commission européenne, il est essentiel d'accroître la confiance dans le partage des données. Or, il existe déjà des modèles de partage de données en B2B qui donnent de bons résultats et démontrent ce qu'il est possible de faire lorsque la confiance est établie entre des partenaires de collaboration jouissant d'une liberté contractuelle.

- Une clarification des relations entre la notion de tiers et les destinataires des données est nécessaire.

- L'article 8 mentionne qu'aucun accord ne doit obliger à divulguer un secret commercial. Les informations sur la situation économique, les actifs et les méthodes de production doivent également être prises en compte, car elles peuvent avoir un effet anticoncurrentiel.

- La procédure de règlement des litiges n'est pas claire, car elle ne précise pas quel est l'organisme de règlement des litiges des États membres compétent. L'IoT peut être mobile et les utilisateurs professionnels, les détenteurs et les destinataires des données peuvent être présents dans plusieurs États membres.

- Les dispositions relatives aux mesures de protection pourraient être renforcées pour les détenteurs de données. Par exemple, le fait de ne pas imposer systématiquement l'effacement des données et de mettre fin à l'offre d'un produit dérivé des données du détenteur des données sur la base de l'absence de préjudice significatif ne constitue pas une protection suffisante de la propriété.

Capitaliser sur les initiatives existantes

- Diverses initiatives se sont déjà créées autour de ce projet structurant pour l'économie européenne, parfois très récemment (Gaia-X). Le Data Governance Act tendait à favoriser le partage volontaire de données. Le Data Act crée un droit au partage quelques mois après l'adoption du DGA, qui n'a eu le temps de laisser déployer ses effets et de créer la confiance nécessaire entre les entreprises européennes.

- Au-delà de la règlementation, l'instauration d'une relation de confiance entre les entreprises concernant le partage de données peut se matérialiser par le biais de **solutions contractuelles**. Les conditions de cette confiance pourraient être les suivantes : obtenir des garanties sur la nature des données partagées, leur hébergement, l'intention derrière leur réutilisation, les conditions et éventuelles limites à cette réutilisation, ou encore des obligations de transparence du traitement ou règles claires relatives aux responsabilités au responsable. Tous ces éléments peuvent être intégrés dans des clauses spécifiques des contrats de partage de données.

- Il est évident que tous les acteurs ne possèdent pas nécessairement l'expertise nécessaire ou la maturité pour rédiger et négocier de telles clauses. Par le Data Act, la Commission européenne pourrait mettre en place des **initiatives pour accompagner les entreprises**. Il serait par exemple pertinent de valoriser des initiatives telles que le Support Centre for Data Sharing qui propose une **assistance juridique sur le partage de données**. Le SCDS a un « assistant de contractualisation » qui génère automatiquement un contrat de licence type en fonction des informations renseignées sur les deux parties concernées par l'échange.

- Différents **modèles de partage de données existent déjà** et permettent des collaborations fructueuses tout en maintenant la confiance nécessaire entre les partenaires. Il pourrait être intéressant de s'appuyer sur les travaux existants et de prendre en compte les bonnes pratiques basées sur des expériences et des méthodes de travail d'autres communautés, comme celle de l'open source.

- Dans le cas d'un **partage obligatoire des données**, il est nécessaire de tenir compte de la distinction entre sous-traitant et responsable de traitement. Les sous-traitants n'ont pas en leur possession et ne contrôlent pas les données de leurs clients. Tout partage de données imposé aux sous-traitants pourrait donc entraîner une rupture de contrat avec le client.

Compensation raisonnable

- Sur la notion de **compensation raisonnable**, cette dernière n'implique-t-elle pas que nous soyons capables d'évaluer les data en tant qu'élément patrimonial ? Concernant cette compensation offerte pour usage de la donnée et du caractère uniforme des modalités d'évaluation de cette compensation (qui s'apparente au total à une sorte de loyer pour usage) quelles sont justement les modalités d'évaluation de cette compensation ? Cette notion doit prendre en compte la structure de coût que le détenteur de données a dû mettre en place pour fournir une telle donnée et non seulement la structure de coût nécessaire à son extraction et à sa mise à disposition du demandeur. A défaut, la donnée pourrait être dans certains cas être mise à disposition à perte.

