N° 3740

———

ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

QUATORZIÈME LÉGISLATURE

Enregistré à la Présidence de l'Assemblée nationale le 11 mai 2016.

RAPPORT D'INFORMATION

DÉPOSÉ

PAR LA COMMISSION DES AFFAIRES EUROPÉENNES (1)

sur l'**accord** de **protection** des **données personnelles « Bouclier de protection »** entre les **États-Unis d'Amérique** et **l'Union européenne**,

ET PRÉSENTÉ

PAR M^ME Marietta KARAMANLI et M. CHARLES DE LA VERPILLIÈRE
Députés

———

(1) La composition de la commission figure au verso de la présente page.

La Commission des affaires européennes est composée de : M^me^ Danielle AUROI, *présidente* ; M. Christophe CARESCHE, M^me^ Marietta KARAMANLI, MM. Jérôme LAMBERT, Pierre LEQUILLER, *vice-présidents* ; M. Philip CORDERY, Mme Sandrine DOUCET, MM. Arnaud LEROY, André SCHNEIDER, *secrétaires ;* MM. Ibrahim ABOUBACAR, Kader ARIF, Philippe BIES, Jean-Luc BLEUNVEN, Alain BOCQUET, Jean-Jacques BRIDEY, M^mes^ Isabelle BRUNEAU, Nathalie CHABANNE, MM. Jacques CRESTA, M^me^ Seybah DAGOMA, MM. Yves DANIEL, Bernard DEFLESSELLES, William DUMAS, M^me^ Marie-Louise FORT, MM. Yves FROMION, Hervé GAYMARD, Jean-Patrick GILLE, M^me^ Chantal GUITTET, MM. Razzy HAMMADI, Michel HERBILLON, Laurent KALINOWSKI, Marc LAFFINEUR, Charles de LA VERPILLIÈRE, Christophe LÉONARD, Jean LEONETTI, M^me^ Audrey LINKENHELD, MM. Lionnel LUCA, Philippe Armand MARTIN, Jean-Claude MIGNON, Jacques MYARD, Rémi PAUVROS, Michel PIRON, Joaquim PUEYO, Didier QUENTIN, Arnaud RICHARD, M^me^ Sophie ROHFRITSCH, MM. Jean-Louis ROUMEGAS, Rudy SALLES, Gilles SAVARY.

SOMMAIRE

___

Pages

INTRODUCTION

Mesdames, Messieurs,

Le développement sans précédent des échanges de données – que l'on doit aux nouvelles pratiques de consommation et de communication permises et accompagnées par la diffusion rapide de technologies supports et de terminaux personnels – emporte avec lui des enjeux majeurs, tant pour l'économie que pour les droits fondamentaux. Trop souvent, la dimension éminemment politique du sujet est peu perçue, notamment en raison de son caractère très technique. Il est pourtant essentiel de nous en saisir, et vos rapporteurs souhaitent insister sur l'importance majeure, dès aujourd'hui et pour le futur, du sort que nous voulons donner à la protection des données européennes au-delà de nos frontières. La position de l'Union européenne doit pour cette raison être sans équivoque et prôner une défense sourcilleuse de nos libertés.

Avec le cadre instauré par la directive de 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, l'Union européenne s'est placée à la pointe de la défense des nouveaux droits numériques, en offrant un espace intégré de protection inégalé dans le monde. La réforme récemment adoptée de ce cadre, composée d'un règlement et d'une directive, va plus loin en consacrant de nouveaux droits offerts aux citoyens européens, comme la portabilité des données ou le droit à « l'oubli numérique ».

Néanmoins, dans un domaine aussi dématérialisé et mondialisé que celui des données personnelles, l'Union européenne est dans l'obligation de nouer des partenariats poussés si nous voulons que les droits consacrés ici pour les citoyens européens ne soient pas ailleurs bafoués.

C'est le sens des décisions d'adéquation prévues par l'article 25 de la directive de 1995 : ces décisions, prises par la Commission au terme d'un processus engageant l'avis des autorités de protection des données nationales et celui des États membres, permettent le transfert de données vers d'autres pays à condition que ceux-ci assurent une protection essentiellement équivalente à celle offerte au sein de l'Union.

Depuis 2000, une telle décision régissait ainsi le transfert des données depuis l'Europe vers les États-Unis sous le nom de « *Safe Harbor* ». Cette sphère de sécurité, censée garantir le respect de la vie privée des citoyens européens, a

pourtant été rapidement critiquée, avant de susciter une franche méfiance dès lors que l'affaire PRISM avait mis en lumière les pratiques de surveillance massive exercées par les États-Unis sur des données américaines et étrangères.

Après avoir émis une série de treize recommandations, la Commission est donc entrée en 2013 dans un processus de renégociation de l'accord fondant la décision d'adéquation. Vos rapporteurs avaient réalisé un déplacement à Washington en avril 2015, et pu constater que la renégociation de l'accord « *Safe Harbor* » était très active entre les différentes parties prenantes. Le « *Judicial Redress Act* », qui permet aux Européens de bénéficier de certains droits de recours devant les tribunaux américains, faisait déjà l'objet de discussions au Congrès et apparaissait comme le signe manifeste de la bonne volonté américaine envers son partenaire européen.

Avec l'invalidation de la décision d'adéquation par la Cour de justice de l'Union européenne le 6 octobre 2015, l'insécurité juridique créée a provoqué une accélération des discussions : le 6 février 2016, la Commission présentait les bases d'un nouvel accord entre les États-Unis et l'Union européenne.

A la veille de l'adoption d'un accord encore largement perfectible, il a paru essentiel à vos rapporteurs que l'Assemblée se prononce sur le texte proposé aux États-membres. D'importantes préoccupations demeurent quant à l'architecture globale de l'accord, trop complexe, et à certains points clés, comme la durée de la rétention possible des données, l'accès par les autorités publiques aux données transférées dans le cadre de l'accord « *Privacy Shield* » ou la possibilité d'un recours effectif pour les Européens. Un accord solide et pérenne nécessite en outre la souplesse nécessaire à l'intégration à l'avenir des plus récentes avancées européennes en matière de protection des données.

Les données européennes sont une ressource dont l'importance économique ne devrait cesser de croître : l'Union doit avoir conscience de cette richesse pour exiger des conditions de transfert, d'usage et de traitement à la hauteur des droits fondamentaux consacrés dans son espace propre.

