Jeudi 25 mars 2021

P9_TA(2021)0111

Rapport d'évaluation de la Commission sur la mise en œuvre du règlement général sur la protection des données deux ans après son entrée en application

Résolution du Parlement européen du 25 mars 2021 concernant le rapport d'évaluation de la Commission sur la mise en œuvre du règlement général sur la protection des données deux ans après son entrée en application (2020/2717(RSP))

(2021/C 494/11)

Le Parlement européen,

— vu l'article 8 de la charte des droits fondamentaux de l'Union européenne,

— vu l'article 16 du traité sur le fonctionnement de l'Union européenne,

— vu le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE («règlement général sur la protection des données», RGPD) ([1]),

— vu la déclaration de la Commission du 24 juin 2020 sur la Communication de la Commission au Parlement européen et au Conseil intitulée «La protection des données: un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique — deux années d'application du règlement général sur la protection des données»,

— vu la communication de la Commission du 24 juin 2020 au Parlement européen et au Conseil intitulée «La protection des données: un pilier de l'autonomisation des citoyens et de l'approche de l'Union à l'égard de la transition numérique — deux années d'application du règlement général sur la protection des données» (COM(2020)0264),

— vu la communication de la Commission du 24 juillet 2019 intitulée «Les règles en matière de protection des données comme instrument pour créer un climat de confiance dans l'Union européenne et au-delà — bilan» (COM(2019)0374),

— vu la contribution du comité européen de la protection des données (CEPD) à l'évaluation du règlement général sur la protection des données (RGPD) au titre de l'article 97, adoptée le 18 février 2020 ([2]),

— vu le «Premier aperçu de la mise en œuvre du RGPD et des rôles et moyens des autorités nationales de surveillance» par le CEPD, du 26 février 2019 ([3]),

— vu les lignes directrices adoptées par le CEPD au titre de l'article 70, paragraphe 1, point e), du RGPD,

— vu l'article 132, paragraphe 2, de son règlement intérieur,

— vu la proposition de résolution de la commission des libertés civiles, de la justice et des affaires intérieures,

A. considérant que le règlement général sur la protection des données (le «RGPD») est applicable depuis le 25 mai 2018; que tous les États membres, à l'exception de la Slovénie, ont adopté la nouvelle législation ou adapté leur législation nationale relative à la protection des données;

B. considérant que les citoyens sont de plus en plus conscients de leurs droits en vertu du RGPD, selon l'enquête sur les droits fondamentaux de l'Agence des droits fondamentaux de l'Union européenne; considérant que les citoyens continuent à rencontrer des difficultés lorsqu'ils tentent d'exercer ces droits, en particulier le droit d'accès, à la portabilité et à la transparence accrue, en dépit des mesures visant à faciliter l'exercice des droits des personnes concernées mises en place par les organisations;

C. considérant que depuis le début de l'application du RGPD, les autorités de contrôle ont assisté à une forte augmentation du nombre de plaintes qu'elles reçoivent; que cela témoigne du fait que les personnes concernées connaissent mieux leurs droits et veulent voir leurs données à caractère personnel protégées conformément au RGPD; que cela témoigne également, par ailleurs, de la persistance d'un grand nombre d'opérations de traitement illicite des données;

([1]) JO L 119 du 4.5.2016, p. 1.
([2]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_contributiongdprevaluation_20200218.pdf
([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

D. considérant que de nombreuses entreprises ont utilisé la période de transition entre l'entrée en vigueur du RGPD et son application pour faire du tri afin d'évaluer quels traitements des données sont vraiment réalisés et ceux qui pourraient ne plus être nécessaires ou justifiés;

E. considérant que de nombreuses autorités de protection des données (APD) ne sont pas en mesure de faire face au nombre de plaintes; que beaucoup d'entre elles manquent d'effectifs et de ressources et ne disposent pas d'un nombre suffisant d'experts en technologie;

F. considérant que le RGPD reconnaît que le droit des États membres devrait concilier les règles régissant la liberté d'expression et d'information, y compris l'expression journalistique, universitaire, artistique ou littéraire, et le droit à la protection des données à caractère personnel; que son article 85 dispose que la législation des États membres prévoit des dérogations pour les traitements de données effectués à des fins journalistiques ou à des fins d'expression universitaire, artistique ou littéraire, si elles sont nécessaires pour concilier le droit à la protection des données à caractère personnel avec la liberté d'expression et d'information;

G. considérant que, comme l'a également souligné le CEPD, la protection des sources journalistiques est la pierre angulaire de la liberté de la presse; que le RGPD ne devrait pas être utilisé de manière abusive à l'encontre des journalistes et pour limiter l'accès à l'information; qu'il ne devrait en aucun cas être utilisé par les autorités nationales pour étouffer la liberté des médias;

Observations générales

1. se félicite que le RGPD soit devenu un modèle au niveau mondial en matière de protection des données à caractère personnel et soit un facteur de convergence dans l'élaboration des normes; applaudit le fait que le RGPD a placé l'Union européenne au premier plan des discussions internationales sur la protection des données et que des pays tiers ont mis leur législation en la matière en conformité avec le RGPD; souligne que la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel a été alignée sur le RGPD (Convention 108+) et que 42 États l'ont déjà ratifiée; invite instamment la Commission ainsi que les États membres à profiter de cette dynamique pour faire pression au niveau des Nations unies, de l'Organisation de coopération et de développement économiques (OCDE), du G8 et du G20 en faveur de la création de normes internationales fondées sur les valeurs et les principes européens, sans affaiblir le RGPD; souligne qu'une position dominante de l'Europe dans ce domaine aiderait notre continent à mieux défendre les droits de nos citoyens, à sauvegarder nos valeurs et nos principes, à promouvoir une innovation numérique fiable et à accélérer la croissance économique en évitant la fragmentation;