- La compensation est une **indemnisation minimale et il demeure nécessaire qu'elle soit maintenue, indépendamment de la situation.** Nous nous interrogeons sur les dispositions qui indiquent que d'autres dispositions européennes ou nationales pourraient exclure une indemnisation ou prévoir une compensation moindre pour la mise à disposition de données (cf Article 9.3). Cette situation pourrait engendrer des asymétries et des incohérences sur le marché.

4. Partage de données en B2G pour des besoins exceptionnels

Un cadre sur les données d'intérêt général devrait s'attacher à ce que le partage des données des entreprises se fasse dans des conditions qui garantissent la confiance. Il est impératif de respecter les droits des personnes concernées, des entreprises, et d'assurer une concurrence équitable. Nous soutenons la mise à disposition des données des entreprises, publiques ou privées, dans des cadres déterminés, pour des usages déterminés en amont, avec une réelle réflexion concernant la rémunération des entreprises.

Tout cadre européen pour le partage des données entre entreprises et administrations devrait favoriser les partenariats et les accords entre les parties co-contractantes. Toute obligation devrait être dûment justifiée et limitée à des circonstances exceptionnelles.

Obligations de partage des données

- Alors que la proposition permet aux organismes publics d'acquérir des données en cas de besoin exceptionnel, elle ne prévoit aucune garantie pour les détenteurs de données contre l'utilisation des données pour leur nuire. Il n'est pas clair pourquoi la compensation n'est envisagée que pour les cas non urgents alors qu'en fait, l'effort pour les entreprises sera le

même dans les deux cas. L'article 15 mentionne comme circonstance exceptionnelle l'impossibilité pour le service public d'acquérir les données au taux du marché (*market rate*). La régulation doit préciser ce terme et la façon dont ce taux serait définit.

- Les articles 14 à 21 proposent une nouvelle approche de principe de l'utilisation des données des entreprises par les organismes du secteur public.

- Il est important de trouver un équilibre entre la charge administrative pour l'intérêt public et pour les entreprises. Le partage des données pose de nombreux problèmes pratiques, tels que la nécessité de traiter les données avant de les fournir.

    - Quid de l'article 20(1) selon lequel les données doivent être fournies gratuitement pour répondre à une urgence publique ?

    - En principe, cela serait possible, mais dans ce cas, l'organisme du secteur public recevra des données brutes non traitées. La crise du coronavirus a montré qu'un travail préalable important de la part des entreprises est nécessaire pour rendre anonymes les données dont ont besoin les organismes du secteur public et les rendre ensuite disponibles sous une forme utilisable. Cela signifie que les entreprises devront supporter des coûts supplémentaires et qu'elles doivent pouvoir demander une compensation. Les organismes publics ne sont normalement pas en mesure de traiter les données pour obtenir les informations correctes à partir d'un ensemble de données.

    - Une autre préoccupation est qu'en cas d'urgence publique, des données doivent être fournies pour sa prévention, sa résolution et sa récupération. Il n'y a **pas de limite au temps de récupération**. Cette disposition doit certainement être affinée et précisée. Il est par ailleurs essentiel que les besoins exceptionnels soient strictement limités à des domaines tout à fait essentiels et qu'une définition précise soit donnée. Par exemple, la référence à la « situation de pandémie » est trop large et imprécise. En outre, quelle autorité en fera la demande et quelle sera celle qui sera autorisée à recevoir des données relatives à l'entreprise et pour quelles finalités ? La Commission européenne doit fournir davantage de clarté sur ce point.

