Vendredi 21 mai 2021

P9_TA(2021)0262

Niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni

Résolution du Parlement européen du 21 mai 2021 sur le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni (2021/2594(RSP))

(2022/C 15/23)

Le Parlement européen,

— vu la charte des droits fondamentaux de l'Union européenne (ci-après «la charte»), en particulier ses articles 7, 8, 16 et 47 ainsi que son article 52,

— vu l'arrêt de la Cour de justice de l'Union européenne (ci-après la «Cour de justice») du 16 juillet 2020 dans l'affaire C-311/18, *Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems* (arrêt Schrems II) ([1]),

— vu l'arrêt de la Cour de justice du 6 octobre 2015 dans l'affaire C-362/14, *Maximillian Schrems contre Data Protection Commissioner* (arrêt Schrems I) ([2]),

— vu l'arrêt de la Cour de justice du 6 octobre 2020 dans l'affaire C-623/17, *Privacy International contre Secretary of State of Foreign and Commonwealth affairs* ([3]),

— vu sa résolution du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures ([4]),

— vu sa résolution du 5 juillet 2018 sur l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis ([5]),

— vu sa résolution du 25 octobre 2018 sur l'exploitation des données des utilisateurs de Facebook par Cambridge Analytica et les conséquences en matière de protection des données ([6]),

— vu sa résolution du 20 mai 2021 sur l'arrêt rendu par la Cour de justice de l'Union européenne le 16 juillet 2020 dans l'affaire C-311/18, Data Protection Commissioner contre Facebook Ireland Ltd et Maximillian Schrems («arrêt Schrems II») ([7]),

— vu sa résolution du 26 novembre 2020 sur l'examen de la politique commerciale de l'Union ([8]),

— vu l'accord de commerce et de coopération du 31 décembre 2020 entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part ([9]),

— vu sa résolution du 28 avril 2021 sur le résultat des négociations entre l'Union européenne et le Royaume-Uni ([10]),

— 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 (règlement général sur la protection des données) ([11]) (RGPD),

---

([1]) ECLI:EU:C:2020:559.
([2]) ECLI:EU:C:2015:650.
([3]) ECLI:EU:C:2020:790.
([4]) JO C 378 du 9.11.2017, p. 104.
([5]) JO C 118 du 8.4.2020, p. 133.
([6]) JO C 345 du 16.10.2020, p. 58.
([7]) Textes adoptés de cette date, P9_TA(2021)0256.
([8]) Textes adoptés de cette date, P9_TA(2020)0337.
([9]) JO L 444 du 31.12.2020, p. 14.
([10]) Textes adoptés de cette date, P9_TA(2021)0141.
([11]) JO L 119 du 4.5.2016, p. 1.

— vu la 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 ([12]) (directive en matière de protection des données dans le domaine répressif),

— vu la 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 ([13]),

— vu la 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 (COM(2017)0010), présentée par la Commission le 10 janvier 2017, ainsi que la position du Parlement y relative du 20 octobre 2017 ([14]),

— vu les recommandations du comité européen de la protection des données (EDPB), y compris sa déclaration du 9 mars 2021 sur le règlement «vie privée et communications électroniques» et ses recommandations 01/2020 du 10 novembre 2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE,

— vu les critères de référence adoptés par le groupe de travail «article 29» le 6 février 2018 et approuvés par le comité européen de la protection des données,

— vu les recommandations 01/2021 du comité européen de la protection des données du 2 février 2021 sur les critères de référence dans le cadre de la directive en matière de protection des données dans le domaine répressif,

— vu les projets de décision d'adéquation publiés par la Commission le 19 février 2021, l'une au titre du RGPD ([15]) et l'autre au titre de la directive en matière de protection des données dans le domaine répressif ([16]),

— vu les avis 14/2021 et 15/2021 du comité européen de la protection des données du 13 avril 2021 concernant le projet de décision d'exécution de la Commission européenne conformément à la directive (UE) 2016/680 concernant le niveau de protection adéquat des données à caractère personnel au Royaume-Uni;

— vu la convention européenne des droits de l'homme (CEDH) et la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ainsi que son protocole d'amendement («convention 108+»), auxquelles le Royaume-Uni est partie,

— vu l'article 11 du règlement (UE) nº 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission,

— 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 la possibilité de transférer des données à caractère personnel par-delà les frontières peut être un moteur essentiel d'innovation, de productivité et de compétitivité économique, et qu'elle revêt une importance cruciale pour garantir une coopération efficace dans la lutte contre la criminalité organisée et la grande criminalité transfrontières ainsi que contre le terrorisme, lutte qui s'appuie de plus en plus sur l'échange de données à caractère personnel;

B. considérant que dans son arrêt Schrems I, la Cour de justice indique que l'accès indifférencié, par les autorités du renseignement, au contenu des communications électroniques porte atteinte au contenu essentiel du droit à la confidentialité des communications consacré à l'article 7 de la charte, et que les États-Unis ne prévoient pas, pour les non-ressortissants américains, suffisamment de voies de recours judiciaires contre la surveillance de masse, en violation de l'article 47 de la charte;

([12]) JO L 119 du 4.5.2016, p. 89.
([13]) JO L 201 du 31.7.2002, p. 37.
([14]) A8-0324/2017.
([15]) Projet de décision d'exécution de la Commission conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par le Royaume-Uni.
([16]) Projet de décision d'exécution de la Commission conformément à la directive (UE) 2016/680 du Parlement européen et du Conseil relative à la protection des personnes physiques par le Royaume-Uni.