2. conclut que, deux ans après son entrée en application, le RGPD est dans l'ensemble une réussite, et partage l'avis de la Commission selon lequel il est inutile à ce stade de mettre à jour ou de réexaminer la législation;

3. reconnaît que, jusqu'à la prochaine évaluation de la Commission, il convient de poursuivre le travail d'amélioration de la mise en œuvre du RGPD et les actions destinées à renforcer son application;

4. reconnaît la nécessité d'une application rigoureuse et effective du RGPD à dans les grandes plateformes numériques, les entreprises intégrées et d'autres services numériques, particulièrement dans les domaines de la publicité en ligne, du microciblage, du profilage algorithmique, ainsi que du classement, de la diffusion et de l'amplification du contenu;

Base juridique du traitement

5. souligne que les six bases juridiques énoncées à l'article 6 du RGPD sont également valables pour le traitement des données à caractère personnel, et qu'une même activité de traitement peut relever de plus d'une base juridique; invite les autorités de contrôle des données à indiquer que les responsables du traitement des données ne peuvent utiliser qu'un seul fondement juridique pour chaque finalité d'une activité traitement et à préciser comment chaque fondement est invoqué dans le cadre des opérations de traitement; s'inquiète que les responsables du traitement mentionnent souvent tous les fondements juridiques du RGPD dans leur déclaration de protection des données sans plus d'explications ni faire référence à l'opération de traitement spécifique concernée; croit qu'une telle pratique restreint la capacité des personnes concernées et des autorités de contrôle d'évaluer si ces fondements juridiques sont appropriés; rappelle que pour le traitement de catégories particulières de données à caractère personnel, il est nécessaire d'identifier un motif de licéité au titre de l'article 6 ainsi qu'une condition du traitement distincte au titre de l'article 9; rappelle aux responsables du traitement leur obligation légale de procéder à une analyse d'impact relative à la protection des données lorsque le traitement des données est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques;

6. rappelle que depuis l'entrée en application du RGPD, on entend par «consentement» toute manifestation de volonté, libre, spécifique, éclairée et univoque de la personne concernée; souligne que cela vaut également pour la directive vie privée et communications électroniques; fait observer que la mise en place d'un consentement valide reste compromise par l'utilisation d'interfaces truquées, un suivi omniprésent et d'autres pratiques contraires à l'éthique; est préoccupé par le fait que les personnes subissent souvent une pression financière qui prend la forme d'une invitation à donner son consentement en contrepartie de ristournes ou d'autres offres commerciales, ou qu'elles sont contraintes par des clauses de prestation subordonnée à donner leur consentement si elles veulent avoir accès à un service, en violation de l'article 7 du RGPD; rappelle les règles harmonisées du CEPD sur ce qui constitue un consentement valide, qui remplacent les diverses interprétations de nombreuses APD nationales et évitent la fragmentation au sein du marché unique numérique; rappelle également les lignes directrices du CEPD et de la Commission, qui établissent que lorsque la personne concernée a donné son consentement pour le traitement initial mais qu'un traitement ultérieur est prévu pour une autre finalité que celles pour lesquelles les données à caractère personnel ont été collectées initialement, le consentement initial ne peut légitimer un traitement ultérieur, car le consentement, pour être valide, doit être éclairé et spécifique; prend note des lignes directrices à venir du CEPD concernant le traitement des données à caractère personnel à des fins de recherche scientifique, qui clarifieront la signification du considérant 50 du RGPD;

7. s'inquiète de l'utilisation fréquente et abusive de l'intérêt légitime comme fondement juridique du traitement; souligne que les responsables du traitement continuent de fonder leur action sur l'intérêt légitime sans procéder à la mise en balance des intérêts, qui comprend une évaluation des droits fondamentaux; est particulièrement préoccupé par le fait que certains États membres adoptent des réglementations nationales pour déterminer les conditions du traitement fondées sur l'intérêt légitime, en prévoyant la mise en balance des intérêts respectifs du responsable du traitement et des personnes concernées, alors que le RGPD oblige chaque responsable du traitement à procéder individuellement à cette mise en balance et à se prévaloir de ce fondement juridique; s'inquiète du fait que certaines interprétations nationales de l'intérêt légitime ne respectent pas le considérant 47 et interdisent dans les faits le traitement sur la base d'un intérêt légitime; salue le fait que le CEPD a déjà entamé les travaux visant à actualiser l'avis du groupe de travail «article 29» sur l'application de l'intérêt légitime en tant que base juridique pour le traitement afin de remédier aux problèmes mis en évidence par le rapport de la Commission;