- L'article 15 (c) soulève de nombreuses questions: **que constitue un besoin urgent en dehors d'une urgence publique?** Cette situation est particulièrement renforcée par l'article 15 (c) (2) qui prévoit que l'obtention de données conformément à la procédure établie dans la proposition réduirait substantiellement la charge administrative pour les détenteurs de données ou d'autres entreprises. Une **liste restreinte d'urgences publiques** serait plus pertinente. Par conséquent, le texte devrait établir des conditions précises et complètes dans lesquelles les organismes du secteur public peuvent demander l'accès aux données détenues et contrôlées par les entreprises, en indiquant quels sont les intérêts publics concernés. Il est à noter que des accords volontaires comme il en existe depuis la pandémie fonctionnent efficacement sans contrainte, il serait certainement plus pertinent de prévoir la mise en place de ce type d'accord que d'élaborer des mesures coercitives.

- Certains **garde-fous devraient être prévus ou renforcés,** comme la protection des secrets d'affaires, la non-réutilisation des données transmises aux autorités publiques ou la possibilité de refuser le partage de données. Dans le cadre des marchés publics, Il faudrait que le texte précise par exemple que les autorités publiques ne doivent pas ouvrir les données ainsi obtenues pour une réutilisation et, d'autre part, que l'autorité qui reçoit les données ne peut les utiliser de manière incompatible avec les finalités présentées. De la même manière, la divulgation de secrets d'affaires ne peut se faire qu'en cas de nécessité pour répondre à une

urgence publique ou une situation exceptionnelle. Il faut en effet rappeler que, dans le cadre des marchés publics, les autorités sont clientes des entreprises.

De l'importance des garanties techniques

- La proposition **ne semble pas disposer de garanties techniques et génériques suffisantes pour la sécurité des données avant, pendant et après leur partage avec les organismes du secteur public.** La capacité des organismes du secteur public à traiter de grandes quantités de données en toute sécurité doit être assurée et les entreprises concernées par ces demandes devraient en obtenir la garantie. Il pourrait être mis en place **une évaluation de leur conformité** en la matière tout en appliquant des règles issues du principe de l'accountability tel que mis en place pour les données personnelles. En effet, des **obligations de transparence** devraient être précisées pour que les gouvernements et les administrations publiques indiquent à l'entreprise comment les données sont utilisées. Il est nécessaire de permettre aux entreprises de vérifier que les obligations conformément aux dispositions de l'article 19 ont bien été remplies par l'organisme du secteur public demandeur.

- Dans la mesure où il peut être très difficile pour les entreprises de contester une demande du secteur public dans les délais impartis (sans compter les amendes potentielles prévues - article 33 et article 83 du RGPD), des définitions claires seront requises.

  A ce titre, il pourrait éventuellement être demandé une clarification du délai évoqué au considérant 63 : « *Les détenteurs de données devraient avoir la possibilité de demander soit une modification de la demande présentée par un organisme du secteur public ou une institution, un organe ou un organisme de l'Union, soit son annulation dans un délai de 5 ou 15 jours ouvrables en fonction de la nature du besoin exceptionnel invoqué dans la demande.* ».

Incitations au partage de données

Imposer des obligations de partage aux entreprises pourrait avoir des effets contre-productifs, en les incitant par exemple à être moins transparentes sur les données qu'elles détiennent. La Commission devrait au contraire faciliter le partage de données volontaire et guidé par des principes, notamment en proposant des clauses contractuelles types pour de tels accords ou en donnant aux entreprises certaines garanties sur leurs perspectives de rémunération.

- Les **coûts ex ante souvent très élevés** qui y sont associés constituent un obstacle crucial au partage des données. La préparation des données qui précède l'accès aux données ou leur transfert est souvent un processus très gourmand en temps et en ressources.

- La mise en place de **mécanismes de compensation attractifs ou simplement d'accords commerciaux d'acquisition** de données/de licence pour les entreprises pourrait être un moyen plus efficace d'atteindre l'objectif souhaité. Ces incitations pourraient être directes (par exemple, monétaires) ou indirectes (par exemple, en termes de réputation).