I. LA PROTECTION DES DONNÉES PERSONNELLES SOUS LE RÉGIME DU SAFE HARBOR

A. UN RÉGIME DEVANT ASSURER UNE PROTECTION ÉQUIVALENTE A CELLE DE L'UNION EUROPÉENNE

1. Le développement des échanges de données appelait un cadre juridique pour protéger les droits des utilisateurs

a. L'explosion du volume des données en ligne ces vingt dernières années

Depuis 2000, un accord entre l'Union européenne et les États-Unis encadrait la transmission et l'usage des données personnelles par les entreprises qui exercent leur activité dans un cadre transatlantique, le *Safe Harbor* (« Sphère de sécurité »). La mise en place d'un cadre juridique adapté était devenue nécessaire face au développement exponentiel des données échangées sur le réseau internet, ce développement rapide des flux de données ne faisant que suivre celui des données elles-mêmes, dans une forme d'hyperinflation explicitée par Kenneth Cukier et Viktor Mayer-Schönberger [(1)] : *« En 2000, un quart seulement des informations consignées dans le monde existaient au format numérique. Papier, film et support analogique se partageaient tout le reste. Du fait de l'explosion des fichiers — leur volume double tous les trois ans —, la situation s'est renversée dans des proportions inouïes. En 2013, le numérique représente plus de 98 % du total. »* Le règne de ce qu'il est convenu d'appeler les « big data », ou « données de masse », est advenu à mesure que les moyens technologiques de produire des données, qu'il s'agisse de texte ou d'image, se diffusaient plus largement à chaque individu.

Comme le relève l'étude annuelle du Conseil d'État de 2014 [(2)], les données personnelles tendent aujourd'hui à se multiplier et à se diversifier. À côté des données institutionnelles collectées par les administrations publiques, les entreprises ou les associations, on peut identifier trois autres sources plus récentes de données.

Il y a d'abord les données mises en ligne par les individus sur les réseaux sociaux (à propos d'eux-mêmes, de leurs identités et de leurs goûts), puis les données communiquées sur des tierces personnes (par exemple la photo où l'on identifie un ami), et enfin les données recueillies automatiquement (cookies sur l'ordinateur enregistrant les préférences de navigation, géolocalisation « passive » des terminaux mobiles en sont deux exemples). Ces données sont également très hétérogènes dans leurs formes et leurs contenus.

---

(1) « Mise en données du monde, le déluge numérique », Le Monde diplomatique, juillet 2013.

(2) « Le numérique et les droits fondamentaux », Conseil d'Etat, 2014.

Aujourd'hui, chacun est producteur au quotidien d'une quantité insoupçonnée de données : de la photo mise en ligne à l'avis déposé sur un site de réservation de vacances, des coordonnées géographiques enregistrées par un système de géolocalisation aux données fiscales ou médicales recueillies par les pouvoirs publics, nous concourrons individuellement à ce que les mêmes auteurs qualifient de « mise en données du monde » (« *datafication* »), conduisant à un ensemble d'usages économiques permis par une mémoire informatique de moins en moins couteuse et par des dispositifs techniques dont l'accès se démocratise également de façon rapide. Désormais, ce sont 58% des Français du panel du baromètre du numérique 2015 qui sont équipés d'un smartphone et 35% d'une tablette - contre respectivement 46% et 29% en 2014 (1). Les enjeux économiques qui en écoulent commencent tout juste à être bien compris.

b. Une manne de données à la source d'une activité économique en pleine expansion

La variété des usages permise par cette avalanche de données (notamment en termes de publicité ciblée : « contextuelle », « personnalisée », ou « comportementale ») et la création de nouvelles activités reposant sur des pratiques de consommation, de sociabilité et de culture innovantes se traduisent dans les faits par des enjeux économiques significatifs. S'il est très difficile d'évaluer la valeur des données dans un paysage numérique en constante mutation, le *Boston Consulting Group* avançait en 2011 le chiffre d'une valeur de 315 milliards d'euros pour les données des Européens, chiffre qui, toujours selon *BCG*, pourrait atteindre 1000 milliards d'euros par an en 2020 (2). En offrant un ordre de grandeur des montants engagés, ces chiffres mettent en lumière le poids qu'une protection poussée des données personnelles peut représenter pour les géants du secteur numérique. Ils illustrent également la nécessité d'un solide cadre juridique pour protéger des données personnelles lucratives et très convoitées.

Les données sont devenues une véritable monnaie d'échange dans l'économie numérique, à tel point que certaines entreprises s'étant spécialisées dans le recueil et le traitement des données personnelles (les « *databrokers* », ou courtiers en données) peuvent prétendre, comme c'est le cas de la société américaine *Acxiom,* posséder des informations sur 700 millions de personnes dans le monde. À côté de ces activités de recueil et d'agrégation des données croissent logiquement des offres de services de plus en plus personnalisées qui se nourrissent des recoupements rendus possibles par le volume des données collectées sur les individus.

---

(1) Source : Baromètre du numérique 2015, CREDOC, rapport en ligne : http://www.arcep.fr/uploads/tx_gspublication/CREDOC-Rapport-enquete-diffusion-TIC-France_CGE-ARCEP_nov2015.pdf

(2) Boston Consulting Group, The value of Our Digital Identity, novembre 2012.

2. La directive de 1995 encadre de manière innovante la protection des données à caractère personnel au sein de l'Union européenne

Lorsque la directive n°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 est adoptée, l'Union européenne se place en position de pointe pour la constitution d'un espace intégré de protection des droits fondamentaux dans le domaine des données personnelles. En outre, elle crée la possibilité, du fait même de l'explosion des flux de données, de déborder son cadre territorial en imposant des impératifs de protection à ses partenaires commerciaux.

Sur le plan des principes affirmés, la directive reprend une approche de protection des droits fondamentaux déjà présente dans certains appareils législatifs nationaux des États-membres (notamment la loi française du 6 janvier 1978 qui créa la Commission nationale de l'informatique et des libertés), et affirmée au niveau européen par la Convention n°108 du Conseil de l'Europe, adoptée le 28 janvier 1981, pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

La directive de 1995 conforte certains principes de la convention n°108, comme ceux de l'article 6 relatifs à la qualité de la donnée, garantit les droits d'information, de rectification, d'opposition, et prohibe certains traitements révélant l'origine raciale ou ethnique, les opinions politiques, religieuses ou philosophiques, l'appartenance syndicale.

La directive s'appuie sur le fondement de l'actuel article 114 du traité sur le fonctionnement de l'Union européenne (TFUE), relatif au rapprochement des législations des États-membres ayant pour objet le fonctionnement et l'établissement du marché intérieur. L'une des innovations remarquables de la directive consiste en la création imposée à chaque Etat d'une autorité de contrôle indépendante dotée de pouvoirs d'investigation et d'intervention, dont la réunion au niveau de l'Union constitue le groupe des autorités nationales de protection des données (dénommé G29 car prévu à l'article 29 de la directive).

La directive distingue les échanges de données entre États-membres, régis par un strict principe de libre-circulation, et les transferts vers les pays tiers, autorisés à la condition que soit respecté un « niveau adéquat de protection ». La Commission européenne est chargée de vérifier celui-ci après l'avis du G29.

