N° 65

SÉNAT

SESSION ORDINAIRE DE 2020-2021

Enregistré à la Présidence du Sénat le 21 octobre 2020

PROPOSITION DE RÉSOLUTION EUROPÉENNE

EN APPLICATION DE L'ARTICLE 73 *QUINQUIES* DU RÈGLEMENT,

pour une **localisation européenne** *des* **données personnelles**,

PRÉSENTÉE

Par Mme Catherine MORIN-DESAILLY, MM. Jean-Michel ARNAUD, Serge BABARY, Jérôme BASCHER, Arnaud BAZIN, Bruno BELIN, Mmes Martine BERTHET, Annick BILLON, Christine BONFANTI-DOSSAT, MM. Bernard BONNE, François BONNEAU, Philippe BONNECARRÈRE, Gilbert BOUCHET, Max BRISSON, Olivier CADIC, François CALVET, Mme Agnès CANAYER, MM. Patrick CHAIZE, Pierre CHARON, Patrick CHAUVET, Mme Marta de CIDRAC, MM. Olivier CIGOLOTTI, Philippe DALLIER, Mme Laure DARCOS, MM. Dominique de LEGGE, Bernard DELCROS, Mme Catherine DEROCHE, M. Yves DÉTRAIGNE, Mmes Élisabeth DOINEAU, Sabine DREXLER, M. Alain DUFFOURG, Mmes Catherine DUMAS, Françoise DUMONT, Françoise FÉRAT, MM. Philippe FOLLIOT, Bernard FOURNIER, Mmes Joëlle GARRIAUD-MAYLAM, Françoise GATEL, Frédérique GERBAUD, Pascale GRUNY, Jocelyne GUIDEZ, MM. Olivier HENNO, Loïc HERVÉ, Alain HOUPERT, Jean-Raymond HUGONET, Mme Else JOSEPH, MM. Claude KERN, Laurent LAFON, Michel LAUGIER, Daniel LAURENT, Antoine LEFÈVRE, Pierre-Antoine LEVI, Mme Anne-Catherine LOISIER, M. Pierre LOUAULT, Mme Marie MERCIER, MM. Sébastien MEURANT, Alain MILON, Jean-Marie MIZZON, Louis-Jean de NICOLAŸ, Cyril PELLEVAT, Cédric PERRIN, Robert del PICCHIA, Stéphane PIEDNOIR, Rémy POINTEREAU, Mmes Sonia de LA PROVÔTÉ, Isabelle RAIMOND-PAVERO, MM. Damien REGNARD, Bruno RETAILLEAU, Mme Marie-Pierre RICHER, M. Olivier RIETMANN, Mme Denise SAINT-PÉ, MM. Hugues SAURY, René-Paul SAVARY, Michel SAVIN, Jean-Marie VANLERENBERGHE et Mme Dominique VÉRIEN,

Sénateurs

(Envoyée à la commission des affaires européennes.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

Le 16 juillet 2020, la Cour de justice de l'Union européenne (CJUE) a rendu un arrêt historique invalidant le régime de transfert de données entre l'Union européenne (UE) et les États-Unis, appelé bouclier de protection des données ou *privacy shield*, au motif qu'il rendait « *possibles des ingérences dans les droits fondamentaux des personnes dont les données sont transférées vers ce pays tiers* ». Le caractère disproportionné des programmes de surveillance sur les données permis par la loi américaine sur l'informatique en nuage ou *cloud act* a convaincu la CJUE de déclarer cette pratique illégale au regard du règlement général sur la protection des données (RGPD) et de la Charte fondamentaux des droits de l'Union européenne.

Pour autant, la Commission européenne dispose toujours du pouvoir de désigner des pays extra-européens comme disposant d'un niveau adéquat de protection des données à caractère personnel. Cette diplomatie numérique de l'Union, qui concerne actuellement 13 pays[1], et le dispositif de clauses contractuelles types pour le transfert de données personnelles vers des sous-traitants situés en dehors de l'espace économique européen (EEE) sont de nature à porter atteinte aux intérêts stratégiques des États membres en les soumettant à des législations étrangères.