C. considérant que le Royaume-Uni a toujours été un partenaire commercial important de nombreux États membres de l'Union ainsi qu'un proche allié dans le domaine de la sécurité; que l'Union et le Royaume-Uni devraient poursuivre cette coopération étroite malgré le retrait du Royaume-Uni de l'Union, car cela sera bénéfique pour les deux parties;

D. considérant que les entreprises européennes ont besoin de clarté et de sécurité juridiques, étant donné que la capacité de transférer des données à caractère personnel par-delà les frontières se révèle de plus en plus importante pour tous les types d'entreprises qui proposent des biens et des services sur la scène internationale; qu'une décision d'adéquation portant sur le Royaume-Uni au titre du RGPD s'avère de la plus haute importance, étant donné que de nombreuses entreprises européennes font des affaires outre-Manche, étant entendu notamment que le Brexit est encore très récent et que les flux de données au sein de l'Union n'ont pas fait l'objet de restrictions; considérant que l'absence d'adoption d'un cadre d'adéquation fiable risquerait d'engendrer des perturbations dans les transferts commerciaux transfrontières, entre l'Union européenne et le Royaume-Uni, de données à caractère personnel, ainsi que des coûts de mise en conformité élevés;

E. considérant que l'accord de commerce et de coopération comporte un certain nombre de garanties et de conditions concernant l'échange de données à caractère personnel pertinentes dans le domaine répressif; que les négociations relatives aux flux de données à caractère personnel ont été menées parallèlement aux négociations sur l'accord de commerce et de coopération, mais n'ont pu être finalisées avant la fin de la période de transition au 31 décembre 2020; qu'une «clause passerelle» a été incluse dans l'accord de commerce et de coopération à titre de solution provisoire, subordonnée à l'engagement du Royaume-Uni de ne pas modifier son régime actuel de protection des données, afin de garantir la continuité des flux de données à caractère personnel entre le Royaume-Uni et l'Union jusqu'à l'adoption d'une décision d'adéquation; que la période initiale de quatre mois a été prolongée et s'achèvera à la fin du mois de juin 2021;

F. considérant que l'évaluation réalisée par la Commission avant de présenter son projet de décision d'exécution n'était pas achevée, ni pleinement conforme aux exigences de la Cour de justice en matière d'évaluation de l'adéquation, ce qui a été mis en exergue par le comité européen de la protection des données dans ses avis sur l'adéquation, dans lesquels il recommande à la Commission d'évaluer plus avant certains aspects spécifiques du droit et de la pratique du Royaume-Uni relatifs à la collecte en masse, la divulgation outre-mer et les accords internationaux dans le domaine de l'échange de renseignements, l'utilisation ultérieure des informations collectées à des fins répressives et l'indépendance des commissaires judiciaires;

G. considérant que certains aspects de la législation ou des pratiques du Royaume-Uni n'ont pas été pris en considération par la Commission, ce qui a donné lieu à des projets de décisions d'exécution qui ne sont pas conformes au droit de l'Union; que l'article 45 du RGPD dispose que, «lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tient compte, en particulier, de […] la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence», et des «engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel», ce qui inclut les accords internationaux dans d'autres domaines impliquant un accès à des données ou le partage d'informations, et nécessite donc une évaluation desdits accords internationaux;

H. considérant que la Cour de justice a clairement indiqué dans son arrêt Schrems I que «lors de l'examen du niveau de protection offert par un pays tiers, la Commission est tenue d'apprécier le contenu des règles applicables dans ce pays résultant de la législation interne ou des engagements internationaux de celui-ci ainsi que la pratique visant à assurer le respect de ces règles, cette institution devant, conformément à l'article 25, paragraphe 2, de la directive 95/46/CE, prendre en compte toutes les circonstances relatives à un transfert de données à caractère personnel vers un pays tiers» (point 75);

I. considérant qu'en ce qui concerne les États membres, les activités des services de renseignement et le partage avec des pays tiers sont exclus du champ d'application du droit de l'Union en vertu des traités, puisque ces activités s'inscrivent dans la nécessaire évaluation de l'adéquation du niveau de protection des données à caractère personnel offert par des pays tiers, ainsi que cela a été confirmé par la Cour de justice dans les arrêts Schrems I et II;

J. considérant que les normes en matière de protection des données reposent non seulement sur la législation en vigueur, mais également sur l'application de ces lois dans la pratique, et que, lors de la préparation de sa décision, la Commission n'a évalué que la législation, mais pas son application réelle dans la pratique;