En 1995, l'Union européenne consacre donc une meilleure défense des droits des personnes quant à la protection de leurs données dans un champ général, public et privé, et concilie un impératif économique, celui de réguler des pratiques digitales appelées à un rapide développement, à l'urgence de consacrer des droits numériques comme de véritables droits fondamentaux.

3. Plusieurs régimes de transfert des données vers des pays tiers sont prévus afin d'assurer la protection la plus adéquate

Les données ne s'arrêtant pas aux frontières de l'Union, il était nécessaire de prolonger les garanties offertes aux utilisateurs européens dans un cadre « extraterritorial », celui de l'espace numérique, ce qui n'allait pas de soi.

L'originalité de la directive repose là aussi sur la conception que le droit à la protection des données ne peut voir son application limitée au territoire européen, le sujet en cause étant par nature dématérialisé. Il faut toutefois souligner que la directive prévoyait dès 1995 à l'article 26.1 un certain nombre de cas très spécifiques dans lesquels, même si le pays de destination n'offrait pas un niveau approprié de protection, les données pouvaient néanmoins être transférées, en l'occurrence, si :

- la personne concernée a donné indubitablement son consentement au transfert envisagé ;
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures pré-contractuelles prises à la demande de la personne concernée ;
- le transfert est nécessaire à la conclusion et l'exécution d'un contrat conclu ou à conclure dans l'intérêt de la personne concernée entre le responsable du traitement et un tiers ;
- le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important ou pour la constatation, l'exercice ou la défense d'un droit de justice ;
- le transfert est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ;
- le transfert intervient au départ d'un registre public qui, en vertu des dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

Hormis ces cas, trois types d'instruments ont été développés de façon à assurer un transfert sécurisé des données personnelles et respectueux des droits des individus sur leurs données.

a. Les clauses contractuelles appropriées

Les garanties suffisantes qui conditionnent l'autorisation du transfert de données personnelles à un États tiers par un Etat membre peuvent selon l'article 26.2 de la directive résulter de « clauses contractuelles appropriées ». Mais la Commission peut également, selon l'article 26.4, reconnaître des « clauses contractuelles types » et sa décision s'impose alors aux États. Ces clauses contractuelles types, formalisées dans une décision de la Commission adoptée pour la première fois en 2001 et modifiées depuis à plusieurs reprises permettent d'assurer le respect d'obligations équivalentes à celles contenues dans la directive dans le cadre d'un contrat de transfert entre un exportateur et un importateur de données.

b. Les règles d'entreprise contraignantes

Création du groupe de l'article 29 sur le fondement de l'article 26.2 de la directive de 1995, ces règles d'entreprise contraignantes (*Binding Corporate Rules,* ou *BCR*) sont des codes de conduite internes à destination des entreprises possédant des filiales internationales amenées à opérer entre elles des transferts de données. Le responsable du traitement doit alors offrir des « garanties suffisantes » dans un projet de règles d'entreprise approuvé par l'autorité de contrôle compétente (cela peut être une autorité chef de file si l'entreprise possède des entités dans plusieurs pays membres de l'Union).

c. La décision d'adéquation

Une décision d'adéquation a pour effet de permettre le transfert, sans garanties supplémentaires, de données à caractère personnel depuis les pays membres de l'Espace économique européen (les vingt-sept États membres de l'Union européenne, ainsi que la Norvège, le Liechtenstein et l'Islande) vers le pays tiers concerné. Pour adopter une telle décision, la Commission européenne se base sur l'article 25.6 de la directive de 1995 établissant que le pays de destination assure un niveau de protection équivalent des données à caractère personnel en raison de sa législation interne ou des engagements internationaux qu'il a souscrits. La protection offerte dans le pays de réception des données est donc censée être de même niveau que la protection au sein de l'Union européenne.

À ce jour, la Commission a reconnu douze pays comme assurant un niveau de protection adéquat des données, constatant par exemple que la Suisse, le Canada, l'Argentine, Guernesey, l'Île de Man et les principes de la « sphère de sécurité » publiés par le ministère du commerce des États Unis d'Amérique, assuraient un niveau de protection adéquat des données à caractère personnel, et que le niveau de protection des données à caractère personnel contenues dans les dossiers des passagers aériens (données PNR) transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique était adéquat.

Les décisions relatives à la pertinence de la protection sont adoptées selon la « procédure de comité », qui comprend les étapes suivantes :

- la Commission présente une proposition ;
- le groupe de l'article 29 rend un avis non contraignant ;
- le comité de l'article 31 rend un avis adopté à la majorité qualifiée des États membres ;
- le Parlement européen et le Conseil peuvent, à tout moment, demander à la Commission de maintenir, modifier ou retirer la décision d'adéquation au motif qu'elle excède les compétences d'exécution prévues par la Directive ;
- le collège des membres de la Commission adopte la décision.

Ces dispositions ont été réaffirmées par la réforme de la protection des données à caractère personnel, dans le chapitre V (articles 40 à 45) du Règlement Général sur la Protection des Données (GDPR) du 15 décembre 2015, adopté après trois années de négociation.

B. UN FRAGILE ÉQUILIBRE MIS EN CAUSE PAR LES RÉVÉLATIONS DE L'AFFAIRE SNOWDEN

1. Le « *Safe Harbor* », ou « sphère de sécurité »

C'est sur le fondement de l'article 25.2 de la directive de 1995 que la Commission a engagé des négociations avec le département du Commerce américain, afin de mettre en œuvre un cadre de protection adéquat pour les échanges de données transatlantiques. Ces négociations ont abouti à la publication par les autorités américaines de « *Principles of Safe Harbor* » le 21 juillet 2000, complétés par des « *Frequently Asked Questions* » concernant l'application de ces principes.

Ces principes reprenaient pour l'essentiel des notions contenues dans la directive européenne :

- l'information des personnes dont les données sont collectées ;
- la faculté pour la personne concernée de s'opposer à un transfert ou à un usage de ses données pour des finalités différentes de celles pour laquelle elle a initialement consenti, son consentement exprès étant requis dans le cas de données sensibles ;
- la soumission du transfert à une tierce partie possible à la condition exprès que celle-ci offre un niveau de protection adéquat ;
- un droit garanti d'accès et de rectification des données ;

- la sécurité des données ;
- l'intégrité des données ;
- le contrôle de l'effectivité de la mise en œuvre de ces principes, notamment par l'instauration de mécanismes de recours pour les personnes concernées.

La Commission a adopté le 26 juillet 2000 la décision d'adéquation 2000/520/CE, qui reconnait le niveau de protection adéquat offert par les États-Unis dans le cadre de ces « Principes de sécurité », et ce, en dépit des réserves émises par le Groupe de l'article 29 et le Parlement européen. Les deux institutions estimaient en effet que les garanties offertes n'étaient pas suffisantes, mais leur avis n'était pas contraignant pour la Commission.