Droits de la personne concernée

8. souligne la nécessité de faciliter l'exercice des droits individuels prévus par le RGPD, tels que la portabilité des données, ou des droits en rapport avec le traitement automatisé, y compris le profilage; se félicite des lignes directrices du CEPD sur la prise de décision fondée sur un traitement automatisé et le droit à la portabilité des données; constate que, dans plusieurs secteurs, le droit à la portabilité des données n'a pas été pleinement mis en œuvre; demande au CEPD d'encourager les plateformes en ligne à créer un point de contact unique pour toutes leurs plateformes numériques sous-jacentes, duquel les demandes des utilisateurs peuvent être transférées au destinataire concerné; souligne que, conformément au principe de minimisation des données, la mise en œuvre du droit à l'anonymat empêche efficacement la divulgation non autorisée, l'usurpation d'identité et d'autres formes d'utilisation abusive des données à caractère personnel;

9. souligne que le respect du droit d'être informé exige des entreprises qu'elles fournissent des informations de manière concise, transparente, intelligible et facilement accessible et qu'elles évitent d'adopter une approche juridique lors de la rédaction des avis relatifs à la protection des données; est préoccupé par le fait que certaines entreprises continuent de manquer à leurs obligations au titre de l'article 12, paragraphe 1, du RGPD et ne fournissent pas toutes les informations pertinentes recommandées par le CEPD, notamment la liste des noms des entités avec lesquelles elles partagent des données; rappelle que l'obligation de fournir des informations simples et accessibles est particulièrement stricte lorsqu'il s'agit d'enfants; est préoccupé par l'absence globale de mécanismes d'accès fonctionnels pour les personnes concernées; souligne que les individus peuvent rarement contraindre les plateformes en ligne à leur révéler leurs données relatives au comportement de l'utilisateur; s'inquiète de ce que les entreprises ignorent trop souvent le fait que les données déduites sont également des données personnelles, soumises à toutes les garanties prévues par le RGPD;

Petites entreprises et organisations

10. souligne que certaines parties prenantes font valoir que l'application du RGPD fut particulièrement difficile, notamment pour les petites et moyennes entreprises (PME), les jeunes entreprises, les organisations et le milieu associatif, y compris les écoles, clubs et sociétés; note cependant l'ancienneté de nombreux droits et obligations du RGPD, qui étaient

déjà en vigueur en vertu de la directive 95/46/CE ([4]), mais étaient rarement appliqués; estime que le RGPD et son application ne doivent pas faire subir aux petites entreprises des conséquences involontaires en matière de conformité qui ne pèseraient pas sur les grandes entreprises; estime que les campagnes d'information des autorités nationales et de la Commission devraient proposer davantage de soutien, d'informations et de formation afin de contribuer à l'amélioration des connaissances, de la qualité de l'application des exigences et de la finalité du RGPD ainsi que de la sensibilisation à ces dernières;

11. souligne qu'il n'existe aucune dérogation pour les PME, les jeunes entreprises, les organisations et le milieu associatif, y compris les écoles, clubs et sociétés, et qu'elles relèvent du champ d'application du RGPD; demande par conséquent au CEPD de fournir des informations claires afin d'éviter toute confusion concernant l'interprétation du RGPD et de créer un outil pratique afin de faciliter la mise en œuvre du RGPD au sein des PME, des jeunes entreprises et des associations, y compris les écoles, clubs et sociétés dont les activités de traitement sont à faible risque; appelle les États membres à mettre suffisamment de moyens à disposition pour que les APD puissent informer au sujet de tels outils pratiques; encourage le CEPD à mettre au point des modèles de politique de protection de la vie privée à l'usage des organisations, afin de les aider à démontrer leur respect effectif du RGPD dans la pratique sans devoir recourir à des services tiers coûteux;

Exécution

12. exprime son inquiétude quant à l'exécution inégale et parfois inexistante du RGPD par les APD nationales, plus de deux ans après son entrée en application, et regrette dès lors que la situation en matière d'exécution n'ait pas été notablement améliorée par rapport à celle qui prévalait pour la directive 95/46/CE;

13. prend acte du fait qu'environ 275 000 plaintes ont été introduites et 785 amendes administratives imposées, pour diverses infractions, au cours des 18 premiers mois d'application du RGPD, mais signale que seule une très faible part des plaintes déposées a fait l'objet d'un suivi à l'heure actuelle; est conscient des problèmes causés par les violations de données à caractère personnel et rappelle les orientations actuelles du CEPD qui apportent des précisions notamment sur le calendrier de la notification, de la communication aux personnes concernées et des voies de recours; souligne qu'un formulaire type de déclaration des violations de données à l'échelle européenne pourrait être bénéfique s'agissant d'harmoniser les différentes approches nationales; déplore toutefois la variation considérable des amendes selon les États membres et le montant de certaines amendes infligées aux grandes entreprises, trop faible pour avoir l'effet dissuasif escompté contre les violations de la protection des données; appelle les APD à renforcer le l'exécution, les poursuites et les pénalités s'agissant de violations de la protection des données, ainsi qu'à utiliser pleinement les possibilités offertes par le RGPD pour imposer des amendes et faire usage des autres mesures correctrices; souligne que les interdictions du traitement ou l'obligation de supprimer les données personnelles acquises d'une manière non conforme au RGPD peuvent avoir un effet dissuasif tout aussi important, sinon plus, que les amendes; demande à la Commission et au CEPD d'harmoniser les sanctions au moyen de recommandations et de critères clairs, comme l'a fait la conférence des autorités de contrôle allemandes, afin d'accroître la sécurité juridique et d'empêcher les entreprises de s'installer dans les zones imposant les plus faibles sanctions;

