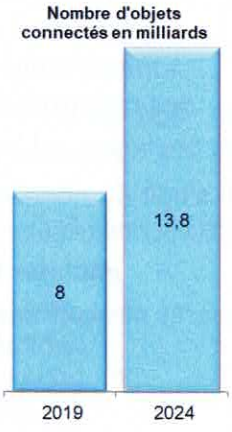
...le rapport d'information relatif au

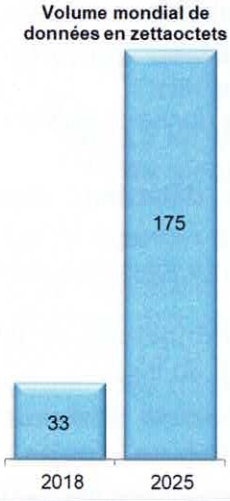
« *DATA ACT* » : UNE NOUVELLE ÉTAPE DANS LA CONSTRUCTION DU MARCHÉ EUROPÉEN DES DONNÉES

adopté par la commission des affaires européennes le 11 mai 2023

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, la valeur de l'internet des données atteignant 5 000 milliards d'euros.**



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 projet de cadre harmonisé (*« Data act »*), destiné à faciliter l'accès à ces données et leur utilisation, et annoncé dans sa stratégie européenne pour les données** publiée en 2020.

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

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

La proposition de règlement européen (*« Data act »*) *prévoit que l'***accès** aux données doit 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 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.

Il est prévu que l'utilisateur soit 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 peut introduire une plainte auprès de l'autorité nationale compétente.

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

La Commission propos que soient mises à la disposition du tiers utilisateur de manière équitable et transparente. Une compensation raisonnable des coûts peut être demandée. 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 peuvent 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**

Trois situations sont identifiées par la Commission européenne : une urgence publique, la prévention d'une telle urgence ou le 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.

La demande d'accès doit être justifiée et précise, 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.

Pour assurer l'effectivité des droits reconnus aux utilisateurs, les rapporteurs de la commission des affaires européennes recommandent de :

- **Préciser la définition des données concernées**

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**
  - 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.
- **Poser comme principe que la protection contractuelle des secrets d'affaires ne saurait conduire à limiter l'accès et l'utilisation des données**

Il devrait toutefois 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**
  - **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.

2. MIEUX ACCOMPAGNER LA SÉCURISATION DES TRANSFERTS DE DONNÉES

Faciliter le changement de fournisseur de services de traitement de données

Dans un marché caractérisé par une très forte concentration (72 % du marché européen est contrôlé par trois 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, dont 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.

Elle prévoit en outre que 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.

Pour assurer l'effectivité du droit de changer de fournisseur, les rapporteurs de la commission des affaires européennes préconisent de renforcer l'information du client et d'interdire certaines pratiques abusives

- **Des obligations d'information du client sur le changement de fournisseur**
  - une information (préalablement 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 ;
  - une information précise sur les étapes techniques du processus de migration ainsi que sur les diligences qui seront mises en œuvre.
- **L'interdiction de refuser le changement de fournisseur au motif de la phase d'utilisation gratuite de ses services dont a bénéficié le client**
- **La suppression rapide des frais de sortie pour permettre d'atteindre l'objectif de rééquilibrage du marché de l'informatique en nuage.**

Des exigences essentielles d'interopérabilité

L'interopérabilité, qui permet de combiner des données provenant de différentes sources à l'intérieur des secteurs et entre les secteurs, est une condition nécessaire du partage des données. La proposition de règlement impose en conséquence 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**.

Les rapporteurs de la commission des affaires européennes souhaitent que les modalités d'élaboration des normes d'interopérabilité soient précisées

La sécurisation des transferts internationaux de données

Certains pays extra-européens se sont dotés de lois permettant à leurs juridictions 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 entend soumettre 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**.

Construire un hébergement souverain pour protéger certaines données

Une liste des données sensibles (dont les données de santé et celles 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 européenne et les États membres se dotent d'hébergements souverains.

3. 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.

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

Les États membres 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.

Sans aller jusqu'à désigner un contrôleur européen comme 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.

Florence Blatrix Contat

Rapporteure

Sénatrice (Socialiste, Écologiste et Républicain) de l'Ain

André Gattolin

Rapporteur

Sénateur (Rassemblement des démocrates, progressistes et indépendants) des Hauts-de-Seine

Catherine Morin-Desailly

Rapporteure

Sénatrice (Union Centriste) de la Seine-Maritime

Commission des affaires européennes

http://www.senat.fr/europe/broch.html

Téléphone : +33 (0)1 42 34 24 80

Consulter le rapport d'information : http://www.senat.fr/notice-rapport/2022/r22-597-notice.html