Concrètement, pour les entreprises américaines, le cadre instauré par le « *Safe Habor* » exigeait qu'elles se conforment aux principes édictés par le biais d'un mécanisme d'auto-certification annuelle auprès du département du commerce américain. Pour cela, elles devaient intégrer dans leur politique interne relative à la protection de la vie privée des critères équivalents à ceux promus par le « *Safe Harbor* » et se conformer à ces principes.

Pour contrôler le respect par les entreprises de leur déclaration de conformité aux principes du « *Safe Harbor* », des voies de recours extrajudiciaires avaient été aménagées.

Il s'agissait d'un système de règlement des litiges pouvant prendre deux formes :

- soit par l'adhésion à des instances indépendantes reconnues compétentes pour examiner les plaintes des particuliers en cas de manquement aux principes du « *Safe Harbor* » (par exemple, un organisme d'arbitrage tel que l'*International Centre for Dispute Resolution/ American Arbitration Association*) ;
- soit dans un panel composé de représentants d'autorités de protection des données personnelles européennes, solution majoritairement retenue par les entreprises américaines, comme signalé dans la communication de la Commission sur le fonctionnement du « *Safe Harbor* » en 2013 [(1)].

En s'engageant à respecter les principes du « *Safe Harbor* », les entreprises américaines reçoivent une certification : en cas de non-respect des principes de protection, elles peuvent donc être accusées de pratiques

(1) Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, COM (2013) 847 final, 27 novembre 2013.

commerciales trompeuses ou frauduleuses sous la section 5 du *Federal Trade Commission Act*. Il faut donc noter que la compétence prévue ne s'étend ni aux pratiques non commerciales, ni à certains secteurs d'activités, comme celui des sociétés de télécommunications [(1)]. Cet accord concernait toutefois un nombre important d'entreprises américaines, 3246 au mois de septembre 2013 (soit huit fois plus de sociétés qu'en 2004) [(2)].

2. Le contexte international met en lumière les insuffisances du « *Safe Harbor* »

a. L'affaire des écoutes de masse (« bulk surveillance »)

Dès juillet 2013, la Vice-Présidente de la Commission Viviane Reding annonçait le réexamen de l'accord, en raison de doutes sur la protection réelle accordée aux données européennes aux États-Unis.

À la suite des révélations de la surveillance de masse opérée par les services de renseignement américains, potentiellement sur des données européennes recueillies par des compagnies telles que Facebook ou Google, l'autorité allemande de protection des données exprimait ses plus vives inquiétudes, suivie par les autorités du G29. L'autorité allemande de la BFDI (*Bundesbeaufragte für den Datenschutz und die Informations Freiheit*) envisageait en effet la possibilité de suspendre certains flux de transferts de données.

L'affaire PRISM

Le 6 juin 2013, les journaux *The Guardian* et *The Washington Post* portaient à la connaissance du public les révélations d'un ancien analyste de la NSA sur un programme nommé PRISM. Selon Edward Snowden, les services de renseignement américains (la NSA et le FBI) procédaient à des surveillances massives en bénéficiant d'un accès direct aux données personnelles de millions d'utilisateurs (américains ou non) par le biais de grandes sociétés qui se seraient ainsi rendues complices de violations de la vie privée. Le caractère apparemment automatique, indifférencié et généralisé des écoutes et interceptions réalisées, ainsi que la révélation du ciblage de certaines personnalités politiques et chefs de gouvernement « alliés » ou « amis » du gouvernement américain (notamment Angela Merkel), ont provoqué une véritable onde de choc mondiale.

Les divulgations d'Edward Snowden ont ainsi ébranlé la confiance indispensable à un accord comme celui de la « Sphère de sécurité », d'autant plus que les Européens ne disposaient pas, à l'égard de dispositifs de surveillance qu'ils

(1) L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne, Rapport d'information de Gaëtan Gorce et Catherine Morin-Desailly, Sénat, 8 juillet 2014.

(2) Mémo/13/1059 de la Commission européenne.

auraient pu vouloir contester, des mêmes garanties juridiques que les citoyens américains, et cela alors même que leurs données personnelles, en transitant par les sociétés commerciales sises aux États-Unis, pouvaient faire l'objet de cette surveillance.

b. La réponse des autorités européennes : une série de recommandations

Quelques mois après ce qui était devenu « l'affaire Snowden », le 27 novembre 2013, la Commission européenne publiait un memorandum porteur de treize recommandations pour réformer le « *Safe Harbor* », de façon à assurer la protection adéquate des données européennes.

Les treize recommandations étaient les suivantes :

- Dans le domaine de la transparence :

1. la publicité des dispositions de protection de la vie privée par les entreprises autocertifiées ;

2. l'inclusion dans celles-ci d'un lien pointant vers le site web du ministère du commerce consacré à la sphère de sécurité, (avec la liste des sociétés adhérentes «à jour» de leur certification ;

3. la publication des conditions de protection de la vie privée figurant dans tout contrat conclu entre les entreprises certifiées et leurs sous-traitants ;

4. le ministère du commerce devrait clairement signaler en ligne toutes les entreprises dont la certification n'est plus à jour.

- Pour améliorer les conditions de recours :

5. les dispositions de protection de la vie privée mises sur les sites web des entreprises doivent inclure un lien dirigeant vers le site d'un prestataire chargé du règlement extrajudiciaire des litiges (REL) ;

6. le REL devrait être facilement accessible et abordable économiquement ;

7. le ministère du commerce devrait contrôler plus systématiquement les prestataires de REL.

- Pour une mise en œuvre plus efficace de la sphère de sécurité :

8. un certain pourcentage des entreprises devraient être soumises à des enquêtes d'office concernant le respect effectif de leurs dispositions de protection de la vie privée (au-delà du contrôle du respect des exigences formelles) ;

9. pour chaque manquement constaté à la suite d'une plainte ou d'une enquête, l'entreprise concernée devrait, après un an, faire l'objet d'une enquête de suivi spécifique ;

10. en cas de doutes au sujet de la conformité d'une entreprise ou si des plaintes sont en cours d'examen, le ministère du commerce devrait en informer l'autorité compétente chargée de la protection des données dans l'État membre de l'UE concerné ;

11. les fausses déclarations d'adhésion à la sphère de sécurité devraient continuer à être examinées.