14. est préoccupé par la durée des enquêtes menées par certaines APD et par ses effets préjudiciables quant à l'application effective du règlement et la confiance des citoyens; exhorte les APD à accélérer la résolution des affaires, ainsi qu'à faire usage de tout l'éventail des possibilités offertes par le RGPD, en particulier en cas de violations systématiques et persistantes, et notamment lorsqu'il existe un intérêt lucratif et un grand nombre de personnes concernées;

15. s'inquiète du fait que les autorités de contrôle de 21 États parmi les 31 États auxquels s'applique le RGPD (à savoir les États membres de l'Union européenne, l'Espace économique européen et le Royaume-Uni) ont explicitement déclaré ne pas disposer des ressources humaines, techniques et financières, ni des locaux et infrastructures suffisants pour remplir correctement leur mission et exercer leurs pouvoirs; s'inquiète du manque de personnel technique spécialisé dans la plupart des autorités de contrôle de l'Union, ce qui complique les enquêtes et l'application de la législation; observe avec inquiétude que les autorités de surveillance sont sous pression étant donné le déséquilibre croissant entre leurs responsabilités en matière de protection des données à caractère personnel et les ressources dont elles disposent; constate que les services numériques sont amenés à devenir de plus complexes en raison de l'utilisation accrue d'innovations telles que l'intelligence artificielle (c'est-à-dire d'une aggravation du problème du manque de transparence du traitement des données, notamment

([4]) Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31).

pour l'entraînement des algorithmes); souligne par conséquent qu'il importe que les autorités de contrôle de l'Union et le CEPD disposent de ressources financières, techniques et humaines suffisantes pour être à même de traiter rapidement mais en profondeur un nombre croissant d'affaires complexes nécessitant d'importantes ressources, ainsi que de coordonner et faciliter la coopération entre les APD nationales, afin de surveiller correctement l'application du RGPD et de protéger les droits et libertés fondamentaux; craint que l'insuffisance des ressources des APD, en particulier si l'on compare leurs ressources aux revenus des grandes entreprises du secteur des technologies de l'information, n'aboutisse à des accords de règlements pour limiter le coût de procédures pesantes et laborieuses;

16. invite la Commission à évaluer la possibilité d'obliger les grandes entreprises de technologie multinationales à payer pour leur propre surveillance au moyen de l'introduction d'une taxe numérique européenne;

17. constate avec inquiétude que l'application insuffisante de la législation par les APD et l'inaction de la Commission pour remédier au manque de ressources de ces autorités laissent la charge de l'application de la législation aux particuliers qui portent les plaintes relatives à la protection des données devant les tribunaux; est préoccupé par le fait que les tribunaux ordonnent parfois l'indemnisation des demandeurs individuels, sans pour autant ordonner à l'organisation ou à l'entreprise de résoudre des problèmes structurels; considère que la mise en œuvre de la législation à l'initiative de la sphère privée peut entraîner une jurisprudence importante, mais ne remplace pas son exécution par les APD ou des mesures de la Commission pour remédier au manque de ressources; déplore que ces États membres enfreignent l'article 52, paragraphe 4, du RGPD; demande dès lors aux États membres de se conformer à leur obligation légale, en vertu de l'article 52, paragraphe 4, d'allouer des fonds suffisants à leurs APD afin qu'elles puissent mener à bien leur travail de la meilleure manière possible et de garantir des conditions de concurrence équitables au niveau européen s'agissant de l'application du RGPD; regrette que la Commission n'ait pas encore engagé de procédures d'infraction à l'encontre des États membres qui ne respectent pas les obligations qui leur incombent en vertu du RGPD, et invite instamment la Commission à le faire sans délai; demande à la Commission et au CEPD d'assurer un suivi de la communication de la Commission du 24 juin 2020, qui évalue le fonctionnement du RGPD et son application;

18. regrette que les États membres aient décidé, dans leur majorité, de ne pas appliquer l'article 80, paragraphe 2, du RGPD; demande à tous les États membres de faire usage de l'article 80, paragraphe 2 et de mettre en œuvre le droit d'introduire des réclamations et de saisir la justice sans être mandaté par une personne concernée; invite les États membres à clarifier le rôle des plaignants au cours des procédures dans la législation relative aux procédures administratives nationales s'appliquant aux autorités de contrôle; souligne qu'il convient de mettre en évidence la possibilité d'intervention des plaignants, qui ne jouent pas un rôle purement passif, à différents stades de la procédure;

Coopération et cohérence

19. souligne que le faible degré d'application est particulièrement évident dans les réclamations transfrontalières, et déplore que, dans 14 États membres, les autorités chargées de la protection des données ne disposent pas des ressources adéquates pour contribuer aux mécanismes de coopération et de cohérence; demande au CEPD d'intensifier ses efforts afin d'assurer l'application correcte des articles 60 et 63 du RGPD, et rappelle aux autorités de contrôle qu'elles peuvent faire usage, dans des circonstances exceptionnelles, de la procédure d'urgence visée à l'article 66 du RGPD, en particulier des mesures provisoires;