K. considérant que la Commission reconnaît actuellement que douze pays tiers offrent une protection adéquate au titre du RGPD et qu'elle a récemment achevé les pourparlers avec la République de Corée à ce sujet; que le Royaume-Uni est le premier pays pour lequel la Commission a proposé de reconnaître l'adéquation au titre de la directive en matière de protection des données dans le domaine répressif;

L. considérant que le cas du Royaume-Uni se distingue de toutes les évaluations d'adéquation antérieures dans la mesure où il s'agit d'un ancien État membre de l'Union qui a transposé les dispositions du RGPD dans son droit national et a en outre prévu que toute la «législation nationale dérivée de l'Union», notamment la législation transposant la directive en matière de protection des données dans le domaine répressif, continuera de s'appliquer au terme de la période de transition;

I. **RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES**

Observations générales

1. fait observer que le Royaume-Uni est signataire de la CEDH et de la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel; attend du Royaume-Uni qu'il garantisse le même cadre minimal de protection des données, même s'il a quitté l'Union européenne;

2. se félicite de l'engagement pris par le Royaume-Uni de respecter la démocratie et l'état de droit, ainsi que de protéger et de donner effet, au niveau national, aux droits fondamentaux, tels que ceux énoncés dans la CEDH, et notamment de garantir des niveaux élevés de protection des données; rappelle qu'il s'agit d'une condition préalable nécessaire à la coopération de l'Union avec le Royaume-Uni; rappelle que, bien que l'article 8 de la CEDH sur le droit au respect de la vie privée fasse partie du droit interne britannique en vertu de la loi britannique sur les droits de l'homme de 1998 ainsi que de la *common law* grâce au nouveau délit d'utilisation abusive des informations relatives à la vie privée, le gouvernement a voté contre les efforts visant à instaurer un droit fondamental à la protection des données;

3. insiste sur le fait que l'Union a opté pour une approche de la gouvernance des données centrée sur les droits de l'homme en définissant des règles solides en matière de protection des données dans le contexte du RGPD, et s'inquiète donc vivement des déclarations publiques du Premier ministre britannique, selon qui le Royaume-Uni essaiera de s'écarter des règles de l'Union européenne en matière de protection des données et établira ses propres contrôles «souverains» dans ce domaine; estime que la stratégie nationale du Royaume-Uni de 2020 en matière de données constitue un glissement de la protection des données à caractère personnel vers une utilisation et un partage plus larges des données, ce qui est incompatible avec les principes d'équité, de minimisation des données et de limitation des finalités au titre du RGPD; constate que, dans ses avis sur l'adéquation, le comité européen de la protection des données insiste sur le fait que cela pourrait entraîner des risques éventuels pour la protection conférée aux données à caractère personnel transférées depuis l'Union;

4. souligne que des décisions d'adéquation valables contribuent grandement à la protection des droits fondamentaux des personnes et à la sécurité juridique des entreprises; précise toutefois que les décisions d'adéquation fondées sur des évaluations incomplètes et qui ne s'accompagnent pas d'une mise en œuvre appropriée par la Commission peuvent donner lieu à l'effet inverse lorsqu'elles sont contestées en justice;

5. souligne que l'évaluation réalisée par la Commission avant de présenter son projet de décision d'exécution n'était pas achevée, ni pleinement conforme aux exigences de la Cour de justice en matière d'évaluation de l'adéquation, ce qui a été mis en exergue par le comité européen de la protection des données dans ses avis sur l'adéquation, dans lesquels il recommande à la Commission d'évaluer plus avant certains aspects spécifiques du droit et de la pratique du Royaume-Uni relatifs à la collecte en masse, la divulgation outre-mer et les accords internationaux dans le domaine de l'échange de renseignements, l'utilisation ultérieure des informations collectées à des fins répressives et l'indépendance des commissaires judiciaires;

Application du RGPD

6. exprime son inquiétude quant à l'application lacunaire voire souvent inexistante du RGPD par le Royaume-Uni alors qu'il était encore membre de l'Union; insiste en particulier sur l'application défaillante du règlement par l'autorité britannique de protection des données (ICO, *Information Commissioner's Office*) par le passé; cite pour exemple le fait que l'ICO a classé une plainte portant sur les technologies publicitaires après avoir organisé deux événements avec les parties prenantes, rédigé un rapport [«Update Report on Adtech» (Rapport actualisé sur les technologies publicitaires»)] et déclaré que «l'industrie des technologies publicitaires semble immature dans sa compréhension des exigences de protection des

données», mais n'a exercé aucun de ses pouvoirs d'application ([17]); s'inquiète du fait que cette absence d'application constitue un problème structurel, exposé dans la «Regulatory Action Policy» (Politique en matière de mesures réglementaires) de l'ICO, qui indique explicitement que «dans la majorité des cas, nous réserverons nos pouvoirs pour les cas les plus sérieux, représentant les violations les plus sévères des obligations en matière de droits à l'information. Il s'agit généralement d'actes volontaires, délibérés ou de négligence, ou de violations répétées des obligations en matière de droits à l'information, causant un préjudice ou des dommages aux personnes»; souligne que, dans la pratique, cela signifie qu'un nombre important de violations de la législation sur la protection des données au Royaume-Uni n'ont par conséquent pas été corrigées;