- Sur l'accès des autorités des États-Unis :

12. les politiques de protection de la vie privée adoptées par les entreprises autocertifiées devraient comporter des informations sur la mesure dans laquelle la législation des États-Unis permet aux autorités publiques de collecter et de traiter des données transférées au titre de la sphère de sécurité. En particulier, les entreprises devraient être encouragées à indiquer, dans leurs politiques de protection de la vie privée, quand elles dérogent auxdits principes pour répondre à des exigences relatives à la sécurité nationale, à l'intérêt public ou au respect des lois ;

13. le recours à la dérogation pour raison de sécurité nationale, prévu par la décision relative à la sphère de sécurité, devrait être étroitement limité aux cas où cela est strictement nécessaire et proportionné ;

L'Union européenne appelait donc à une révision profonde de l'accord et soulignait ses insuffisances : cette position allait se confirmer et se durcir avec l'appel du Parlement européen en mars 2014 à suspendre immédiatement le « *Safe Harbor* », au motif que ses principes ne garantissaient pas une protection adéquate pour les citoyens européens. Le Parlement européen appelait également l'administration américaine à proposer de nouvelles règles de transfert conformes au niveau d'exigence européen.

3. Une demande croissante de révision du cadre juridique

Comme l'a bien montré le groupe de travail ad hoc UE-États-Unis constitué en juillet 2013, de nombreux points restaient à clarifier pour assurer le respect des droits des usagers européens. Lors de ce travail, les États-Unis ont confirmé l'existence de ces programmes de surveillance en vertu de dispositions légales américaines fixant des conditions spécifiques et des garanties. Toutefois, il

apparaît bien, à la lumière des conclusions du groupe, que les procédures concernant le ciblage et la réduction au minimum de la collecte de données existaient pour les ressortissants américains (et particulièrement, les dispositions constitutionnelles du 1er et du 4ème amendement les contraignent) sans s'appliquer aux citoyens de l'Union européenne.

Par ailleurs, le manque de transparence autour des procédures en question était très problématique. Comme le soulignait la Commission européenne en novembre 2013 : « Puisque les ordonnances de *la Foreign Intelligence Surveillance Court* sont secrètes et que les sociétés sont tenues de garder le secret sur l'assistance qu'elles sont obligées de fournir, il n'y a aucune possibilité (judiciaire ou administrative) pour les personnes concernées, européennes ou américaines, de savoir si des données à caractère personnel les concernant font l'objet d'une collecte ou d'un traitement ultérieur. Les particuliers n'ont pas la possibilité d'obtenir l'accès aux données les concernant, ni de les faire rectifier ou effacer, et ils n'ont pas non plus de recours administratif ou judiciaire ».

Dans ce climat où la confiance avec le partenaire américain était largement entamée, les autorités nationales de protection des données au sein de l'UE manifestent alors également leur volonté de voir le texte renégocié : en avril 2014, le G29 insiste sur les recommandations 12 et 13 avancées par la Commission européenne dans son mémorandum, qui portent plus particulièrement sur l'utilisation des données à des fins de sécurité nationale aux États-Unis.

En mars 2015, l'autorité allemande de protection des données adoptait une résolution établissant que la décision d'adéquation relative au « *Safe Harbor* » adoptée en 2000 par la Commission ne fournissait pas une protection suffisante pour les droits fondamentaux lors des transferts transatlantiques de données. Elle réaffirmait la responsabilité de l'entité exportant les données et le caractère insuffisant de l'autocertification du respect des principes par les entreprises concernées.

C. LA RÉPONSE JURIDIQUE DE LA CJUE ENTÉRINE LE CARACTÈRE INADÉQUAT DU « SAFE HARBOR »

1. Le jugement de la Cour de Justice européenne (CJUE) d'octobre 2015 invalide le « *Safe Harbor* »

Mars 2015 voit le début de l'examen par la CJUE du cas adressé par la Haute cour d'Irlande, dans lequel l'activiste Max Schrems accusait l'entreprise Facebook de ne pas fournir la protection adaptée aux données européennes, permettant aux autorités américaines de mener des opérations de surveillance massive, à l'instar du programme PRISM. C'est la conclusion de ce procès, en octobre 2015, qui voit tomber le « *Safe Harbor* ». L'avocat général Yves Bot affirmait dans ses conclusions que l'instrument était invalide, le jugement de la CJUE confirme cette analyse, en soulignant notamment qu'une législation permettant aux autorités un accès général au contenu de communications

électroniques privées bafouait les droits fondamentaux, et particulièrement le droit au respect de la vie privée, garanti notamment par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme. Les autorités de protection des données personnelles doivent examiner toute plainte déposée sur cette base (ce qu'avait refusé de faire la DPC irlandaise sollicitée par M. Schrems), même s'il relève de la seule juridiction de la CJUE de déclarer une décision d'adéquation de la Commission invalide.

Le jugement, très attendu, de la CJUE, confirme les réserves de plus en plus fortes émises par les autorités de protection des données personnelles de l'Union européenne, dont la déclaration du 16 octobre pose les bases d'une renégociation de l'accord « *Safe Harbor* ». Le Groupe de l'article 29 estime en effet que les transferts ne peuvent plus être réalisés sous l'égide du « *Safe Harbor* », devenu illégal, et que seules les clauses contractuelles types (« Standard Contractual Clauses – SCS – contrats types de transfert de données adoptés par la Commission européenne), et les règles internes d'entreprise (« Binding Corporate rules » - BCR- codes de conduite au sein d'une entreprise pour les transferts entre les filiales notamment) peuvent fournir un cadre transitoire à défaut d'un accord plus global. Le G29 donne trois mois à la Commission pour la négociation d'un nouvel accord.

2. La Commission tire les conséquences du caractère invalide de la décision d'adéquation de 2000

a. La reprise des négociations avec les États-Unis

À la suite de sa communication de 2013 concernant le fonctionnement de la sphère de sécurité, la Commission avait entrepris des négociations avec le partenaire américain afin de fonder un nouvel accord, plus solide, sur les treize recommandations préconisées. L'invalidation de la décision d'adéquation de 2000 par la Cour de justice de l'Union européenne n'intervient donc pas véritablement comme une surprise pour la Commission, qui avait déjà souligné elle-même les défauts de l'accord à la lumière des éléments portés à sa connaissance par les révélations de l'affaire Snowden.

Dans sa communication en réaction à l'arrêt de la Cour de justice dans l'affaire Schrems, la Commission indique sa volonté de reprendre et d'intensifier les négociations et de les voir aboutir à un accord plus conforme aux recommandations de la Cour. Pour cela, la Commission se fixait un délai de trois mois.

b. Avant la conclusion d'un nouvel accord, le recours à des instruments transitoires de protection des droits

Dans l'intervalle, et en conformité avec l'avis du Groupe de l'article 29, ce sont d'autres instruments juridiques qui devront servir à pallier le vide laissé par

l’invalidation de la sphère de sécurité. Ces instruments, prévus dans la directive de 1995, sont les clauses contractuelles types et les règles d’entreprise contraignantes.

