

Informations de base	
2016/2225(INI) INI - Procédure d'initiative	Procédure terminée
Incidences des mégadonnées sur les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi Subject 1.10 Droits fondamentaux dans l'Union, Charte 1.20.09 Protection de la vie privée et des données 3.30.06 Technologies de l'information et de la communication, technologies numériques	

Acteurs principaux			
Parlement européen	Commission au fond		Date de nomination
	LIBE	Libertés civiles, justice et affaires intérieures	GOMES Ana (S&D) 07/03/2016
			Rapporteur(e) fictif/fictive VOSS Axel (PPE) ŠKRIPEK Branislav (ECR) PETERSEN Morten (ALDE) VERGIAT Marie-Christine (GUE/NGL) ALBRECHT Jan Philipp (Verts /ALE)
	Commission pour avis		Date de nomination
	ITRE	Industrie, recherche et énergie	La commission a décidé de ne pas donner d'avis.
Commission européenne	DG de la Commission		Commissaire
	Justice et consommateurs		JOUROVÁ Věra

Événements clés			
Date	Événement	Référence	Résumé

15/09/2016	Annonce en plénière de la saisine de la commission		
09/02/2017	Vote en commission		
20/02/2017	Dépôt du rapport de la commission	A8-0044/2017	Résumé
13/03/2017	Débat en plénière		
14/03/2017	Décision du Parlement	T8-0076/2017	Résumé
14/03/2017	Résultat du vote au parlement		
14/03/2017	Fin de la procédure au Parlement		

Informations techniques	
Référence de la procédure	2016/2225(INI)
Type de procédure	INI - Procédure d'initiative
Sous-type de procédure	Rapport d'initiative
Base juridique	Règlement du Parlement EP 55
Autre base juridique	Règlement du Parlement EP 165
État de la procédure	Procédure terminée
Dossier de la commission	LIBE/8/07753

Portail de documentation				
Parlement Européen				
Type de document	Commission	Référence	Date	Résumé
Projet de rapport de la commission		PE592.279	19/10/2016	
Amendements déposés en commission		PE595.750	19/12/2016	
Rapport déposé de la commission, lecture unique		A8-0044/2017	20/02/2017	Résumé
Texte adopté du Parlement, lecture unique		T8-0076/2017	14/03/2017	Résumé
Commission Européenne				
Type de document	Référence		Date	Résumé
Réaction de la Commission sur le texte adopté en plénière	SP(2017)390		22/08/2017	

Incidences des mégadonnées sur les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi

2016/2225(INI) - 14/03/2017 - Texte adopté du Parlement, lecture unique

Le Parlement européen a adopté par 561 voix pour, 71 contre et 49 abstentions, une résolution sur les incidences des mégadonnées pour les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi.

Les mégadonnées peuvent offrir des avantages aux citoyens, à la communauté universitaire et scientifique, aux secteurs privé et public, mais elles comportent également **des risques considérables**, notamment sur le plan de la protection des droits fondamentaux tels que le droit au respect de la vie privée.

Le Parlement a souligné que le **respect de la législation** en vigueur sur la protection des données, combiné à des **normes scientifiques et éthiques** rigoureuses, était essentiel pour créer la confiance dans les solutions en matière de mégadonnées ainsi que leur fiabilité.

Pour permettre aux citoyens de mieux connaître et comprendre la nature des mégadonnées, les députés ont préconisé d'investir dans la culture numérique et la sensibilisation aux droits numériques ainsi qu'à la protection des données et de la vie privée, y compris auprès des enfants.

Mégadonnées à des fins commerciales et dans le secteur public : la résolution a insisté sur la nécessité d'une responsabilité et d'une transparence nettement plus grandes dans le traitement et l'analyse des données par les secteurs privé et public.

Protection des données : les députés ont souligné l'importance :

- de promouvoir **la transparence, le respect du droit et la sécurité juridique**, et plus particulièrement les normes concrètes protégeant les droits fondamentaux et les garanties associées au traitement et à l'analyse des données par les secteurs privé et public ;
- de renforcer la collaboration entre les organismes de réglementation des pratiques dans l'environnement numérique ;
- de se concentrer sur la recherche et l'innovation dans le domaine de **l'anonymisation** et d'élaborer des **lignes directrices** sur l'anonymisation correcte des données, tout en assurant un suivi concernant les pratiques en la matière; l'anonymisation devrait être un processus irréversible ;
- de garantir que les technologies fondées sur les données **ne limitent pas l'accès à un environnement médiatique pluraliste**, mais favorisent plutôt la liberté et la pluralité des médias.

Les secteurs privé et public devraient utiliser les instruments fournis par le **règlement général sur la protection des données**, tels que les codes de conduite et les régimes de certification et à agir en conformité avec les normes et garanties juridiques appropriées de l'Union.

Sécurité : pour s'attaquer aux risques les plus urgents associés aux activités de traitement des données, le Parlement a :

- souligné la nécessité d'une véritable coopération entre les secteurs privé et public, les services répressifs et les autorités de contrôle indépendantes pour s'attaquer aux menaces que représentent **les failles de sécurité, l'accès non autorisé aux données et la surveillance illégale** ;
- préconisé d'encourager l'utilisation du **chiffrement de bout en bout** et, si nécessaire, de la rendre obligatoire en vertu du principe de protection intégrée des données ;
- recommandé l'application des principes de la **protection de la vie privée dès la conception et par défaut**.

Non-discrimination : les mégadonnées peuvent non seulement devenir une source d'inégalités de traitement et de discrimination indirecte à l'égard de groupes de citoyens notamment en termes d'équité et d'égalité des chances dans l'accès à l'éducation et à l'emploi.