- Il est également nécessaire que ce cadre prévienne toute violation potentielle des données, toute fuite de propriétés intellectuelle et de données commercialement sensibles, toute charge administrative et toute concurrence déloyale, ou des problèmes de confidentialité et sécurité.

- En outre, il est important de noter que le secteur public dispose déjà d'une grande quantité de données, qui ne sont pas toujours utilisées de la manière la plus efficace. Ainsi, il est important de s'assurer que les secteurs publics utilisent au mieux les données existantes. Pour y parvenir, les gouvernements doivent disposer des ressources et des compétences nécessaires. Il est

impératif que les organismes publics soient en mesure : d'avoir une vue d'ensemble des ensembles de données qu'ils pourront traiter et de comprendre leurs avantages et leurs inconvénients.

Exclusion des petites entreprises

Il est positif que les petites et micro-entreprises soient exclues du champ d'application. Cette exclusion devrait également s'appliquer aux entreprises de taille moyenne. Un droit d'accès obligatoire aux données B2G crée une charge disproportionnée pour les entreprises de taille moyenne.

5. Portabilité pour les utilisateurs professionnels de services de cloud

Valeur ajoutée du passage au cloud

Le changement de modèle vers le cloud permet la réduction des coûts de maintenance des infrastructures informatiques : les organisations qui y recourent bénéficient d'une offre entièrement intégrée qui leur permet de concentrer leurs efforts sur des tâches à plus forte valeur ajoutée. Les serveurs, le réseau, le stockage, les sauvegardes, le système d'exploitation, les bases de données et les applications sont entièrement gérées par le fournisseur. Sur le long terme, cette solution s'avère être la plus efficace en matière de coûts et de gestion des ressources humaines. Par ailleurs, le cloud permet aux utilisateurs de bénéficier des mises à jour technologiques les plus récentes, correspondant à l'évolution très rapide des technologies.

Le passage au cloud permet également d'améliorer la sécurité des données, en la confiant à une entreprise experte en la matière. Les fournisseurs de cloud mutualisent à grande échelle les investissements dans la sécurité, dans la résilience et dans une infrastructure distribuée géographiquement, qui surpassent les ressources qu'une organisation pourrait mobiliser individuellement pour des solutions sur sites, en particulier pour des organisations de petite taille. Cela explique également que la migration vers le cloud soit particulièrement importante dans les secteurs financiers ou la santé. Migrer ses données dans des infrastructures modernes permet de contribuer à la réduction de l'empreinte environnementale du secteur numérique dans sa globalité.

Les utilisateurs européens devraient avoir accès à une large gamme de services de cloud. L'accumulation de standards ou normes nationaux créent des barrières au marché unique numérique, contraignant tout particulièrement les petites entreprises qui tentent de passer à l'échelle sur le marché européen. Ainsi, il convient d'encourager une harmonisation de ces standards au niveau européen.

Obligations de portabilité

Nous accueillons favorablement l'idée de faciliter le changement de fournisseur pour les utilisateurs de services de cloud. A cet effet, le considérant 69 explicite le sens des articles du Chapitre VI : « La capacité des clients de services de traitement de données, y compris de services en nuage et de services à la périphérie, de passer d'un service de traitement de donnes à un autre, tout en maintenant une fonctionnalité minimale du service, est une condition essentielle pour un marché plus concurrentiel, avec des barrières à l'entrée moins élevées pour les nouveaux fournisseurs de services. ». Cependant, les définitions des termes clés sont souvent trop larges ou ne sont pas données.

- Le Data Act vise à fournir un cadre réglementaire, contractuel, technique et financier pour permettre une portabilité efficiente entre un fournisseur de services A, le client, et le fournisseur de services B. Une portabilité et un switching efficaces **nécessitent la coopération des**

fournisseurs de services entrant et sortant. A ce titre, les rôles de chacun devrait être davantage clarifié.