II. LE NOUVEAU CADRE NÉGOCIÉ PAR LA COMMISSION EUROPÉENNE PRESENTE DES AVANCÉES CERTAINES MAIS PEINE À CONVAINCRE DEFINITIVEMENT LES PARTIES PRENANTES

A. UN NOUVEAU « BOUCLIER DE PROTECTION DES DONNEES PERSONNELLES » VISANT À PALLIER LES FAILLES DU « SAFE HARBOR »

Le 29 février 2016, la Commission a rendu public l'ensemble des documents destinés à former le nouvel accord Union européenne-États-Unis pour la protection des données transférées, ainsi que la première version d'une décision d'adéquation visant à remplacer la précédente, invalidée par le jugement d'octobre 2015 de la CJUE. Le texte proposé par la Commission présente les principes (« *Privacy Shield Principles* ») devant guider les transferts de données.

1. Une meilleure protection des droits avec une large palette de recours non juridictionnels

L'accord prévoit une protection effective des droits avec plusieurs possibilités de recours effectif des citoyens européens. Sans les citer tous, d'autant que la mise en œuvre de certains n'est pas parfaitement expliquée dans les documents, il faut mettre en lumière les principales options données aux individus souhaitant contester le traitement ou l'usage de leurs données.

Ceux-ci pourront d'abord s'adresser directement aux compagnies s'étant rangées sous le bouclier de sécurité pour leur exposer leurs récriminations en cas de non-respect des principes du « *Privacy Shield* ». Les sociétés doivent à cet égard prévoir un organe indépendant de résolution des conflits afin d'enquêter et de donner une réponse à ces plaintes individuelles. Cette procédure ne devra entrainer aucun frais pour les individus souhaitant contester le respect des principes. Les entreprises visées devront en outre fournir une réponse dans les quarante-cinq jours.

Seconde option, les plaintes pourront être adressées directement à la FTC (*Federal Trade Commission*), sans toutefois que celle-ci n'ait d'obligation de les traiter. Les autorités européennes de protection des données personnelles pourraient également s'adresser au Département du Commerce américain, qui s'est engagé à faire de son mieux (dans l'annexe 1 de l'accord) pour faciliter la résolution du litige, auquel il sera donné ensuite priorité d'examen par la FTC. Là encore, la liberté laissée à la FTC dans l'examen des plaintes ne donne aucune garantie définitive à voir celles-ci effectivement examinées.

La possibilité est ouverte aux organisations de coopérer avec les autorités européennes de protection des données personnelles au sein d'un panel, mais l'organisation pratique d'une telle solution n'est pas explicitée dans le traité, ce qui est à regretter.

Une procédure d'arbitrage est également envisagée sans que le texte de l'accord n'en expose tous les rouages, mais devrait avoir pour cadre le droit américain et pour langue exclusive l'anglais. Cette condition, ainsi que la prise en charge des frais d'avocat par les individus eux-mêmes, pourraient rendre ce moyen inopérant dans les faits.

2. L'accord *« Privacy Shield »* intervient dans un paysage renouvelé quant à la protection des données personnelles

Parallèlement au bouclier de protection des données personnelles, qui vise les données commerciales, l'accord parapluie (« *umbrella agreement* ») devrait permettre de donner de meilleurs garde-fous pour les transferts de données à des fins de protection de l'ordre public (prévention et lutte contre le terrorisme, coopération policière et judiciaire). L'adoption du « *Judicial Redress Act* », qui garantit un droit d'accès aux citoyens européens devant les juridictions américaines pour contester le traitement fait de leurs données, a en effet permis de débloquer un processus de négociation complexe et sensible.

Trois motifs de recours juridictionnels (refus d'accès, refus de rectification et divulgation illicite par les autorités de l'autre Partie) sont désormais ouverts aux citoyens des « pays couverts » par le récent *« Judicial Redress Act »*. Cette nouvelle législation promulguée par le Président Obama en février 2016 étend en effet aux citoyens de pays tiers des garanties prévues pour les citoyens américains par le *« Privacy Act »* de 1974 : elle répond à une exigence européenne déjà ancienne et marque un réel progrès dans la protection des droits des citoyens européens.

Mais ce recours juridictionnel ne concerne que les données transférées par des autorités répressives de l'Union, il ne s'applique donc pas aux données commerciales. Cette voie de recours vient compléter des voies de recours juridictionnel disponibles à d'autres titres en ce qui concerne le traitement des données et ouvertes à toutes les personnes concernées de l'Union dont les données sont transférées à des fins répressives.

Un mécanisme de réexamen annuel conjoint doit permettre de contrôler le fonctionnement du dispositif du bouclier de protection dans la durée. Réalisé par la Commission européenne et la FTC, ce processus pourrait prendre appui sur des rencontres annuelles avec les ONG engagées dans le domaine du respect de la vie privée.

B. LE NOUVEAU DISPOSITIF RENCONTRE UN ACCUEIL MITIGÉ ET DEVRA ÊTRE PRÉCISÉ

1. Sortir du vide juridique

Depuis la publication des documents composant le futur « Bouclier de protection des données », les parties prenantes se sont exprimées dans des sens

contraires. Au regard des enjeux économiques très importants, il n'est pas étonnant que les entreprises les plus concernées aient salué un accord qui permettait de reprendre le « *business as usual* », et qui, selon elles, offrait des garanties assez solides pour les citoyens européens. Microsoft a ainsi affirmé son soutien au dispositif. En revanche, L'Observatoire des Libertés et du Numérique, qui regroupe en son sein Amnesty International France, le Syndicat de la magistrature, le Syndicat des Avocats de France, la Ligue des droits de l'Homme, La Quadrature du Net, le Cecil et le Creis-Terminal, a estimé que l'accord ne souscrivait pas aux obligations soulignées par l'avis de la Cour d'octobre, et continuait d'offrir trop peu de garanties pour les usagers européens.

2. Un avis du Groupe de l'article 29 mitigé, qui appelle à des précisions et des compléments pour que l'accord assure un niveau de protection équivalent

L'avis des autorités de protection des données personnelles européennes, très attendu, a offert un tableau en demi-teinte. Alors que des bruits couraient sur un possible refus en bloc de l'accord, qui aurait notamment émané d'une autorité allemande « maximaliste » en termes de protection des données à l'encontre d'une intervention de services de renseignement étrangers, le G29 a finalement rendu un avis mitigé reflétant la position médiane de l'ensemble des pays. Il a salué les avancées opérées par rapport au *« Safe Harbor »*, tout en signalant que des progrès restaient à accomplir pour parvenir à un accord pleinement satisfaisant.

Il faut souligner que l'arrêt de la CJUE du 6 octobre 2015 (arrêt Schrems) réaffirmait avec force le rôle des autorités nationales de contrôle, et donc leur autorité pour la protection des droits fondamentaux tels que définis par les articles 8 de la Convention européenne de sauvegarde des droits de l'homme et 7 et 8 de la Charte des droits fondamentaux.