20. souligne l'importance du mécanisme du guichet unique pour assurer la sécurité juridique et réduire la charge administrative des entreprises et des citoyens; exprime cependant sa grande préoccupation quant au fonctionnement du mécanisme, notamment en ce qui concerne le rôle de l'autorité irlandaise et luxembourgeoise chargée de la protection des données; fait observer que les autorités en question doivent traiter un grand nombre de cas, de nombreuses entreprises de technologie ayant enregistré leur siège social européen en Irlande ou au Luxembourg; s'inquiète particulièrement du fait que l'autorité irlandaise de protection des données clôture généralement la plupart des affaires par un règlement plutôt que par une sanction et que les affaires soumises à l'Irlande en 2018 n'ont même pas atteint le stade de projet de décision conformément à l'article 60, paragraphe 3, du RGPD; demande à ces autorités chargées de la protection des données d'accélérer leurs enquêtes en cours concernant des affaires importantes afin de montrer aux citoyens européens que la protection des données est un droit opposable dans l'Union; souligne que le succès du «mécanisme du guichet unique» dépend du temps et des efforts que les autorités chargées de la protection des données peuvent consacrer au traitement des affaires transfrontalières individuelles et à la coopération sur ces affaires au sein du CEPD, et que le manque de volonté politique et de ressources a des conséquences immédiates sur le bon fonctionnement de ce mécanisme;

21. relève des incohérences entre les directives des États membres et les lignes directrices du CEPD; souligne que les autorités nationales chargées de la protection des données peuvent arriver à différentes interprétations du RGPD, ce qui entraîne des applications divergentes parmi les États membres; note que cette situation crée des avantages ainsi que des inconvénients géographiques pour les entreprises; presse la Commission d'évaluer si les procédures administratives nationales entravent la pleine efficacité de la coopération au titre de l'article 60 du RGPD ainsi que sa mise en œuvre

effective; appelle les autorités chargées de la protection des données à fournir une interprétation et des recommandations cohérentes au travers du CEPD; demande en particulier au CEPD d'établir les éléments de base d'une procédure administrative commune pour traiter les réclamations dans les affaires transfrontalières en vertu de la coopération mise en place au titre de l'article 60; insiste pour que soient suivies à cette fin des recommandations concernant des calendriers communs pour la réalisation des enquêtes et l'adoption des décisions; demande au CEPD de renforcer le mécanisme de cohérence et de le rendre obligatoire pour toute question d'application générale ou pour toute affaire ayant des effets transfrontaliers, afin d'éviter l'incohérence des approches et des décisions des différentes autorités chargées de la protection des données, car celle-ci menacerait l'uniformité d'interprétation et d'application du RGPD; estime que cette interprétation, cette application et ces recommandations communes contribueront à la création et au succès du marché unique numérique;

22. demande au CEPD de publier son ordre du jour avant ses réunions et de fournir aux citoyens et au Parlement des résumés plus détaillés de ses réunions;

Fragmentation de la mise en œuvre du RGPD

23. déplore que l'utilisation par les États membres de clauses de spécification facultatives (par exemple: le traitement dans le cadre d'une mission d'intérêt public ou par les autorités publiques sur la base de la loi et de l'âge de consentement de l'État membre) ait été préjudiciable à la réalisation de l'harmonisation totale de la protection des données et à l'élimination des différences de conditions de marché pour les entreprises de l'Union, et craint que cela puisse augmenter le coût de la mise en conformité avec le RGPD; demande au CEPD de présenter des recommandations sur la manière de traiter les différences de mise en œuvre des clauses de spécification facultatives entre les États membres; invite la Commission à utiliser ses pouvoirs pour intervenir dans les États membres lorsque des mesures, actions et décisions nationales portent atteinte à l'esprit, à l'objectif et au texte du RGPD, afin d'éviter une protection inégale des citoyens et des distorsions du marché; souligne, à ce propos, que les États membres ont adopté un éventail d'âges différents pour l'accord parental; demande donc à la Commission et aux États membres d'évaluer l'incidence de cette fragmentation sur les activités des enfants et leur protection en ligne; souligne qu'en cas de conflit de lois entre une loi nationale d'un État membre et le RGPD, les dispositions du RGPD devraient l'emporter;

24. se dit très préoccupé quant à l'usage abusif que les autorités publiques de certains États membres font du RGPD pour restreindre les journalistes et les organisations non gouvernementales; partage résolument l'avis de la Commission selon lequel les règles de protection des données ne devraient pas entraver l'exercice de la liberté d'expression et d'information, notamment en créant un effet dissuasif ou en étant interprétées comme un moyen de pression sur les journalistes pour qu'ils révèlent leurs sources; exprime toutefois sa déception quant au fait que la Commission n'a toujours pas terminé son évaluation du respect de l'équilibre entre le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information, consacré à l'article 85 du RGPD; invite la Commission à achever dans les meilleurs délais son évaluation des législations nationales à cet égard et à utiliser tous les outils disponibles, y compris les procédures d'infraction, pour veiller au respect du RGPD par les États membres et pour limiter toute fragmentation du cadre de protection des données;

