PROPOSITION DE REGLEMENT EUROPEEN SUR LES DONNEES (DATA ACT)
POSITION DE L'AFEP

Les entreprises membres de l'Afep (Association française des entreprises privées) soutiennent l'objectif du Data Act de **stimuler l'innovation par un meilleur accès aux données des objets connectés**. Elles apprécient que des principes favorables à un partage équitable des données soient envisagés.

Les entreprises déplorent cependant **l'absence d'une étude d'impact détaillée** qui aurait pu permettre de préciser les types de données déjà échangées ou non et **d'identifier les défaillances de marché justifiant cette obligation de partage des données**.

Ce texte soulève ainsi des interrogations sur son périmètre, sur la définition de la donnée et sur celle des produits visés. De plus, les données ayant un coût (dans leur création, gestion, diffusion ou préservation), celles-ci ne peuvent pas être mises à disposition des utilisateurs et tiers sans filtrage par le détenteur ni compensation proportionnelle à ces coûts. En outre, ce texte conduit à une remise en cause de la protection de la propriété intellectuelle et du savoir-faire des entreprises dans un monde éminemment concurrentiel. Il augmente, enfin, indûment leur responsabilité dans un environnement juridique flou et vaste.

Une **claire définition de la donnée** s'avère ainsi nécessaire. Les conditions de partage des données doivent être également précisées afin de préserver des « business models » performants tout en **stimulant l'innovation sur des bases concurrentielles favorables aux acteurs économiques européens**.

Table des matières

Introduction

L'Afep partage l'objectif de la Commission qui entend améliorer l'accès aux données d'objets connectés pour soutenir l'innovation, développer des marchés plus équitables, assurer une plus grande interopérabilité et renforcer la confiance des consommateurs et des utilisateurs en exigeant une plus grande transparence précontractuelle.

Diverses dispositions contribuent à instaurer des principes favorables à un partage équitable des données (transparence accrue sur les données générées par l'utilisation d'un objet connecté pour son utilisateur et les fournisseurs de service ou sur les conditions commerciales d'accès à ces données pour les fournisseurs de service, possibilité pour le fabricant du produit de traiter des données générées par l'utilisation de l'objet connecté…) et à une meilleure harmonisation du marché via l'encouragement de la mise en place d'outils standards tels que des APIs (interface de programmation d'application), des contrats intelligents ou des règles communes de gouvernance. Pour les acteurs européens, l'interopérabilité des services en nuage est, en outre, source potentielle de développement de services conformes aux valeurs et aux règles européennes.

Ce nouveau cadre juridique imposant aux entreprises européennes le partage de leurs données induit cependant de réels risques pour elles. Il remet en cause le principe de la liberté contractuelle des acteurs économiques. Ce partage peut, ensuite, potentiellement dépasser le cadre de l'Union européenne. Il s'accompagne d'une remise en cause de la protection de leur propriété intellectuelle et de leur savoir-faire dans un monde éminemment concurrentiel. Il augmente indûment leur responsabilité dans un environnement juridique flou et vaste.

Face aux incertitudes juridiques et à ses conséquences économiques, ce texte requiert donc de réels efforts de clarifications pour en circonscrire la portée et les risques pour les acteurs économiques s'il souhaite atteindre ses objectifs de soutien à l'innovation tout en prenant en compte les réalités sectorielles. La donnée est en effet une information qui a un coût de création, d'exploitation, et donc, de diffusion. Cette donnée peut également être sensible et exposer les acteurs et produits européens à des risques forts (cf. le *retro-engineering* notamment) En tant qu'actif stratégique et économique, elle contribue à conforter la souveraineté européenne.

Il est à noter que cette proposition ne repose pas sur une étude d'impact détaillée, qui aurait permis de préciser, par exemple sur une base sectorielle, les données déjà échangées ou pas. Cet exercice aurait permis d'identifier spécifiquement des défaillances de marché et leurs causes éventuelles, avant d'imposer un principe général d'obligation de partage (souvent gratuit) des données.

Dans ce cadre, une claire définition de la donnée s'avère nécessaire pour permettre ensuite une structuration des dispositions de ce texte (périmètre, obligation de partage, responsabilité des acteurs, rôle des autorités publiques…). De même, une protection appropriée des données sensibles doit être assurée – la voie contractuelle proposée dans le texte apparaissant insuffisante.