- Il conviendra de trouver le **bon équilibre entre les responsabilités des clients et des fournisseurs de services**. Si le chapitre VI du Data Act vise à corriger une asymétrie observée actuellement sur le marché européen du cloud entre clients/utilisateurs et fournisseurs de services, l'imprécision des termes ne semble pas à ce stade offrir de garanties suffisantes pour assurer la correction de cette assymétrie.

De plus, la proposition de règlement devrait tenir compte de la **complexité technique des projets de migration.** En pratique, déplacer de larges volumes de données hébergés à travers de multiples serveurs ou hébergeurs peut représenter des projets de migration sur plusieurs mois, voire années.

- L'obligation pour le fournisseur d'assurer la continuité du service [Article 24(1)a et b et Article 24(2)] : Les utilisateurs et les fournisseurs s'accordent sur le niveau de service que le fournisseur est tenu de respecter pendant la phase d'assistance à la résiliation, au cours de laquelle le fournisseur transfère les workloads de l'utilisateur vers un autre fournisseur. La continuité du service est généralement mieux garantie par une collaboration entre le fournisseur et le client, plutôt que par un transfert des obligations sur le fournisseur. Si la proposition expose clairement ces obligations (considérant 70), elle **ne laisse toutefois pas la place à la liberté contractuelle.**

- La notion d'équivalence fonctionnelle, définie comme le « *même niveau de performance et avec le même niveau de sécurité, de résilience opérationnelle et de qualité de service* » parait floue et difficile à évaluer tant sur le plan opérationnel que technique. L'obligation d'assurer une « équivalence fonctionnelle » pour les services IaaS (art 26(1)) est donc difficile à apprehender. A ce titre, nous nous interrogeons sur les attentes qui incombent au fournisseur de cloud : sera-t-il tenu d'assurer le même niveau de sécurité, de performance, de qualité de service, de rendement et de performance dans l'environnement d'un concurrent ? A ce stade, il parait impossible pour les services de traitement de données d'avoir une connaissance suffisante des fonctionnalités des autres services concurrents pour garantir « l'équivalence fonctionnelle » envisagée dans la proposition.

- Il conviendrait de tenir compte des spécificités techniques des services au niveau de l'infrastructure (IaaS) et des services logiciels plus souvent sur mesure, comme PaaS ou SaaS.

- Il convient de noter que les mesures d'interopérabilité, les mesures d'information complémentaires et la mise en œuvre du « droit d'accès » (articles 3 et 4) (adaptation des systèmes) entraînent des coûts qui peuvent être répercutés sur les clients finaux.

- Des précisions supplémentaires sont nécessaires sur la notion *d'ostacle* visée à l'article 23(2). Le Data Act ne donne pas de définition du terme *obstacle* et n'exige pas qu'un obstacle atteigne un certain seuil d'importance. Il semble que pratiquement tout facteur commercial, technique, contractuel ou organisationnel (laissé à la discrétion de l'utilisateur) pourrait constituer un obstacle.

- L'article 25 du règlement sur le retrait graduel des coûts de migration prévoit que le fournisseur facture la migration à prix coutant pendant une période transitoire de 3 ans après l'entrée en vigueur du texte, puis ne pourra plus facturer ensuite.

    - Qu'en est-il si le contrat est résilié en raison d'une violation par le client ?

- Quelle est la justification du maintien, par le fournisseur de services initial, de tels frais en cas de changement effectif de fournisseur de services opéré par le client (cf. art. 23, 24) ?
- Quelle est la justification de l'absence de partage du coût, alors que cela se pratique par exemple dans le secteur des télécommunications ?

Encourager les initiatives en cours

La montée en maturité des entreprises sur leurs données combinée à davantage de pratiques de portabilité fait déjà partie des objectifs de l'UE dans le domaine du cloud. Les fournisseurs et utilisateurs de services de cloud se sont structurés pour élaborer conjointement des codes de conduite d'autoréglementation. Il faut continuer d'encourager ce type d'initiatives, surtout lorsqu'elles sont portées par la Commission européenne.