7. prend acte de la stratégie nationale du Royaume-Uni en matière de données, actualisée le 9 décembre 2020, qui suggère de passer de la protection des données à caractère personnel à une utilisation et un partage accrus et plus larges des données; insiste sur le fait que la position décrite dans la stratégie, selon laquelle «conserver les données peut avoir une incidence négative sur la société», n'est pas compatible avec les principes de minimisation des données et de limitation des finalités prévus par le RGPD et le droit primaire;

8. prend acte du fait que la commission des affaires constitutionnelles, en 2004 ([18]), et la commission des affaires publiques du Parlement britannique, en 2014 ([19]), ont recommandé de garantir l'indépendance de l'ICO en lui octroyant le statut d'agent du Parlement qui relève directement de ce dernier plutôt que de continuer à être nommé par le ministre des médias numériques et des sports; regrette que cette recommandation n'ait pas été suivie d'effet;

Traitement de données à des fins de contrôle de l'immigration

9. relève que la législation britannique en matière de protection des données prévoit une dérogation à certains aspects des principes et droits fondamentaux de la protection des données, tels que le droit d'accès et le droit de toute personne concernée de savoir avec qui ses données ont été partagées, dans le cas où une telle protection «nuirait à un contrôle efficace de l'immigration»; souligne que le contrôle et la conformité de l'utilisation de la dérogation doivent être assurés conformément aux normes visées dans les critères de référence pour l'adéquation qui requièrent la prise en considération à la fois de la pratique et du principe, en insistant sur le fait qu'«il convient donc de tenir compte non seulement du contenu des règles applicables aux données personnelles transférées vers un pays tiers […], mais également du système mis en place afin de garantir l'effectivité de ces règles»; prend note du fait que cette dérogation, susceptible d'être utilisée par tous les responsables du traitement des données au Royaume-Uni, a été approuvée par l'ICO et par un tribunal, qu'elle ne peut être invoquée qu'au cas par cas et que son application doit respecter les principes de nécessité et de proportionnalité; rappelle les informations récemment révélées selon lesquelles 17 780 demandes d'accès ont été déposées pour des données traitées par le ministère de l'intérieur entre le 1er avril 2018 et le 31 mars 2019 et concernant 146,75 millions de personnes, et selon lesquelles la dérogation concernant l'immigration a été utilisée dans plus de 70 % des demandes de personnes concernées adressées au ministère de l'intérieur en 2020 ([20]); souligne que, même dans les cas où le ministère de l'intérieur a fait usage de la dérogation, l'accès aux informations n'a pas été totalement refusé, mais a été limité à des documents expurgés;

10. relève que cette dérogation s'applique désormais aux citoyens de l'Union qui résident ou envisagent de résider au Royaume-Uni; exprime sa profonde inquiétude quant au fait que la dérogation prive les personnes concernées de possibilités essentielles en matière d'obligation de rendre compte et de voies de recours, et fait valoir qu'il ne s'agit pas d'un niveau de protection adéquat;

([17]) Lomas, N., *UK's ICO faces legal action after closing adtech complaint with nothing to show for it*, («L'autorité britannique de protection des données risque des poursuites judiciaires pour avoir classé sans justification une plainte relative aux technologies publicitaires»), TechCrunch, San Francisco, 2020.

([18]) Septième rapport de la commission spéciale sur les affaires constitutionnelles, publié par la Chambre des communes le 13 juin 2006. Paragraphe 108: «Nous estimons qu'il serait très utile que le commissaire à l'information soit directement responsable devant le Parlement et financé par ce dernier, et nous recommandons qu'un tel changement soit envisagé lorsque l'occasion se présentera de modifier la législation».

([19]) Rapport de la commission de l'administration publique intitulé «Who's accountable? Relationships between Government and arm's-length bodies» (Qui est responsable? Relations entre le gouvernement et les organismes indépendants), publié par la Chambre des communes le 4 novembre 2014. Paragraphe 64: «Le commissaire à l'information et le Bureau d'inspection des prisons devraient jouir d'une indépendance plus totale vis-à-vis du gouvernement et devraient rendre compte au Parlement. Le commissaire à l'information, le commissaire chargé des nominations publiques et le président du comité des normes de la vie publique devraient devenir des agents du Parlement, comme le sont déjà le médiateur du Parlement et des services de santé de même que le contrôleur et l'auditeur général».

([20]) Communiqué de presse d'Open Rights Group du 3 mars 2021 intitulé «Documents reveal controversial Immigration Exemption used in 70 % of access requests to Home Office» (Des documents révèlent le recours à la dérogation controversée en matière d'immigration dans 70 % des demandes d'accès adressées au ministère de l'intérieur).