Enfin, si le partage de données doit être encouragé, il convient d'éviter de déstabiliser indument les « business models » d'innovation existants, notamment du fait de la gratuité des accès aux données. Ce texte est en effet source de distorsion concurrentielle dans la mesure où il s'appliquera pleinement aux acteurs européens alors qu'il ne s'appliquera aux entreprises étrangères que pour leurs fournitures dans l'Union, ouvrant la voie à une rupture des conditions de concurrence équitables.

Si l'Afep soutient l'approche horizontale recherchée par la Commission européenne dans cette proposition de règlement, il apparaît à ce stade difficile d'établir des paramétrages et définitions adaptés aux réalités sectorielles très hétérogènes (par ex. données partageables ou non). Or un règlement trop intrusif ou mal paramétré pourrait rapidement aboutir à décourager l'innovation dans l'Union. L'approche horizontale pourrait par conséquent être allégée, et complétée via des actes sectoriels à même de clarifier certaines définitions et obligations de manière plus fine et pertinente, notamment dans le cadre des travaux européens sur des espaces de données par écosystèmes.

Des remarques générales précèdent des commentaires plus précis sur cette proposition de règlement.

Remarques générales

La complexité du texte au regard d'autres législations

En créant de nouvelles obligations, le *Data Act* impacte d'autres législations horizontales, en particulier le RGPD.

Bien que le texte indique que le traitement des données couvertes par le nouveau règlement doit être effectué conformément au RGPD, leur application simultanée s'avérera difficile (voir en ce sens l'avis du CEPD adopté le 4 mai 2022). Ainsi, à titre d'exemples :

- la proposition introduisant l'idée d'un principe de « partage dès la conception » (Article 3) est *a priori* en opposition avec l'approche de « confidentialité dès la conception » (*privacy by design*) du RGPD ,
- l'interdiction d'utiliser les données reçues par un tiers à des fins de profilage (Article 6-2-b) apparaît contraire à l'Article 6 du RGPD qui définit les bases légales (traitement rendu nécessaire pour l'exécution du contrat, consentement de l'individu, intérêt public, conformité à une obligation légale ou intérêt légitime du responsable de traitement) permettant aux responsables de traitement de traiter les données personnelles,

- alors que le RGPD oblige les entreprises qui collectent des données personnelles à garantir leur sécurité tout au long de leur cycle de vie, le Data Act encourage le détenteur de données à les partager « en continu et en temps réel », soulevant ainsi la responsabilité du détenteur qui ne peut plus en assurer la protection dans toute la chaîne de valeurs.

Cette confusion complexifie la mise en œuvre des textes par les entreprises et augmente inutilement leurs efforts et investissements pour renforcer la sécurité des données et la cybersécurité de leurs produits.

La mise en risque potentielle des entreprises européennes

Cette mise en risque se traduit à la fois par des remises en cause fortes de cadres juridiques structurant l'économie européenne et par des charges administratives supplémentaires créant des distorsions de concurrence peu propices à l'innovation.

- La proposition de règlement repose sur l'hypothèse que des données existeraient d'ores et déjà « sur étagère » et pourraient être aisément partagées pour autant que l'obligation de le faire soit introduite en droit. Au demeurant, la donnée étant disponible, la gratuité de transmission serait la règle.

  Les réalités sectorielles montrent toutefois que cette hypothèse de travail est souvent erronée : dans de nombreuses situations, les entreprises industrielles sont au contraire engagées dans un effort continu d'extraction, de collecte, de formatage et de traitement d'un volume croissant de données afin de les rendre exploitables. Dans ces situations, développer l'innovation et le partage de données ne peut se faire qu'en préservant les incitations de ces industriels à continuer à investir dans l'accroissement du volume général de données. A défaut, le règlement aurait un effet contreproductif.
- Le respect des droits de propriété intellectuelle et des secrets d'affaires est essentiel afin d'éviter des distorsions de concurrence pour les entreprises détenant des données et de maintenir pour celles-ci une incitation suffisante à investir et innover. Le champ d'application, qui ne fait pas de distinction entre les utilisateurs de l'UE et les utilisateurs ou les tiers non européens, pourrait conduire à une faible protection de ces droits et secrets, même avec les garanties proposées.

- Le texte ne considère pas suffisamment -par exemple- les situations d'obligation de partage de données pouvant contenir des secrets d'affaires vers des concurrents ou des entreprises risquant de transmettre ces informations à des concurrents. Les fragiles garanties envisagées (de nature contractuelles, donc insuffisamment dissuasives et contrôlables *ex ante*) sont susceptibles de freiner les investissements vers l'innovation faute de protection contre de potentielles violations du secret d'affaires et des distorsions de concurrence. La proposition laisse également ouverte la question des possibles garanties pour le détenteur de

données s'il ne réussit pas à trouver un accord avec les destinataires de données sur les mesures de protection.