En effet, les affaires Snowden et Cambridge Analytica ont démontré que les données personnelles revêtent un enjeu stratégique en matière de politique industrielle, de libertés individuelles et collectives ou encore de démocratie. L'avènement des objets connectés – dont on estime qu'ils seront 50 milliards dans le monde en 2030[2] – et les mutations technologiques liées à l'intelligence artificielle dans des domaines sensibles tels que la santé, la maitrise de l'énergie, la sécurité ou encore les transports posent dès à présent des questions de

1 En réaction à la décision de la Cour du 16 juillet 2020, la Commission européenne a déclaré se préparer à réévaluer les décisions d'adéquation couvrant les pays suivants : Andorre, Argentine, Canada, l'Ile de Man, Guernesey, Israël, Iles Féroé, Jersey, Nouvelle-Zélande, Suisse et Uruguay.

[2] Strategy Analytics, « Global Connected and IoT Device Forecast Update » (2019)

souveraineté sur la masse considérable de données, 175 zettaoctects[3], qui devrait être produite en 2025.

Face à ce constat, les États membres de l'UE se sont dotés du RGPD, lequel a posé les premières bases d'une souveraineté européenne sur les données. Si l'Europe a su montrer la voie dès 2016 en imposant ce cadre réglementaire ambitieux, nous assistons encore aujourd'hui au dévoiement, par certains États membres, des données collectées sur leur territoire. En témoignent les contrats conclus entre la Direction générale de la sécurité intérieure et Palantir, société historiquement liée à l'Agence centrale du renseignement (CIA) et à l'Agence nationale de la sécurité (NSA). Plus récemment, le ministère de l'Éducation nationale, qui a pourtant créé un comité d'éthique pour les données de l'éducation et lancé des états généraux du numérique pour l'éducation, a contracté avec Microsoft, de même que le ministère des Solidarités et de la santé pour l'hébergement des données de santé collectées par le Health Data Hub.

Ces choix sont autant de renoncements à la préservation de nos intérêts vitaux. Ils confirment que nos gouvernements, chantres de l'autorégulation des plateformes, cultivent une forme de complaisance vis-à-vis des géants du numérique extra-européens, plaçant nos démocraties libérales entre le modèle du capitalisme de surveillance à l'américaine[4] et celui du crédit social chinois. Leur justification ne tient qu'au fait que les pays européens pâtissent d'un déficit d'offre en matière d'infrastructures et technologies de données, résultat d'une politique industrielle et de règles de concurrence inadaptées à l'ère numérique.

En effet, les règles européennes en matière de marchés publics, de concurrence, ou encore d'aides d'État n'ont pas permis d'aider à développer des champions européens, d'où l'impérieuse nécessité d'imposer la localisation et le traitement par des entités européennes des données issues des citoyens et des entreprises européennes.

Prenant la mesure de l'enjeu, la Commission européenne a présenté son agenda numérique avec la parution d'un recueil réglementaire pour l'informatique en nuage, un cadre législatif pour la gouvernance des données, une loi sur les données de grande valeur et la conclusion de protocoles d'accord avec les États membres afin d'aboutir à une fédération en nuage sur le modèle de l'initiative Gaia-X développée par la France et l'Allemagne.

Cette proposition de résolution européenne appelle à aller plus loin, c'est-à-dire à imposer la localisation européenne des données pour assurer la protection

[3] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 février 2020 : « Une stratégie européenne pour les données » (COM(2020) 66)

[4] Shoshana Zuboff, *L'âge du capitalisme de surveillance : le combat pour un avenir humain face aux nouvelles frontières du pouvoir*, Broché (2020)

des données à caractère personnel des Européens en interdisant le recours à des responsables de traitement et/ou sous-traitant soumis à une législation extra-européenne ou disposant d'un siège social en dehors de l'EEE.