Par ailleurs, la procédure d'adoption de la décision d'adéquation prévoit, à l'article 30 de la directive 95/46/EC cet avis non contraignant du groupe des autorités nationales. Ici, le G29 a donc examiné le projet d'accord au regard des articles évoqués plus haut (7 et 8 de la Charte, 8 de la CESDH), de la directive de 1995 toujours en vigueur et du droit à un recours effectif et à un procès équitable défini à l'article 47 de la Charte des droits fondamentaux.

Sans prétendre donner un compte rendu exhaustif de l'analyse du G29 disponible en ligne [(1)], les éléments suivants doivent être particulièrement relevés pour juger du degré de conformité, en l'état, du futur accord, à l'exigence d'une protection essentiellement équivalente.

---

(1) http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

a. Remarques sur l'accord dans son ensemble

Le G29 rappelle que son objectif principal est de s'assurer que le nouvel accord offre « un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive lue à la lumière de la Charte ». Il suit en cela les recommandations rappelées par la CJUE dans son arrêt d'octobre. D'un point de vue général, le G29 reconnait les progrès réalisés et observe la prise en compte de certaines critiques adressées par le passé au *Safe Harbor*.

Toutefois, le G29 déplore que la décision ne soit pas accompagnée d'une évaluation générale de la loi américaine et des exigences internationales auxquelles se conforment les États-Unis dans leurs activités de traitement des données.

Il regrette également la complexité des documents présentés (une décision d'adéquation et des annexes reprenant les échanges de lettres durant la négociation) ainsi que le manque de clarté et de lisibilité quant au langage adopté, certaines notions faisant l'objet de définitions parfois contradictoires ou changeantes au fil des pages.

Un glossaire, comme le suggère le travail du Groupe de l'article 29, pourrait à cet effet avoir le mérite de fixer des notions de manière plus claire et de dissiper ainsi certains risques d'insécurité juridique. La question des individus concernés par l'accord (s'agira-t-il des citoyens européens ou de tous les résidents européens ?) revêt par exemple une importance toute particulière, puisqu'elle conditionne l'accès aux mécanismes de recours mis en place.

b. Sur le volet commercial

Bien qu'il ne puisse être question d'exiger que le bouclier de protection soit un simple décalque du cadre juridique européen, le G29 estime néanmoins que certains principes et notions essentiels manquent dans la proposition ou les annexes, ou qu'on leur a substitué des principes alternatifs inadéquats.

C'est particulièrement le cas pour le principe de conservation des données, aucune notion de date ou de garantie n'étant donnée sur ce point dans l'accord, alors que ce principe est strictement encadré dans le droit européen. Ici, on voit bien que s'affrontent plusieurs logiques, celle de la protection des droits entendue du point de vue de l'individu, qui plaide pour que les données soient conservées le moins longtemps possible et dans un but strictement circonscrit à l'usage autorisé au départ par l'utilisateur, et une logique plus économique, qui voit la donnée comme une ressource commerciale et sa conservation comme source d'une valeur potentielle.

L'absence de mention de durée pourrait ainsi ouvrir la voie à une conservation indéfinie de la donnée par l'entreprise qui l'aurait récoltée, même si l'entreprise quittait le Bouclier de sécurité.

L'absence de recours contre des décisions individuelles prises sur le seul fondement d'un traitement automatisé de données est également préoccupante, dès lors que ces décisions peuvent évaluer certains aspects personnels de la vie des individus (le respect de leurs obligations de crédit, leur performance professionnelle) et avoir un impact significatif pour ceux-ci.

La question des transferts à des tiers de données importées sur le sol américain n'apparaît pas réglée dans le projet actuel, du moins le G29 insiste pour que les transferts vers des pays tiers garantissent un niveau de protection identique (y compris en matière de sécurité nationale) et n'aboutissent pas à affaiblir ou contourner les principes européens de protection des données.

c. Sur les exceptions au titre de la sécurité nationale

Le G29 déplore que le partenaire américain n'ait pas apporté d'éléments suffisamment précis pour écarter la possibilité d'une surveillance massive et indiscriminée des données des citoyens européens (« *bulk surveillance* »). Le Groupe de l'article 29 a toujours condamné cette surveillance massive et indiscriminée, qui n'est pas acceptable dans une société démocratique, malgré la tendance actuelle à collecter toujours plus de données dans le cadre de la lutte contre le terrorisme. Les exceptions aux principes de protection de la vie privée doivent être possibles, à condition que des garanties essentielles puissent les encadrer strictement.

Le G29 souligne dans son avis que le gouvernement a manifesté une réelle volonté d'accroitre la transparence autour des pratiques de renseignement des services de sécurité, notamment en mettant en ligne les textes encadrant ces pratiques, et en introduisant des directives devant guider l'action des services (il s'agit essentiellement ici du *Presidential Policy Directive 28*).

Malheureusement, de nombreuses imprécisions dans ces textes, ainsi que l'absence de garantie juridique sur l'application du *Foreign Intelligence Security Act* aux non-Américains (cette application ayant été assurée par les autorités mais non inscrite dans les textes) maintiennent un flou juridique encore regrettable.

Étant donné les préoccupations que cela implique en terme de protection des droits fondamentaux à la vie privée et à la protection des données, le G29 a annoncé qu'il suivra avec attention les décisions prochaines de la CJUE relatives à des cas de collecte massive et indiscriminée. Deux décisions, attendues pour le 9 juillet 2016, sur les *cas Tele2 Sveridge AB V. Post- och telestyrelsen* et *Secretary of State for the Home department V. Davis and others* pourraient en effet avoir des répercussions importantes sur ce sujet, et il conviendra selon vos rapporteurs d'être très vigilants quant à cette jurisprudence très évolutive.

En l'état actuel des choses, le G29 réitère donc ses inquiétudes quant à la prise en compte du principe de proportionnalité dans les collectes massives de données, et vos rapporteurs partagent les inquiétudes exprimées dans son avis.

d. Sur les procédures de recours

Plusieurs observations peuvent être apportées sur les voies de supervision et de recours présentées dans le Bouclier de sécurité.

D'une part, le partenaire américain a visiblement fait un véritable effort pour proposer une large palette de recours à la disposition des Européens, et il faut saluer le progrès que constitue l'adoption par le Président Obama du « *Judicial Redress Act* », qui leur étend un certain nombre de droits dans le transfert des données par les autorités à des fins répressives (ce qui fait l'objet d'un autre accord, « l'accord parapluie »). Cette avancée témoigne d'une plus grande sensibilité aux inquiétudes européennes.