De manière générale, le détenteur de données devrait pouvoir refuser ce partage, ex ante, et ce pour des échanges avec des utilisateurs tiers ou des autorités publiques.

- L'exception introduite par la proposition de règlement (Article 35) au droit Sui Generis pourrait mettre en péril la **propriété intellectuelle des producteurs de bases de données**. La création de bases de données nécessite en effet des ressources humaines, techniques et financières considérables. Cette dérogation pourrait compromettre leurs investissements futurs, ce qui aurait un impact significatif sur la capacité d'innovation des acteurs économiques européens.

- En outre, le fait que la **gratuité de ce partage** soit érigée en principe souffrant peu d'exceptions constituera un frein fort à l'innovation dans toutes les situations où les données ne sont pas disponibles « sur étagère » et où les industriels doivent encourir des coûts significatifs d'extraction, collecte, formatage et traitement des données afin de les rendre exploitables. Ceci pourra de surcroît induire de réelles distorsions de concurrence avec des pays tiers.

  A ce titre, préserver l'incitation des acteurs industriels à développer le volume de données disponibles doit être pleinement prise en compte, comme condition indispensable au développement ultérieur du partage de ces données.

Commentaires portant sur les principales dispositions du texte

Un champ d'application et des définitions peu clairs (Chapitre I)

Les notions applicables à l'Acte sur les données doivent être claires, pour assurer la **sécurité juridique des parties prenantes et harmoniser les interprétations possibles** au sein des Etats membres. A ce stade, les définitions proposées des données et des produits ou services liés qui doivent être disponibles sont très larges, horizontales et parfois non alignées avec d'autres textes existants (par exemple : l'Acte sur la gouvernance des données). La notion d'objet connecté n'étant elle-même pas définie, les données générées par un produit ou service lié couvrent potentiellement un champ très large insécurisant les futures innovations technologiques.

Le partage de données et les cadres contractuels diffèrent aussi largement, selon le secteur économique considéré ou le type d'activités considérées (B2C et B2B). Une **approche différenciée** serait susceptible de limiter les incertitudes juridiques et les risques pour les entreprises. L'obligation de partager les données générées par l'internet des objets avec les utilisateurs (consommateurs ou entreprises) semble en effet illimitée. Or ces produits connectés génèrent une large variété de données, **différentes dans leurs volumes, natures ou niveaux de traitement**, y compris selon les secteurs. Les défaillances de marché

éventuelles, les incitations à l'innovation et la situation concurrentielle au sein et hors de l'Union diffèrent fortement selon les situations considérées.

A titre d'exemple, le propriétaire du produit connecté et son utilisateur sont mal différenciés. Il sera nécessaire pour certains secteurs de devoir clarifier l'attribution des droits et obligations dans les situations où les configurations d'utilisation et de propriété de l'appareil sont plus complexes que la relation fabricant-utilisateur.

Il est également difficile de déterminer si l'obligation de partage concerne les données brutes ou des ensembles de données consolidés (données ayant été traitées, transformées ou valorisées suivant un processus logiciel). A ce stade, les situations sectorielles empêchent de dégager une position univoque sur le type de données qui pourraient être concernées par une obligation de partage. Ainsi que souligné précédemment, si favoriser le partage des données est légitime dans une certaine mesure, il est également fondamental de préserver l'incitation des acteurs à investir dans le développement de la collecte et du traitement des données en amont. Ceci nécessite de préserver efficacement les secrets commerciaux ou des droits de propriété intellectuelle et de permettre la compensation des investissements financiers, humains engagés par les entreprises.

Une clarification de ce qu'est la donnée et la donnée partageable au sens de l'Acte sur les données est essentielle et prioritaire à la structure de ce texte et à sa possible application. La difficulté consiste à dégager des définitions claires susceptibles d'embrasser les réalités sectorielles diverses, en permettant d'intensifier le partage des données tout en préservant les incitations à investir suffisantes en amont et à maintenir un *level playing field* mondial.

De là découlent d'autres améliorations notamment sur de nombreuses définitions telles que celles d'objet connecté, d'utilisateur, de « tiers », de besoins exceptionnels/urgence publique. La compréhension du texte en sera plus aisée en termes de partage de la donnée ou de responsabilité.