Protection des données dès la conception

25. demande aux autorités de contrôle d'évaluer la mise en œuvre de l'article 25 relatif à la protection des données dès la conception et à la protection des données par défaut, notamment en vue d'évaluer les mesures techniques et opératoires nécessaires pour appliquer les principes de minimisation des données et de limitation de la finalité, ainsi que pour déterminer l'effet qu'a eu cette disposition sur les fabricants de technologies de traitement; se félicite du fait que le CEPD ait adopté, en octobre 2020, les lignes directrices 04/2019 relatives à la protection des données dès la conception et à la protection des données par défaut au titre de l'article 25 afin de contribuer à la clarté juridique des concepts; demande aux autorités de contrôle d'évaluer également l'utilisation correcte des paramètres par défaut prévus à l'article 25, paragraphe 2, y compris par les principaux prestataires de services en ligne; recommande que le CEPD adopte des lignes directrices pour déterminer dans quelles conditions spécifiques et dans quels cas ou catégories de cas les fabricants de technologies de l'information et de la communication doivent être considérés comme des responsables du traitement en vertu de l'article 4, paragraphe 7, en ce sens qu'ils déterminent les moyens du traitement; souligne que les pratiques de protection des données dépendent encore largement de tâches manuelles et de configurations arbitraires, ainsi que de systèmes incompatibles; demande au CEPD d'élaborer des lignes directrices destinées à favoriser la mise en œuvre pratique des exigences en matière de protection des données, y compris des lignes directrices portant sur les analyses d'impact relatives à la protection des données (article 35), la protection des données dès la conception et la protection des données par défaut (article 25), les informations à communiquer aux personnes concernées (articles 12 à 14), l'exercice des droits des personnes concernées (articles 15 à 18, 20 et 21) et les registres pour les activités de traitement (article 30); demande au CEPD de s'assurer que ces lignes directrices soient d'une application aisée et permettent également une communication de machine à machine entre

les personnes concernées, les responsables du traitement et les autorités chargées de la protection des données, assurant ainsi l'automatisation de la protection des données; invite la Commission à développer les icônes exploitables sur machine pour l'information des personnes concernées, conformément à l'article 12, paragraphe 8, en étroite coordination avec le CEPD; encourage le CEPD et les autorités de contrôle à exploiter pleinement le potentiel de l'article 21, paragraphe 5, sur l'exercice du droit d'opposition au traitement de données à caractère personnel à l'aide de procédés automatisés;

Lignes directrices

26. demande au CEPD d'harmoniser la mise en œuvre pratique des exigences en matière de protection des données grâce à l'élaboration de lignes directrices portant, entre autres, sur la nécessité d'évaluer les risques liés à l'information des personnes concernées quant au traitement des données (articles 12 à 14), à l'exercice des droits des personnes concernées (articles 15 à 18, 20 et 21) et à la mise en œuvre du principe de responsabilité; demande au CEPD de publier des lignes directrices classant les différents cas d'utilisation légitime du profilage en fonction des risques qu'ils présentent pour les droits et libertés des personnes concernées, ainsi que des recommandations concernant les mesures d'ordre technique et organisationnel appropriées et une définition claire des cas d'utilisation illicite; invite le CEPD à examiner l'avis 05/2014 du groupe de travail «article 29» sur la protection des données, du 10 avril 2014, concernant les Techniques d'anonymisation et à établir une liste de critères univoques pour parvenir à l'anonymisation; encourage le CEPD à clarifier le traitement des données à des fins de ressources humaines; prend acte de la conclusion du CEPD selon laquelle la nécessité d'évaluer les risques liés au traitement des données, comme le prévoit le RGPD, devrait être maintenue, étant donné que les risques pour les personnes concernées ne sont pas liés à la taille des responsables du traitement; appelle à une meilleure utilisation du mécanisme par lequel la Commission peut demander l'avis du CEPD sur les questions qui relèvent du RGPD;

27. fait observer que la pandémie de COVID-19 a mis en évidence la nécessité d'orientations claires de la part des autorités chargées de la protection des données et du CEPD sur la mise en œuvre et l'application appropriées du RGPD dans les politiques de santé publique; rappelle, à cet égard, les lignes directrices 03/2020 sur le traitement de données concernant la santé à des fins de recherche scientifique dans le contexte de la pandémie de COVID-19 et les lignes directrices 04/2020 relatives à l'utilisation de données de localisation et d'outils de recherche de contacts dans le cadre de la pandémie de COVID-19; demande à la Commission d'assurer le plein respect du RGPD lors de la création de l'espace européen commun des données de santé;

Flux internationaux de données à caractère personnel et coopération internationale

28. souligne l'importance de permettre un libre flux des données à caractère personnel à l'échelle internationale sans abaisser le niveau de protection garanti au titre du RGPD; soutient la pratique de la Commission européenne qui consiste à traiter la protection des données et les flux de données à caractère personnel séparément des accords commerciaux; estime que la coopération internationale dans le domaine de la protection des données et la convergence des règles pertinentes vers le RGPD amélioreront la confiance mutuelle, favoriseront la compréhension des défis technologiques et juridiques et, à terme, faciliteront les flux transfrontaliers de données qui sont d'une importance capitale pour le commerce international; reconnaît l'existence d'exigences juridiques contradictoires pour les entreprises qui mènent des activités de traitement de données dans l'Union ainsi que dans les juridictions de pays tiers, notamment aux États-Unis;