Proposition de résolution européenne pour une localisation européenne des données personnelles

① Le Sénat,

② Vu l'article 88-4 de la Constitution,

③ Vu les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, 2000/C 364/01,

④ Vu la décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique, C(2000) 2441,

⑤ Vu le règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données,

⑥ Vu la décision 2010/87 de la Commission 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, C(2010) 593,

⑦ Vu les articles 45 et 46 du 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,

⑧ 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, et abrogeant la décision-cadre 2008/977/JAI du Conseil,

⑨ Vu l'arrêt C-311/18 de la Cour de justice de l'Union européenne du 16 juillet 2020,

⑩ Vu la communication de la Commission au Parlement européen et au Conseil du 24 janvier 2018 : « Une meilleure protection et de nouvelles perspectives – Orientations de la Commission relatives à l'application directe du règlement général sur la protection des données à partir du 25 mai 2018 », COM(2018) 043 final,

⑪ Vu la communication de la Commission au Parlement européen et au Conseil du 24 juillet 2019 : « Les règles en matière de protection des données comme instrument pour créer un climat de confiance dans l'UE et au-delà – bilan », COM(2019) 374 final,

⑫ Vu la communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions du 19 février 2020 : « Une stratégie européenne pour les données », COM(2020) 66 final,

⑬ Vu la communication de la Commission au Parlement européen et au Conseil du 24 juin 2020 : « Marche à suivre en ce qui concerne la mise en conformité de l'acquis de l'ancien troisième pilier avec les règles en matière de protection des données », COM(2020) 262 final,

⑭ Vu la communication de la Commission au Parlement européen et au Conseil du 24 juin 2020 : « 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) 264 final,

⑮ Considérant que les données personnelles revêtent un enjeu de stratégie industrielle dans des domaines sensibles tels que la santé, la maitrise de l'énergie ou encore les transports et de plus que ces données, lorsqu'elles sont liées aux opinions politiques ou religieuses, constituent un élément de souveraineté des États européens en ce que leur traitement peut aussi influer sur le débat démocratique comme l'a montré l'affaire Cambridge Analytica ;

⑯ Considérant que les gouvernements européens, à l'aune de l'affaire Cambridge Analytica et des différents contrats conclus en France entre la Direction générale de la sécurité intérieure et Palantir et entre les ministères des Solidarités et de la santé et de l'Éducation nationale et Microsoft, n'ont pas pris la mesure des dangers relatifs au traitement des données personnelles par des sociétés d'origine extra-européenne ;

⑰ Considérant que le déficit d'offre en matière d'infrastructures et de technologies de données place les États européens dans une position de dépendance vis-à-vis des modèles américain du capitalisme de surveillance et chinois du crédit social ;

⑱ Considérant, de ce fait, indispensable la conclusion de protocoles d'accord entre la Commission européenne et les États membres afin d'aboutir à une fédération en nuage sur le modèle de l'initiative franco-allemande Gaia-X ;

⑲ Considérant que seul un espace européen des données sera à même de garantir la sécurité des 175 zettaoctets de données qui circuleront en 2025 et des données générées par les 50 milliards d'objets connectés qui seront en service en 2030 dans le monde ;

⑳ Considérant que la diplomatie numérique de l'Union, laquelle a conduit à identifier 13 pays extra-européens comme disposant d'un niveau adéquat de protection des données à caractère personnel, et les clauses contractuelles types pour le transfert de données personnelles vers des sous-traitants situés en dehors de l'espace économique européen portent atteinte aux intérêts stratégiques des États européens en les soumettant notamment à la loi américaine sur l'informatique en nuage ;

㉑ Invite l'Union à imposer le traitement des données personnelles et des données industrielles par des entreprises européennes et à imposer la localisation européenne de ces données ;

㉒ Demande, par conséquent, en amont de la parution par l'Union d'un recueil réglementaire pour l'informatique en nuage, à prohiber le recours à des responsables de traitement et/ou sous-traitants soumis à une législation extra-européenne ;

㉓ Demande, alors que l'Union doit présenter son cadre législatif pour la gouvernance des données ainsi qu'une loi sur les données de grande valeur, à prohiber le recours à des responsables de traitement et/ou sous-traitants disposant d'un siège social en dehors de l'espace économique européen.