Des obligations de partage des données B2C et B2B mettant en risque les entreprises (Chapitres II, III et IV)

Les articles portant sur les obligations d'accès de l'utilisateur aux données sont très détaillés, les rendant souvent inadaptés à la multiplicité des cas et des acteurs selon les secteurs et les produits. Ils ne différencient pas suffisamment les spécificités propres au déploiement par les entreprises d'objets connectés dans le cadre de leurs activités économiques.

Garantir des principes appropriés au niveau horizontal tout en laissant le détail du partage aux actes sectoriels et aux accords contractuels pourrait contribuer à améliorer la compréhension de ce texte et trouver l'équilibre entre préservation des incitations à innover, partage des données et maintien d'une concurrence équitable

En outre, si les entreprises soutiennent le développement de la portabilité des données (Articles 4 et 5 du *Data Act*) conforme à l'Article 20 du RGPD, la portabilité en temps réel soulève cependant des questions de mise en œuvre technique, sur lesquelles il serait

opportun de réfléchir. S'agit-il en effet d'un partage constant, d'une donnée partagée pendant son utilisation ou uniquement à la demande de l'utilisateur, de manière ponctuelle ?

Ce partage induit de plus des conséquences iniques pour les détenteurs de données :

- la majorité des obligations de partage de données ne permettent pas d'indemnisation suffisantes, dans le cas d'accès du tiers (ou de partage B2G dans les cas d'urgence). Les coûts techniques de collecte, formatage, traitement et mise à disposition pour le détenteur des données devraient au minimum être pris en charge par l'autorité publique à l'origine de la demande du partage de données ;
- si le détenteur de données est tenu de les mettre à disposition du destinataire dans des conditions FRAND (Article 8-1), il appartient encore au détenteur de démontrer l'absence de discrimination lorsque le destinataire de données considère discriminatoires les conditions de mises à disposition de ces données (Article 8-3) ;
- le caractère « raisonnable » de la compensation convenue entre un détenteur et un destinataire de données (Article 9-1) doit être précisé afin de mieux prendre en compte la valeur réelle de ces données et le coût de leur mise à disposition, en supprimant les dispositions nationales ou européennes susceptibles de remettre en cause ce principe de compensation (Article 9-3) ;

L'Article 13 vise les clauses contractuelles abusives imposées unilatéralement aux micros, petites ou moyennes entreprises. Cette approche semble inadaptée dans le monde numérique où toute taille de structure peut-être économiquement puissante. A ce titre, il est proposé de viser « les parties » en lieu et place des micros, petites ou moyennes entreprises.

Une mise à disposition obligatoire des données aux services publics soulevant des difficultés (Chapitre V)

Ici encore, une étude d'impact détaillée aurait été nécessaire afin d'identifier précisément au préalable les situations dans lesquelles une défaillance de marché peut être avérée, justifiant ainsi une intervention législative. A contrario, dans nombre de situations, les partages de données vers les autorités publiques fonctionnent de manière satisfaisante et ne doivent pas être déstabilisés. En particulier, ceux-ci peuvent reposer sur des compensations financières nécessaires à équilibrer les investissements amont des détenteurs de données. Ces situations ne s'accommoderaient pas de l'application d'obligations imposant la gratuité des transferts.

Ce partage de données peut en outre déboucher sur des échanges ultérieurs de données vers d'autres organismes publics voire des tiers (Article 15 § 4 notamment). Ces échanges peuvent potentiellement dépasser le strict cadre européen et, donc, porter atteinte à leur compétitivité sans conditions de réciprocité.

De nombreuses entreprises, actives sur les marchés publics, ont également pour clients des autorités publiques qui peuvent demander un accès aux données découlant d'un "besoin

exceptionnel". Il est proposé de mieux définir le cadre s'appliquant à ces autorités (B2B ou B2G).

La mise à disposition dans le cadre d'une "mission spécifique d'intérêt public" (Article 15 - c) parait également disproportionnée.

Enfin, les entreprises s'étonnent que le détenteur de données ait la charge d'apprécier la proportionnalité de la demande de données émanant des organismes publics. Cette disposition illustre une nouvelle fois l'ambiguïté de ce texte qui assimile tous les types de données.

La portée de l'accès aux données par les organismes du secteur public pour « *des besoins exceptionnels* » doit être clarifiée ; les obligations de partage vers les organismes du secteur public (B2G) devraient être dûment justifiées (pas d'intervention lorsque la situation actuelle est satisfaisante) afin d'éviter des interprétations nationales extensives risquant de fragiliser les entreprises. De même, il est proposé de mieux définir le cadre s'appliquant aux autorités publiques en relation avec des entités privées (B2B ou B2G). Enfin, l'obligation de gratuité des transferts est susceptible de déstabiliser indûment les équilibres d'investissement et commerciaux existants, au détriment de la préservation des incitations à investir.