29. souligne que les décisions d'adéquation ne doivent pas être de nature politique, mais juridique; encourage la poursuite des efforts visant à promouvoir des cadres juridiques globaux permettant les transferts de données sur la base du RGPD et de la convention 108 + du Conseil de l'Europe; constate, en outre, que les parties prenantes considèrent les décisions d'adéquation comme un instrument essentiel pour ces flux de données puisqu'elles ne leur ajoutent pas de conditions ou d'autorisations supplémentaires; souligne toutefois que, jusqu'à présent, des décisions d'adéquation n'ont été adoptées que pour neuf pays, bien que de nombreux autres pays tiers aient récemment adopté de nouvelles lois sur la protection des données comportant des règles et des principes similaires à ceux du RGPD; relève que, à ce jour, aucun mécanisme garantissant le transfert légal de données à caractère personnel en vue d'un usage commercial entre l'UE et les États-Unis n'a résisté à un recours juridique devant la Cour de Justice de l'Union européenne;

30. se félicite de l'adoption de la première décision d'adéquation mutuelle entre l'Union et le Japon, donnant naissance au plus grand espace de libre circulation sécurisée des données au monde; demande cependant à la Commission de tenir compte de tous les problèmes soulevés par le Parlement lors du premier examen de cet instrument et de publier les résultats dès que possible, étant donné que cet examen aurait dû être adopté pour janvier 2021;

31. demande à la Commission de publier l'ensemble des critères utilisés pour déterminer si un pays tiers est réputé assurer un niveau de protection «essentiellement équivalent» à celui garanti dans l'Union, notamment pour ce qui est de l'accès aux voies de recours et de l'accès des pouvoirs publics aux données; insiste sur la nécessité de garantir l'application et

le respect effectifs des dispositions de l'article 48 du RGPD relatives aux transferts ou aux divulgations non autorisés par l'Union, en particulier en ce qui concerne les demandes d'accès aux données à caractère personnel dans l'Union présentées par les autorités de pays tiers; demande au CEPD et aux autorités chargées de la protection des données d'émettre des recommandations et d'appliquer ces dispositions, notamment pour l'évaluation et le développement de mécanismes de transfert de données à caractère personnel;

32. invite la Commission à adopter des actes délégués afin de préciser les critères à prendre en compte pour le mécanisme de certification en matière de protection des données visé à l'article 42, paragraphe 1, le but étant de stimuler l'utilisation de ce mécanisme, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées, comme instrument pour les transferts internationaux, conformément à l'article 46, paragraphe 2, point f);

33. répète que les programmes de surveillance de masse qui incluent la collecte des données en masse empêchent les constats d'adéquation; demande instamment à la Commission d'appliquer les conclusions de la Cour de justice de l'Union européenne dans les arrêts Schrems I ([5]), Schrems II ([6]) et Privacy International et al. (2020) ([7]) à toutes ses évaluations des décisions d'adéquation ainsi qu'aux négociations en cours et à venir; rappelle que les transferts reposant sur des dérogations pour des situations spécifiques conformément à l'article 49 du RGPD devraient rester exceptionnels; se félicite des lignes directrices du CEPD et des autorités chargées de la protection des données à cet égard et les invite à assurer une interprétation cohérente lors de l'application et du contrôle de ces dérogations, conformément aux lignes directrices du 02/2018 du CEPD;

34. demande aux autorités chargées de la protection des données et à la Commission de déterminer de manière systématique si les règles de protection des données sont respectées dans la pratique par les pays tiers, conformément à la jurisprudence de la Cour de justice de l'Union européenne;

35. demande instamment à la Commission de publier dans les meilleurs délais son examen des décisions d'adéquation adoptées en vertu du RGPD; souligne que, en l'absence de décision d'adéquation, les clauses contractuelles types sont l'outil le plus largement utilisé pour les transferts internationaux de données; relève que la Cour de justice de l'Union européenne a confirmé la validité de la décision 2010/87/UE relative aux clauses contractuelles types ([8]) tout en requérant une évaluation du niveau de protection accordé aux données transférées dans un pays tiers et des éléments pertinents du système juridique de ce pays tiers au regard de l'accès de ses autorités publiques aux données à caractère personnel transférées; invite instamment la Commission à accélérer ses travaux de modernisation des clauses contractuelles types pour les transferts internationaux de données afin de garantir des conditions de concurrence équitables pour les petites et moyennes entreprises (PME) au niveau international; se félicite de la publication d'un projet de clauses contractuelles types par la Commission et de l'objectif visant à rendre les clauses contractuelles types plus faciles à utiliser et à remédier aux lacunes décelées dans les normes actuelles;

36. rappelle les lignes directrices 1/2019 du CEPD relatives aux codes de conduite et aux organismes de suivi au titre du règlement (UE) 2016/679; constate que cet instrument est actuellement sous-utilisé, alors qu'il garantit la conformité au RGPD lorsqu'il est assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées; souligne le potentiel que présente cet instrument pour ce qui est de mieux soutenir les PME et d'apporter une plus grande sécurité juridique dans le contexte des transferts internationaux de données entre différents secteurs;

Future législation de l'Union européenne

37. estime que grâce à sa neutralité technologique, le RGPD fournit un cadre réglementaire solide pour les technologies émergentes; estime néanmoins que davantage d'efforts sont nécessaires pour aborder des questions plus larges de numérisation, telles que les situations de monopole et les déséquilibres de pouvoir, au moyen d'une réglementation spécifique, et pour examiner attentivement la corrélation du RGPD avec chaque nouvelle initiative législative afin d'assurer

---

([5]) Arrêt de la Cour de justice du 6 octobre 2015, *Maximillian Schrems* contre *Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.