11. réitère sa profonde inquiétude quant à l'existence d'une dérogation aux droits des personnes concernées dans la politique du Royaume-Uni en matière d'immigration; rappelle sa position selon laquelle la dérogation pour le traitement des données à caractère personnel à des fins d'immigration prévue par la loi britannique sur la protection des données doit être modifiée avant qu'une décision d'adéquation valable puisse être adoptée, position qu'il a maintes fois exprimée, notamment dans sa résolution du 12 février 2020 sur la proposition de mandat pour la négociation d'un nouveau partenariat avec le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord ([21]) et dans l'avis de la commission des libertés civiles, de la justice et des affaires intérieures du 5 février 2021 ([22]); invite la Commission à demander la suppression de la dérogation concernant l'immigration ou à veiller à ce qu'elle soit réformée de manière à ce que la dérogation et son utilisation offrent des garanties suffisantes aux personnes concernées et ne violent pas les normes attendues d'un pays tiers;

Surveillance de masse

12. rappelle les révélations faites par le lanceur d'alerte Edward Snowden concernant la surveillance de masse exercée par les États-Unis et le Royaume-Uni; rappelle que le programme «Tempora» du Royaume-Uni, géré par le Centre national de communications (GCHQ), intercepte les communications en temps réel à partir des câbles à fibre optique de la dorsale internet et enregistre les données de manière à pouvoir les traiter et les consulter ultérieurement; rappelle que cette surveillance de masse du contenu et des métadonnées des communications a lieu indépendamment du fait qu'il existe des soupçons spécifiques ou des données cibles;

13. rappelle que, dans les arrêts Schrems I et II, la Cour de justice a estimé que l'accès massif au contenu des communications privées touche au contenu essentiel du droit au respect de la vie privée, et qu'en pareils cas, il n'est plus nécessaire de réaliser un test de nécessité et de proportionnalité; souligne que ces principes s'appliquent aux transferts de données vers des pays tiers autres que les États-Unis, dont le Royaume-Uni;

14. rappelle sa résolution du 12 mars 2014, selon laquelle les programmes de surveillance de masse, menés par les services de renseignement du GCHQ sans aucun discernement et sans se baser sur des soupçons, sont incompatibles avec les principes de nécessité et de proportionnalité dans une société démocratique et ne sont pas conformes au droit de l'Union en matière de protection des données à caractère personnel; constate que le Royaume-Uni a depuis lors considérablement réformé sa législation en matière de surveillance et introduit des garanties qui vont au-delà des conditions définies par la Cour de justice de l'Union européenne dans son arrêt Schrems II ([23]) et qui sont plus protectrices que celles prévues dans la législation en matière de surveillance de la plupart des États membres; se félicite en particulier de la disposition prévoyant le plein accès à un recours juridictionnel effectif; rappelle que le rapporteur spécial des Nations unies sur le droit à la vie privée a salué les solides garanties introduites par l'Investigatory Powers Act (loi portant réglementation des pouvoirs d'enquête, IPA) de 2016 en matière de nécessité, de proportionnalité et d'autorisation indépendante par un organe judiciaire;

15. rappelle qu'en septembre 2018, la Cour européenne des droits de l'homme a confirmé que les programmes britanniques d'interception et de conservation massive de données, y compris Tempora, étaient illégaux et incompatibles avec les conditions nécessaires à une société démocratique ([24]);

16. estime qu'il est inacceptable que les projets de décisions d'adéquation ne tiennent pas compte de l'absence de limitations à l'utilisation des pouvoirs du Royaume-Uni en matière de données de masse, ni de l'utilisation réelle des opérations de surveillance britanniques et américaines révélée par Edward Snowden, et notamment des faits suivants:

a) il n'existe aucun contrôle effectif sur le fond par l'ICO ou les tribunaux de l'utilisation de l'exception de la sécurité nationale dans la loi britannique sur la protection des données;

b) les limites à l'utilisation des «pouvoirs en matière de données de masse» du Royaume-Uni ne sont pas énoncées dans la loi elle-même, comme l'exige la Cour de justice (mais sont plutôt laissées à la discrétion de l'exécutif, sous réserve d'un contrôle judiciaire «respectueux»);

([21]) Textes adoptés de cette date, P9_TA(2020)0033.

([22]) Avis de la commission des libertés civiles, de la justice et des affaires intérieures sur la conclusion, au nom de l'Union, de l'accord de commerce et de coopération entre l'Union européenne et la Communauté européenne de l'énergie atomique, d'une part, et le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord, d'autre part, et de l'accord entre l'Union européenne et le Royaume-Uni de Grande- Bretagne et d'Irlande du Nord relatif aux procédures de sécurité pour l'échange d'informations classifiées et leur protection, LIBE_AL(2021)680848.

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

([24]) Arrêt de la Cour européenne des droits de l'homme du 13 septembre 2018 *Big Brother Watch et autres contre Royaume-Uni*, 58170/13, 62322/14, 24960/15.