Le Parlement a demandé de prendre toutes les mesures possibles afin de réduire au minimum toute discrimination et partialité algorithmiques, et de mettre en place un **cadre éthique commun** pour le traitement en toute transparence des données à caractère personnel et la prise de décision automatisée. Ce cadre commun pourrait servir de guide pour l'utilisation des données et pour l'application de la législation européenne en vigueur.

De plus, l'utilisation des mégadonnées **à des fins scientifiques** devrait se faire dans le respect de la charte des droits fondamentaux et conformément à la réglementation européenne en vigueur sur la protection des données.

Mégadonnées aux fins de l'application de la loi : les activités de surveillance de masse du gouvernement pourraient mettre à mal la confiance des citoyens dans les services numériques.

Soulignant l'importance du respect de la **directive (UE) 2016/680**, le Parlement s'est déclaré favorable à la publication de **lignes directrices, recommandations et bonnes pratiques** en vue de mieux préciser les critères et conditions applicables aux décisions fondées sur le profilage et l'utilisation de mégadonnées à des fins répressives.

La résolution a souligné la nécessité absolue de protéger les bases de données des services répressifs contre les failles de sécurité et l'accès illégal. Elle a invité à la plus grande prudence pour **éviter toute discrimination illégale** et le ciblage d'une certaine personne ou d'un certain groupe de personnes lors du traitement et de l'analyse de données.

Incidences des mégadonnées sur les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi

2016/2225(INI) - 20/02/2017 - Rapport déposé de la commission, lecture unique

La commission des libertés civiles, de la justice et des affaires intérieures a adopté un rapport d'initiative d'Ana GOMES (S&D, PT) sur les incidences des mégadonnées pour les droits fondamentaux: respect de la vie privée, protection des données, non-discrimination, sécurité et application de la loi.

Les mégadonnées peuvent offrir des avantages aux citoyens, à la communauté universitaire et scientifique, aux secteurs privé et public, mais elles comportent également des risques considérables, notamment sur le plan de la protection des droits fondamentaux tels que le droit au respect de la vie privée.

Le rapport a souligné que le **respect de la législation** en vigueur sur la protection des données, combiné à des **normes scientifiques et éthiques** rigoureuses, était essentiel pour créer la confiance dans les solutions en matière de mégadonnées ainsi que leur fiabilité.

Pour permettre aux citoyens de mieux connaître et comprendre la nature des mégadonnées, les députés ont préconisé d'investir dans la culture numérique et la sensibilisation aux droits numériques ainsi qu'à la protection des données et de la vie privée, y compris auprès des enfants.

Mégadonnées à des fins commerciales et dans le secteur public : le rapport a insisté sur la nécessité d'une responsabilité et d'une transparence nettement plus grandes dans le traitement et l'analyse des données par les secteurs privé et public.

Protection des données : les députés ont souligné le rôle fondamental que devraient jouer, à l'avenir, la Commission, le comité européen de la protection des données, les autorités nationales chargées de la protection des données et les autorités de contrôle indépendantes en vue de promouvoir **la transparence, le respect du droit et la sécurité juridique**, et plus particulièrement les normes concrètes protégeant les **droits fondamentaux**. Ils ont insisté sur l'importance de la recherche dans le domaine de **l'anonymisation** et invité à élaborer des lignes directrices sur l'anonymisation correcte des données.

Les secteurs privé et public ont été invités à utiliser les instruments fournis par le **règlement général sur la protection des données**, tels que les codes de conduite et les régimes de certification et à agir en conformité avec les normes et garanties juridiques appropriées de l'Union.

Sécurité : le rapport a souligné la nécessité d'une véritable coopération entre les secteurs privé et public, les services répressifs et les autorités de contrôle indépendantes pour s'attaquer aux menaces que représentent les failles de sécurité, l'accès non autorisé aux données et la surveillance illégale.

Le rapport a préconisé d'encourager l'utilisation du **chiffrement de bout en bout** et, si nécessaire, de la rendre obligatoire en vertu du principe de protection intégrée des données. Il a recommandé l'application des principes de la **protection de la vie privée dès la conception et par défaut**.

Non-discrimination : les députés ont demandé de prendre toutes les mesures possibles afin de réduire au minimum toute discrimination et partialité algorithmiques, et de mettre en place un **cadre éthique commun** pour le traitement en toute transparence des données à caractère personnel et la prise de décision automatisée. Ce cadre commun pourrait servir de guide pour l'utilisation des données et pour l'application de la législation européenne en vigueur.

De plus, l'utilisation des mégadonnées **à des fins scientifiques** devrait se faire dans le respect de la charte des droits fondamentaux et conformément à la réglementation européenne en vigueur sur la protection des données.

Mégadonnées aux fins de l'application de la loi : les députés ont rappelé à l'ensemble des intervenants chargés de faire respecter la loi qui ont recours au traitement et à l'analyse de données que la **directive (UE) 2016/680** régissait le traitement de données à caractère personnel effectué par les États membres à des fins répressives. Ils se sont déclarés favorables à la publication de **lignes directrices, recommandations et bonnes pratiques** en vue de mieux préciser les critères et conditions applicables aux décisions fondées sur le profilage et l'utilisation de mégadonnées à des fins répressives.

Enfin, le rapport a souligné la nécessité absolue de protéger les bases de données des services répressifs contre les failles de sécurité et l'accès illégal. Il a invité à la plus grande prudence pour **éviter toute discrimination illégale** et le ciblage d'une certaine personne ou d'un certain groupe de personnes lors du traitement et de l'analyse de données.