([6]) Arrêt de la Cour de justice du 16 juillet 2020, *Data Protection Commissioner* contre *Facebook Ireland Ltd et Maximillian Schrems* C-311/18, ECLI:EU:C:2020:559.

([7]) Arrêts dans l'affaire C-623/17, Privacy International, et dans les affaires conjointes C-511/18, La Quadrature du Net e.a., C-512/18, French Data Network e.a., et C-520/18, Ordre des barreaux francophones et germanophone e.a.

([8]) Décision 2010/87/UE du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, modifiée par la décision d'exécution (UE) 2016/2297 de la Commission du 16 décembre 2016 (JO L 39 du 12.2.2010, p. 5)

la cohérence et de remédier aux lacunes juridiques; rappelle à la Commission son obligation de veiller à ce que les propositions législatives, par exemple sur la gouvernance des données, sur les données, sur les services numériques ou sur l'intelligence artificielle, soient toujours conformes au RGPD et à la directive en matière de protection des données dans le domaine répressif ([9]); estime que les textes définitifs adoptés par les colégislateurs dans le cadre de négociations interinstitutionnelles doivent respecter pleinement l'acquis en matière de protection des données; déplore cependant que la Commission elle-même n'ait pas toujours une approche cohérente de la protection des données dans ses propositions législatives; souligne qu'une référence à l'application du RGPD, ou la mention «sans préjudice du RGPD», n'assure pas d'office la conformité d'une proposition au RGPD; demande à la Commission de consulter le Contrôleur européen de la protection des données et le CEPD lorsque l'adoption de propositions d'acte législatif a un impact sur la protection des droits et libertés des personnes au regard du traitement des données à caractère personnel; invite également la Commission, lorsqu'elle prépare des propositions de recommandations, à s'efforcer de consulter le Contrôleur européen de la protection des données afin d'assurer la cohérence des règles de protection des données à travers l'Union, et à toujours procéder à une analyse d'impact;

38. observe que le profilage, même si l'article 22 du RGPD ne le permet que dans des conditions strictes et rigoureuses, est de plus en plus utilisé car les activités en ligne d'une personne permettent d'acquérir des connaissances approfondies sur sa psychologie et sa vie privée; relève que, puisque le profilage permet de manipuler le comportement des utilisateurs, il convient de limiter la collecte et le traitement de données à caractère personnel relatives à l'utilisation de services numériques à la mesure strictement nécessaire pour fournir le service et le facturer; invite la Commission à proposer une législation sectorielle stricte en matière de protection des données pour les catégories sensibles de données à caractère personnel, si elle ne l'a pas encore fait; demande l'application stricte du RGPD dans le traitement des données à caractère personnel;

39. appelle à l'autonomisation des consommateurs, de sorte qu'ils puissent prendre des décisions éclairées sur les implications de l'utilisation de nouvelles technologies pour le respect de la vie privée et demande d'assurer un traitement équitable et transparent en fournissant des options faciles à utiliser pour donner et retirer le consentement au traitement de leurs données à caractère personnel conformément au RGPD;

Directive en matière de protection des données dans le domaine répressif

40. est préoccupé par la grande insuffisance des règles de protection des données utilisées à des fins répressives pour faire face aux compétences nouvellement créées en matière d'application de la loi; demande à la Commission d'évaluer la directive en matière de protection des données dans le domaine répressif avant l'échéance prévue dans la directive et de rendre cette évaluation publiquement accessible;

Le règlement «vie privée et communications électroniques»

41. se dit profondément préoccupé par l'absence de mise en œuvre par les États membres de la directive vie privée et communications électroniques ([10]) compte tenu des changements introduits par le RGPD; demande à la Commission d'accélérer son évaluation et d'engager des procédures d'infraction à l'encontre des États membres qui n'appliquent pas correctement la directive vie privée et communications électroniques; craint vivement que le retard de plusieurs années pris dans la réforme des règles en matière de protection de la vie privée dans le secteur des communications électroniques ne conduise à une fragmentation du paysage juridique dans l'Union, au détriment des entreprises et des citoyens; rappelle que le règlement «vie privée et communications électroniques» ([11]) a été conçu pour compléter et préciser le RGPD et coïncider avec l'entrée en application du RGPD; souligne que la réforme des règles en matière de protection de la vie privée dans le secteur des communications électroniques ne doit pas mener à un abaissement du niveau actuel de protection apporté au titre du RGPD et de la directive privée et communications électroniques; regrette qu'il ait fallu quatre ans au Conseil pour finalement adopter sa position de négociation sur la proposition de règlement «vie privée et communications électroniques», alors que le Parlement a adopté sa position de négociation en octobre 2017; rappelle qu'il importe d'actualiser les règles de protection de la vie privée dans le secteur des communications électroniques de 2002 et 2009 afin d'améliorer la protection des droits fondamentaux des citoyens et la sécurité juridique des entreprises, en complément du RGPD;

([9]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

([10]) Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (JO L 201 du 31.7.2002, p. 37).

([11]) Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (COM(2017)0010).

Jeudi 25 mars 2021

o

o o

42. charge son Président de transmettre la présente résolution à la Commission, au Conseil européen, aux gouvernements et aux parlements nationaux des États membres, au comité européen de la protection des données et au Contrôleur européen de la protection des données.