La création d'un recueil réglementaire du cloud (Cloud rulebook) - prévu par la Commission au deuxième trimestre 2022- permettra de rassembler en un seul document la réglementation existante et les normes et systèmes reconnus par les fournisseurs de cloud. Celui-ci comprendra un recueil des codes de conduite et de certification existants en ce qui concerne la sécurité, l'efficacité énergétique, la qualité des services, la protection des données et la portabilité des données. Ce recueil de règles devrait être facile à lire, à comprendre et à consulter, afin d'aider les utilisateurs du cloud à préparer leurs projets d'utilisation du cloud, à planifier leurs évaluations des risques, etc. A ce titre, l'initiative Gaia-X – à laquelle Numeum adhère en tant que Day-1 Member- constitue une réelle opportunité. Cette initiative permettra aux Européens d'avancer à la fois sur leur transformation numérique, en adoptant une politique de « Cloud au centre ».

6. Sauvegarde des données non personnelles dans des contextes internationaux

La proposition impose des mesures techniques, juridiques et organisationnelles pour empêcher l'accès ou le transfert international de données non personnelles détenues dans l'UE lorsque ce transfert ou cet accès serait contraire à la législation de l'UE ou à la législation nationale de l'État membre concerné.

- Si nous reconnaissons la nécessité d'encadrer d'une manière plus claire (en garantissant la sécurité juridique), les demandes d'accès aux données des gouvernements, nous pensons qu'une solution internationale découlant des accords internationaux existants serait la plus appropriée. Actuellement, l'accès aux données fait l'objet de discussions dans le cadre des négociations sur e-evidence et le DGA, ainsi que dans le cadre international de l'OCDE. Il conviendra d'assurer la cohérence entre ces différentes législations.

Nous nous félicitons que la Commission ait inclus des dispositions dans l'article 27 pour fournir des orientations supplémentaires concernant le processus de vérification. Nous pourrions appeler de nos vœux une plus grande implication des autorités afin qu'elles se substituent, le cas échéant, aux entreprises qui recevraient une telle requête.

- Il convient de noter que, dans le cas spécifique du cloud, les données ne sont pas stockées ou traitées séparément entre données personnelles et non personnelles.

- Nous invitons la Commission à poursuivre le dialogue avec les fournisseurs et les groupes d'utilisateurs du cloud, afin de définir ces orientations techniques, juridiques et organisationnelles. Elles devraient également être mises à disposition avant que le Data Act entre en application.

7. Interopérabilité

Standardisation et normalisation

- La standardisation est essentielle pour garantir que les données puissent être protégées tout en étant accessibles, et qu'elles puissent être facilement partagées entre différents acteurs. Trop souvent reléguée à de lointaines échéances, la structuration sémantique des données est pourtant essentielle pour que ces dernières puissent être analysées, compilées et fusionnées dans des ensembles de données plus larges. Or, le coût de structuration des données existantes, lorsque ces dernières n'ont pas été capturées à la source dans des formats ouverts et partageables, peut s'avérer rédhibitoire pour les acteurs et freiner la mutualisation et l'exploitation commune des données. C'est la raison pour laquelle il est important de 1) sensibiliser et d'accompagner les acteurs, filière par filière, mais aussi à une échelle cross-sectorielle, à identifier ensemble les données pour lesquelles le partage et la mise en commun peuvent être bénéfiques et 2) les aider dans la structuration de ces données et la définition des protocoles de partage. C'est la condition sine qua non pour une interopérabilité effective des systèmes d'information et des plateformes, et in fine pour un partage efficient de la donnée.
- Ces initiatives pourraient être précédées d'un état des lieux des nombreux standards et normes qui coexistent aujourd'hui pour définir la sémantique (taxonomies communes, formats de données, modèles, etc.), les API et les protocoles d'interopérabilité. Cette première étape permettrait également d'identifier les meilleures pratiques actuelles. Il est nécessaire de soutenir et de consacrer par ce texte les efforts menés par les différentes parties prenantes à l'échelle européenne (Gaia-X, SWIPO, etc.) et internationale (ISO, UNE/CEFACT, etc.) permettant d'atteindre une harmonisation par le haut d'un ensemble de règles et standards et garantissant aux utilisateurs les plus hauts niveaux de sécurité dans l'usage de leurs données, en les adoptant comme spécificités d'interopérabilité ouvertes.
- Pour cette raison, l'évaluation et la cartographie doivent être effectuées sur la législation déjà en place afin de proposer un état des lieux exhaustif des cadres juridiques actuels qui s'appliquent aux objectifs que la Commission veut atteindre. C'est notamment le cas pour les données qui peuvent également être considérées comme des secrets commerciaux, contenir des données personnelles ou être critiques sur le plan de la sécurité.