Vendredi 21 mai 2021

c) la description des «données secondaires» (métadonnées) dans les projets de décisions induit gravement en erreur et ne tient pas compte du fait que ces données peuvent être très révélatrices et intrusives et qu'elles font l'objet d'analyses automatisées sophistiquées (comme l'a constaté la Cour de justice dans l'affaire *Digital Rights Ireland* ([25])); pourtant, en vertu du droit britannique, les métadonnées ne sont pas protégées de manière significative contre tout accès non autorisé, la collecte en masse et l'analyse basée sur l'IA par les agences de renseignement britanniques;

d) les agences «5EYES», en particulier le GCHQ et l'Agence de sécurité nationale (NSA), partagent dans la pratique toutes les données de renseignement;

indique en outre que, s'agissant des États-Unis, les citoyens britanniques bénéficient de certaines garanties informelles entre le GCHQ et la NSA; se dit vivement préoccupé par le fait que ces garanties ne protégeraient pas les citoyens ou résidents de l'Union dont les données pourraient être ultérieurement transférées et partagées avec la NSA;

17. invite les États membres à conclure des accords de non-espionnage avec le Royaume-Uni et invite la Commission à profiter de ses échanges avec ses homologues britanniques pour faire passer le message selon lequel, en l'absence de modification des lois et pratiques de surveillance du Royaume-Uni, la seule option envisageable pour faciliter les décisions d'adéquation consisterait à conclure des accords de «non-espionnage» avec les États membres;

Transferts ultérieurs

18. insiste fortement sur le fait que la loi de 2018 sur l'Union européenne (retrait) [European Union (Withdrawal) Act 2018] prévoit que la jurisprudence de la Cour de justice produite avant la fin de la période de transition sera maintenue dans le droit interne et donc juridiquement contraignante pour le Royaume-Uni; souligne que le Royaume-Uni est lié par les principes et les conditions définis dans les arrêts Schrems I et Schrems II de la Cour de justice lorsqu'il évalue l'adéquation d'autres pays tiers; est préoccupé par le fait que les tribunaux britanniques n'appliqueront toutefois plus la charte; met l'accent sur le fait que le Royaume-Uni n'est plus sous la juridiction de la Cour de justice, qui est la plus haute instance en mesure d'interpréter la charte;

19. insiste sur le fait que les règles britanniques en matière de partage des données à caractère personnel au titre de la loi sur l'économie numérique de 2017 (*Digital Economy Act 2017*) et concernant les transferts ultérieurs de données de recherche ne sont clairement pas «substantiellement équivalentes» aux règles énoncées dans le RGPD, telles qu'interprétées par la Cour de justice;

20. est préoccupé par le fait que le Royaume-Uni s'est octroyé le droit de déclarer que d'autres pays ou territoires tiers offrent un niveau de protection adéquat des données, sans tenir compte du fait que l'Union ait ou non considéré que le pays ou territoire tiers concerné offrait une telle protection; rappelle que le Royaume-Uni a déjà déclaré que Gibraltar offrait un tel niveau de protection alors que l'Union ne l'a pas fait; exprime sa vive préoccupation quant au fait qu'un statut d'adéquation du Royaume-Uni ne manquerait pas d'entraîner un contournement des règles de l'Union relatives aux transferts vers des pays ou territoires qui ne sont pas réputés adéquats au regard du droit de l'Union;

21. prend acte du fait que, le 1er février 2021, le Royaume-Uni a envoyé une demande d'adhésion à l'accord de partenariat transpacifique global et progressiste (PTPGP), notamment pour «bénéficier de règles modernes en matière de commerce numérique qui permettent la libre circulation des données entre les membres, lèvent les obstacles inutiles pour les entreprises […]»; constate avec inquiétude que le PTPGP compte onze membres, dont huit ne font pas l'objet d'une décision d'adéquation de la part de l'Union; est vivement préoccupé par les éventuels transferts ultérieurs de données à caractère personnel de citoyens et de résidents de l'Union vers ces pays si une décision d'adéquation est prise au sujet du Royaume-Uni ([26]);

([25]) Arrêt de la Cour de justice du 8 avril 2014, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e. a. et Kärntner Landesregierung e.a.*, affaires C-293/12 et C-594/12, ECLI:EU:C:2014:238.

([26]) Communiqué de presse du ministère britannique du commerce international du 30 janvier 2021 intitulé «UK applies to join huge Pacific free trade area CPTPP» [Le Royaume-Uni demande à rejoindre l'immense zone de libre-échange du Pacifique (PTPGP)].

