Libre circulation des données non personnelles dans l'Union européenne

2017/0228(COD) - 04/10/2018 - Texte adopté du Parlement, 1ère lecture/lecture unique

Le Parlement européen a adopté par 520 voix pour, 81 contre et 6 abstentions, une résolution législative sur la proposition de règlement du Parlement européen et du Conseil concernant un cadre applicable à la libre circulation des données à caractère non personnel dans l'Union européenne.

La position du Parlement européen adoptée en première lecture suivant la procédure législative ordinaire a modifié la proposition de la Commission comme suit:

Objet: le règlement proposé vise à assurer la **libre circulation de données autres que les données à caractère personnel au sein de l'Union**, en établissant des règles concernant les exigences de localisation des données, la disponibilité des données pour les autorités compétentes et le portage des données pour les utilisateurs professionnels.

L'essor de l'internet des objets, l'intelligence artificielle et l'apprentissage automatique représentent des sources importantes de données à caractère non personnel. Parmi les données à caractère non personnel, le projet d'acte législatif cite notamment les ensembles de données agrégées et anonymisées utilisées pour l' analyse des mégadonnées, les données sur l'agriculture de précision qui peuvent aider à contrôler et à optimiser l'utilisation des pesticides et de l'eau, ou encore les données sur les besoins d'entretien des machines industrielles.

Principe de libre circulation des données à caractère non personnel: en vertu du texte amendé, les exigences de localisation des données seraient **interdites**, sauf si elles sont justifiées par des raisons impérieuses de **sécurité publique**, dans le respect du principe de proportionnalité.

Le concept de sécurité publique, au sens de l'article 52 du traité sur le fonctionnement de l'Union européenne et tel que l'interprète la Cour de justice, englobe à la fois la sécurité intérieure et extérieure d' un État membre, mais aussi les questions de sûreté publique.

Le Parlement a fixé une **échéance précise** (au plus tard **deux ans** après l'entrée en vigueur du règlement] avant laquelle les États membres doivent communiquer les exigences existantes de localisation des données qu'ils souhaitent maintenir. La Commission devrait examiner le projet d'acte dans un délai de six mois et adresser, le cas échéant, des **observations** à l'État membre concerné, y compris en lui recommandant de modifier ou d'abroger la mesure.

Les États membres devraient publier les détails de toutes les exigences de localisation des données par l' intermédiaire d'un **point d'information unique en ligne national**. La Commission publierait sur son site internet les liens vers ces points d'information unique ainsi qu'une liste consolidée régulièrement mise à jour de toutes les exigences de localisation des données.

Accès aux données pour les autorités compétentes: l'accès aux données par les autorités compétentes ne pourrait être refusé au motif que les données sont traitées dans un autre État membre.

Lorsqu'une autorité compétente **n'obtient pas l'accès aux données** après avoir contacté l'utilisateur du service de traitement de données et qu'il n'existe pas de mécanisme de coopération spécifique en vertu du

droit de l'Union ou d'accords internationaux pour l'échange de données entre autorités compétentes de différents États membres, cette autorité pourrait solliciter l'assistance de l'autorité compétente dans un autre État membre.

Les États membres pourraient imposer des **sanctions** effectives, proportionnées et dissuasives en cas de manquement à l'obligation de fournir des données, conformément au droit de l'Union et au droit national.

Codes de conduite: la Commission devrait encourager l'élaboration de codes de conduite par autorégulation au niveau de l'Union afin de contribuer à une économie des données compétitive, fondée sur les **principes de transparence et d'interopérabilité** et tenant compte des normes ouvertes, concernant, notamment, les aspects suivants :

- les bonnes pratiques qui facilitent le changement de fournisseurs et le portage des données dans des formats structurés, usuels, interopérables et lisibles par machine;
- les exigences minimales d'information afin que les utilisateurs professionnels disposent d' informations suffisamment détaillées, claires et transparentes, préalablement à la signature d'un contrat de traitement des données;
- les approches en matière de dispositifs de certification facilitant la comparaison entre les produits et services de traitement des données pour les utilisateurs professionnels.

La Commission devrait encourager les fournisseurs à terminer le développement des codes de conduite au plus tard un an après la date de publication du règlement et à les mettre effectivement en œuvre **au plus tard 18 mois** après cette date. Elle devrait veiller à ce que les codes de conduite soient élaborés en étroite coopération avec toutes les parties intéressées, y compris les associations de PME et de jeunes pousses, les utilisateurs et les fournisseurs de services en nuage.

Données mixtes: dans le cas d'un ensemble de données mixtes, à savoir un ensemble de données composé à la fois de données à caractère personnel et de données à caractère non personnel, le règlement devrait s' appliquer **aux données à caractère non personnel de l'ensemble**. Lorsque des données à caractère personnel et non personnel dans un ensemble de données mixtes sont inextricablement liées, le règlement s'appliquerait sans préjudice du règlement général sur la protection des données (règlement (UE) 2016/679).

Réexamen: au plus tard **quatre ans** après la date de publication du règlement, la Commission devrait soumettre un rapport évaluant la mise en œuvre du règlement, notamment en ce qui concerne: i) l' application du règlement aux ensembles de données mixtes; ii) la mise en œuvre par les États membres de l'exception relative à la sécurité publique; iii) l'élaboration et la mise en œuvre effective des codes de conduite.