Si la proposition de règlement semble faire de la base contractuelle la pierre angulaire du partage des données détenues par des entreprises, elle impose aux entreprises détentrices de données de nombreuses obligations, parfois trop lourdes. En effet, avant la conclusion du contrat, l'utilisateur doit par exemple bénéficier d'une information sur la nature et le volume des données générées par l'utilisation du produit ou service. **Cette notion d'information sur la « volumétrie des données générées » manque de clarté et il est difficile de chiffrer et donner cette information pour une entreprise.**

Droit des bases de données

La proposition de règlement révise certains aspects de la directive sur les bases de données, qui avait été adoptée dans les années 1990 pour protéger les investissements dans la présentation structurée de données. Il précise notamment que les bases de données contenant des données provenant de dispositifs et de l'IoT ne devraient pas faire l'objet d'une protection juridique distincte. Il sera ainsi possible d'y avoir accès et de les utiliser.

Selon les dispositions de l'article 35 : « afin de ne pas entraver l'exercice du droit des utilisateurs d'accéder à ces données et de les utiliser conformément à l'article 4 ou du droit de partager ces données avec des tiers conformément à l'article 5, le droit sui generis prévu à l'article 7 de la directive 96/9/CE

ne s'applique pas aux bases de données contenant des données obtenues ou générées par l'utilisation d'un produit ou d'un service lié. »

Aussi, plusieurs interrogations subsistent :

- Faut-il considérer que le droit sui generis est inapplicable seulement dans les cas où cela empêche les droits d'accès et d'usage des utilisateurs conformément à l'article 4 de la proposition de règlement ou le droit de partage des données avec des tiers conformément à l'article 5 ?

- Faut-il considérer que le droit sui generis est inapplicable dès lors qu'une base de données contient des données générées par l'utilisation d'un produit ou d'un service lié, et donc générées par l'IoT ? Cela pourrait concerner toutes les bases de données, ce qui remettrait en cause le principe même du droit prévu par la directive 96/9/CE. Il nous semble qu'il faudrait encadrer plus strictement le périmètre d'exclusion du droit sui generis. Il convient de se demander quelles seraient les conséquences pour le détenteur qui aurait fait des investissements substantiels pour vérifier ou afficher les données en question.

- Une remise en cause de cette protection dans le contexte de l'IoT, ne serait-elle pas le début d'une remise en cause plus fondamentale de ce droit dès lors qu'il est confronté à une question de portabilité ?

8. Mise en œuvre et application

- Compte tenu de la grande diversité des sujets visés par la proposition, l'attribution au niveau national d'une ou plusieurs autorités compétentes pourrait entraîner une grande hétérogénéité dans l'application du règlement (notamment en ce qui concerne les décisions et les sanctions).

- Aussi, il est nécessaire d'énoncer pleinement le régime de responsabilité, de recours et de sanctions au lieu de transférer cette discussion au niveau des États membres dans certains cas. Ceci éviterait des lacunes potentielles dans les lignes d'application, découragerait le forum-shopping et empêcherait la fragmentation du marché unique.