Ce cadre devra prévenir toute violation potentielle des données et de droit de propriété intellectuelle et s'assurer contre les risques de cybersécurité et d'atteinte à la confidentialité. Les données ainsi partagées ne doivent pas devenir publiques. De manière générale, le détenteur de données devrait pouvoir refuser ce partage, lorsque ces garanties ne sont pas assurées ou respectées.

Des clarifications à apporter sur les changements de services de traitement de données (Chapitre VI)

Le chapitre VI traite du changement de services de traitement des données, soutenu par les entreprises de l'Afep.

Faciliter le changement de sous-traitant par une meilleure portabilité des données et une interopérabilité accrue dans les services contribuera à soutenir l'innovation et la concurrence entre acteurs économiques.

La faisabilité technique de tels projets doit être néanmoins intégrée dans ces dispositions en précisant les responsabilités des fournisseurs de services entre eux (entrant et sortant), les responsabilités des clients et de ces mêmes fournisseurs ou en affirmant la liberté contractuelle de ces acteurs dans l'organisation concrète de ces changements de service (calendrier, par exemple). La migration de volumes conséquents de données hébergées sur de multiples serveurs peut en effet induire des délais plus ou moins longs.

Autres : garanties dans un contexte international et mise en œuvre et exécution (Chapitres VII et IX)

Le chapitre VII traite des garanties en matière de données à caractère non personnel dans un contexte international. Le chapitre IX aborde la mise en œuvre et l'exécution de *Data Act*.

Le chapitre VII entend consacrer le principe de souveraineté européenne en matière de données non personnelles.

- La multiplication de données traitées implique une responsabilité accrue des responsables de traitement et des risques de conflits concernant la gestion des données personnelles.
  Dans ce cadre, une clarification du rôle devant incomber aux autorités publiques s'avère nécessaire. A ce titre, la charge d'étudier les systèmes juridiques des pays tiers devraient incomber aux autorités publiques.

- L'Afep rappelle également l'importance des flux de données depuis et vers l'UE pour les entreprises européennes et appelle à éviter de nouvelles barrières et incertitudes sur le marché. A ce titre, la charge pesant sur le fournisseur de services de traitement des données pour empêcher les transferts internationaux (Article 27) apparaît disproportionnée au regard de la réalité de ces flux.

La cEnfin, si le chapitre IX vise à régler les compétences des autorités chargées de l'application et de l'exécution de ce règlement, les entreprises soulignent leur souhait de simplification et de cohérence administratives.

Les entreprises s'étonnent en particulier de l'effet rétroactif de possibles astreintes ou sanctions par ces autorités compétentes (Article 31-3-d). La mise en œuvre du *Data Act* sera forcément longue au sein des entreprises (lourdeur de la migration de données) - a fortiori dans des grandes structures. Les entreprises ne peuvent être pénalisées pour leurs efforts alors que le principe de cette rétroactivité est non encadré et non précisé (sur la période ou le type d'acte visé).

*

À propos de l'Afep

Depuis 1982, l'Afep rassemble les grandes entreprises opérant en France. L'association, basée à Paris et à Bruxelles, a pour objectif de favoriser un environnement favorable aux entreprises et de présenter la vision des entreprises membres aux pouvoirs publics français, aux institutions européennes et aux organisations internationales. Restaurer la compétitivité des entreprises pour assurer la croissance et l'emploi durable en Europe et relever les défis de la mondialisation est la principale priorité de l'Afep.

L'Afep compte 114 membres. Plus de 8 millions de personnes sont employées par les entreprises membres de l'Afep et leur chiffre d'affaires annuel combiné s'élève à 2 600 milliards d'euros.

L'Afep participe à l'élaboration de législations trans-sectorielles, au niveau français et européen, dans les domaines suivants : économie, fiscalité, droit des sociétés et gouvernement d'entreprise, financement des entreprises et marchés financiers, concurrence, propriété intellectuelle et numérique, droit du travail et protection sociale, environnement et énergie, responsabilité sociale des entreprises et commerce.

Contacts :
Emmanuelle Flament-Mascaret, Directrice Droit économique / concurrence@afep.com
Alix Fontaine, Conseillère Affaires européennes / a.fontaine@afep.com