22. regrette que la Commission n'ait pas évalué l'incidence et les risques potentiels de l'accord de partenariat économique global entre le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et le Japon, qui inclut des dispositions sur les données à caractère personnel et sur le niveau de protection des données;

23. craint que le niveau de protection offert par le RGPD ne soit compromis si le Royaume-Uni inclut des dispositions sur les transferts de données dans tout accord commercial futur, notamment dans les accords commerciaux entre les États-Unis et le Royaume-Uni;

II. **DIRECTIVE EN MATIÈRE DE PROTECTION DES DONNÉES DANS LE DOMAINE RÉPRESSIF**

24. insiste sur le fait que le Royaume-Uni est le premier pays pour lequel la Commission a proposé d'adopter une décision d'adéquation au titre de la directive (UE) 2016/680;

25. prend acte de l'accord sur l'accès transfrontière aux données conclu entre le Royaume-Uni et les États-Unis ([27]) dans le cadre de la loi américaine sur l'informatique en nuage (*CLOUD Act*), qui facilite les transferts à des fins répressives; s'inquiète vivement du fait que cet accord permettra aux autorités américaines d'accéder indûment aux données à caractère personnel des citoyens et résidents de l'Union; partage les préoccupations du comité européen de la protection des données quant au fait que les garanties prévues dans le contexte de l'accord-cadre UE-États-Unis ([28]), appliquées *mutatis mutandis*, pourraient ne pas répondre aux critères de règles claires, précises et accessibles en matière d'accès aux données à caractère personnel ou consacrer suffisamment ces garanties pour qu'elles soient effectives et exploitables au titre du droit britannique;

26. rappelle que l'arrêt rendu par la Cour de justice dans l'affaire C-623/1 doit être interprété en ce sens qu'il s'oppose à une législation nationale permettant à une autorité étatique d'exiger des fournisseurs de services de communications électroniques qu'ils assurent la transmission généralisée et indifférenciée des données relatives au trafic et à la localisation aux services de sécurité et de renseignement de l'État en vue de la sauvegarde de la sécurité nationale;

27. relève que, dans ce cas, la Cour de justice a jugé que la collecte de données en masse effectuée au Royaume-Uni au titre de la loi de 2000 régissant les pouvoirs d'enquête (*Regulation of Investigatory Powers Act 2000*) était illégale; souligne que le règlement a depuis été remplacé par la loi portant réglementation des pouvoirs d'enquête (*Investigatory Powers Act* — IPA 2016) afin de renforcer les principes de nécessité et de proportionnalité; insiste sur le fait que l'IPA 2016 subordonne l'interception à un contrôle judiciaire et autorise les personnes à accéder à leurs données et à introduire des plaintes devant le tribunal du Royaume-Uni chargé des pouvoirs d'enquête; déplore toutefois que l'IPA 2016 continue d'autoriser la pratique de la conservation de données en masse;

28. s'inquiète des informations récentes selon lesquelles le ministère de l'intérieur britannique a mis en place, dans le cadre d'une expérience entreprise au titre de l'IPA 2016, un système de collecte et de conservation massives de données;

29. rappelle que, dans sa résolution du 12 février 2020, le Parlement européen souligne que «le Royaume-Uni ne peut pas disposer d'un accès direct aux données des systèmes d'information de l'Union ou participer aux structures de gestion des agences de l'Union dans le domaine de la liberté, de la sécurité et de la justice et que tout partage d'informations comportant des données à caractère personnel avec le Royaume-Uni doit être soumis à des règles strictes de garantie, de contrôle et de surveillance, notamment un niveau de protection des données à caractère personnel équivalent à celui que prévoit le droit de l'Union»; prend acte des lacunes constatées dans la manière dont le Royaume-Uni a mis en œuvre la législation sur la protection des données alors qu'il était encore membre de l'Union; rappelle que le Royaume-Uni enregistrait et conservait une copie du système d'information Schengen (SIS); espère que les services répressifs britanniques respecteront pleinement les règles applicables lorsqu'ils échangeront des données à caractère personnel à l'avenir; rappelle que le Royaume-Uni conserve un accès à certaines bases de données des services répressifs de l'Union, uniquement sur la base d'un système de «concordance/non-concordance» et qu'il lui est juridiquement proscrit d'accéder au SIS;

([27]) Accord entre le gouvernement du Royaume-Uni de Grande-Bretagne et d'Irlande du Nord et le gouvernement des États-Unis d'Amérique du 3 octobre 2019 sur l'accès aux données électroniques aux fins de la lutte contre la grande criminalité.

([28]) Accord entre les États-Unis d'Amérique et l'Union européenne sur la protection des informations à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière (JO L 336 du 10.12.2016, p. 3).

30. fait part de son inquiétude quant à la révélation, en janvier 2021, du fait que 400 000 casiers judiciaires avaient été accidentellement effacés de l'ordinateur national de la police britannique; souligne que cela n'inspire pas la confiance dans les efforts déployés par le Royaume-Uni pour garantir la protection des données utilisées à des fins répressives;

31. constate que le projet de décision d'adéquation examine de manière approfondie les droits de chaque autorité britannique habilitée par le droit national à intercepter et à conserver des données à caractère personnel à des fins de sécurité nationale; se félicite en outre que les rapports de contrôle détaillés portant sur les autorités de la communauté du renseignement fournissent des informations sur les pratiques actuelles du Royaume-Uni en matière de surveillance; invite la Commission à poursuivre l'évaluation et le suivi des types de données de communication qui relèvent des pouvoirs britanniques en matière de conservation des données et d'interception légale;

32. souligne que l'accord de commerce et de coopération UE-Royaume-Uni comprend des titres concernant l'échange de données ADN, dactyloscopiques et relatives à l'immatriculation des véhicules, le transfert et le traitement des données des dossiers passagers (données PNR), la coopération quant aux informations opérationnelles, la coopération avec Europol et Eurojust, qui s'appliqueront indépendamment de la décision d'adéquation; rappelle toutefois les préoccupations exprimées dans l'avis de la commission des libertés civiles, de la justice et des affaires intérieures de février 2021 sur l'accord précité en ce qui concerne l'utilisation spéciale et la durée de conservation plus longue des données à caractère personnel accordées au Royaume-Uni sous les titres Prüm et PNR de l'accord, qui ne sont pas conformes aux utilisations et aux durées de conservation pratiquées par les États membres; rappelle le droit de saisir la Cour de justice afin de faire vérifier la légalité de l'accord international proposé et, plus particulièrement, sa compatibilité avec la protection d'un droit fondamental ([29]);

Conclusions

33. invite la Commission à garantir aux entreprises de l'Union que la décision d'adéquation fournira une base juridique solide, suffisante et tournée vers l'avenir pour les transferts de données; souligne qu'il importe de veiller à ce que cette décision d'adéquation soit jugée acceptable en cas d'examen par la Cour de justice de l'Union européenne et souligne que toutes les recommandations formulées dans l'avis du comité européen de la protection des données devraient donc être prises en compte;

34. se félicite que les décisions d'adéquation ne soient applicables que pendant quatre ans, puisque le Royaume-Uni, n'étant plus un État membre de l'Union, pourrait choisir de modifier la législation soumise à l'évaluation d'adéquation de la Commission; demande à la Commission de continuer entre-temps à surveiller le niveau de protection des données au Royaume-Uni en droit et dans la pratique, et de procéder à une évaluation approfondie avant de renouveler la décision d'adéquation en 2025;

35. estime qu'en adoptant les deux décisions d'exécution, qui ne sont pas conformes au droit de l'Union, sans avoir répondu à toutes les préoccupations exprimées dans la présente résolution, la Commission outrepasse les compétences d'exécution qui lui sont conférées par le règlement (UE) 2016/679 et la directive (UE) 2016/680; s'oppose par conséquent aux deux actes d'exécution dans la mesure où les projets de décisions d'exécution ne sont pas conformes au droit de l'Union;

36. invite la Commission à modifier les deux projets de décisions d'exécution afin de les rendre pleinement conformes au droit de l'Union et à sa jurisprudence;

37. demande aux autorités nationales chargées de la protection des données de suspendre le transfert de données à caractère personnel qui pourraient faire l'objet d'un accès indifférencié par les services de renseignement britanniques si la Commission devait adopter ses décisions d'adéquation à l'égard du Royaume-Uni avant que ce dernier ne résolve les problèmes mentionnés ci-dessus;

38. invite la Commission et les autorités compétentes du Royaume-Uni à mettre en place un plan d'action afin de remédier dans les meilleurs délais aux lacunes recensées dans les avis du comité européen de la protection des données ainsi qu'aux autres questions en suspens relatives à la protection des données par le Royaume-Uni, éléments qui doivent constituer une condition préalable à la décision d'adéquation finale;

39. demande à la Commission de continuer à surveiller de près le niveau de protection des données ainsi que les lois et pratiques en matière de surveillance de masse au Royaume-Uni; fait remarquer que le chapitre V du RGPD prévoit d'autres possibilités juridiques pour les transferts de données à caractère personnel vers le Royaume-Uni; rappelle que, en vertu des orientations du comité européen de la protection des données, les transferts fondés sur des dérogations pour des situations particulières en vertu de l'article 49 du RGPD doivent être exceptionnels;

([29]) Résolution du Parlement européen sur le projet de décision de la Commission constatant le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis (JO C 103 E du 29.4.2004, p. 665).

40. regrette que la Commission ait ignoré les appels du Parlement à suspendre le bouclier de protection des données jusqu'à ce que les autorités américaines se conforment à ses termes, et qu'elle ait toujours préféré «suivre la situation» sans aucun résultat concret en matière de protection des données pour les personnes ni de sécurité juridique pour les entreprises; exhorte la Commission à tirer les leçons de ses échecs passés, lorsqu'elle a ignoré les appels du Parlement et des experts concernant la conclusion et le suivi des décisions d'adéquation antérieures, et à ne pas laisser à la Cour de justice le soin de faire appliquer correctement la législation européenne sur la protection des données à la suite de plaintes déposées par des citoyens;

41. invite la Commission à suivre de près la législation et les pratiques en matière de protection des données au Royaume-Uni, à informer immédiatement et à consulter le Parlement à propos de toute modification future du régime de protection des données du Royaume-Uni et à prévoir un rôle de contrôle pour le Parlement dans le nouveau cadre institutionnel, y compris pour les organes compétents tels que le comité spécialisé chargé de la coopération des services répressifs et judiciaires;

o

o o

42. charge son Président de transmettre la présente résolution à la Commission et aux États membres, ainsi qu'au gouvernement du Royaume-Uni.