Toutefois, on pourrait ici avancer que pour les recours dans le cadre des transferts de données personnelles commerciales, la quantité a été privilégiée à la qualité. En effet, pas moins de sept voies de recours sont proposées, mais dans des conditions matérielles telles qu'elles compromettent le droit à un recours effectif. La complexité de leur architecture, d'abord, qui rend très difficile la perception par un non-spécialiste de ses droits. Mais aussi la difficulté que représente pour un Européen le recours à un processus d'arbitrage sur le sol américain, quand bien même la procédure serait gratuite. Il faut noter que le mécanisme expliqué dans le Bouclier de sécurité ne tient pas compte de la recommandation selon laquelle les Européens devraient pouvoir disposer d'une voie de recours devant une Cour européenne.

D'autre part, des doutes subsistent sur le rôle et l'indépendance du Médiateur à l'égard du gouvernement américain. L'innovation que constitue l'introduction d'un tel mécanisme dans les relations des États-Unis avec un autre pays doit être saluée, mais l'étendue de ses pouvoirs et de son indépendance ne semble pas suffisamment assurée pour que cette avancée puisse être jugée complètement satisfaisante.

3. Un processus qui doit maintenant être complété

a. Vers l'adoption du texte

La procédure d'adoption de la décision d'adéquation prévoit encore la consultation des États-membres avant d'être finalisé par la Commission

Au sein du Comité de l'article 31 (prévoyant sa réunion dans la directive de 1995), les États-membres doivent à présent se prononcer sur la proposition de texte qui leur est soumise. La Commission souhaiterait pouvoir mettre en œuvre la décision d'adéquation dès le mois de juin 2016, afin que ne subsiste pas une situation d'insécurité juridique dommageable autant aux droits des Européens qu'aux intérêts économiques très importants que recouvre le sujet de l'échange transatlantique des données.

Plusieurs éléments donnent à penser que la décision d'adéquation pourrait être adoptée plus tard qu'initialement prévu, ou faire l'objet d'une remise en cause. Le Parlement européen pourrait adopter une résolution afin de souligner les manquements du texte. Mais surtout, l'arrêt de la CJUE sur la surveillance de masse, attendu pour juillet, pourrait remettre en cause l'équilibre du texte.

b. Un texte susceptible d'être amendé à l'avenir ?

Au vu des innovations introduites par la réforme du paquet Protection des données (directive et règlement de 2012 définitivement adoptés récemment et destinés à être applicables en 2017), certains principes absents de l'accord actuel pourraient devenir des objets de négociations à l'avenir, comme la portabilité des données ou le « droit à l'oubli numérique ».

Si la décision d'adéquation prévoit un mécanisme annuel d'examen conjoint du Bouclier de sécurité, qu'il faut saluer, cette procédure ne pourra que contrôler l'application effective du bouclier tel qu'il a été adopté. Il est très peu probable qu'elle soit un tremplin pour la discussion de nouveaux principes. Il apparaîtrait donc opportun que la décision d'adéquation comprenne une clause de renégociation fixant d'ores et déjà un rendez-vous aux autorités européennes et américaines. De la sorte, le standard établi par la réforme européenne de la protection des données pourrait plus rapidement devenir celui des échanges transatlantiques de données.

Ces perspectives s'inscrivent dans un contexte de jurisprudence évolutive et créatrice sur ces sujets, qui ouvre la voie à la conquête de nouveaux droits pour les Européens. Il fait peu de doute que les associations de protection de la vie privée et des droits fondamentaux de manière plus large se saisiront de l'opportunité de porter la nouvelle décision à l'attention de la CJUE, qui pourrait donc avoir rapidement à évaluer la solidité de l'accord *« Privacy Shield »* remplaçant le « *Safe Harbor »* qu'elle a décidé d'invalider en octobre.

TRAVAUX DE LA COMMISSION

La Commission s'est réunie le 11 mai 2016, sous la présidence de M[me] Danielle Auroi, Présidente, pour examiner le présent rapport d'information.

« **La Présidente Danielle Auroi.** Les propositions du rapport me paraissent refléter tout à fait les préoccupations de notre Commission et je vous propose d'adopter la proposition de résolution. »

La Commission *a adopté*, à l'unanimité, *la proposition de résolution ci-après.*

PROPOSITION DE RÉSOLUTION EUROPÉENNE

Article unique

L'Assemblée nationale,

Vu l'article 88-4 de la Constitution,

Vu le Traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

Vu la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

Vu la Convention européenne de sauvegarde des droits de l'homme, et notamment son article 8,

Vu la Convention 108 du Conseil de l'Europe,

Vu la 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,

Vu la proposition de directive COM(2012) 10 du Parlement européen et du Conseil du 25 janvier 2012 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,

Vu la proposition de règlement COM(2012) 11 du Parlement européen et du Conseil du 25 janvier 2012 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),

Vu la décision de la Commission 2000/520/CE 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,

Vu l'arrêt de la Cour de justice de l'Union européenne du 6 octobre 2015, dans l'affaire C-362/14, M. Schrems c/ Data Protection Commissioner,

Vu la communication COM(2015) 566 final de la Commission au Parlement européen et au Conseil du 6 novembre 2015 concernant le transfert transatlantique de données à caractère personnel conformément à la directive 95/46/CE faisant suite à l'arrêt de la Cour de justice dans l'affaire C-362/14 (Schrems),

Vu la communication COM(2016) 117 de la Commission au Parlement européen et au Conseil du 29 février 2016 « Flux de données transatlantiques: rétablir la confiance grâce à des garanties solides »,

Vu le projet d'accord pour un « Bouclier de sécurité » entre l'Union européenne et les États-Unis présenté le 29 février 2016,

Vu l'opinion 01/2016 du Groupe de l'article 29, constitué des autorités nationales de protection des données personnelles, sur le projet de décision d'adéquation concernant le bouclier de protection des données personnelles entre l'Union européenne et les États-Unis,

Considérant que les systèmes de traitement de données doivent respecter les libertés et droits fondamentaux des personnes, notamment la vie privée, et contribuer au progrès économique et social, au développement des échanges ainsi qu'au bien-être des individus,

Considérant le volume important des échanges de données personnelles avec les États-Unis, premier partenaire commercial de l'Union, et la nécessité de créer un cadre de protection des droits essentiellement équivalent à celui de l'Union européenne,

Considérant l'invalidation par la Cour de justice de l'Union européenne de l'accord « Safe Harbor- sphère de sécurité » introduit en 2000 entre l'Union et les États-Unis, et l'insécurité juridique qui pourrait en découler,

1. Se félicite des améliorations significatives apportées par le nouveau cadre pour les transferts transatlantiques de données, le «bouclier vie privée UE-États-Unis», notamment dans la définition de termes-clés, dans le respect des droits de correction ou de suppression de données ou encore dans la mise en place d'un mécanisme de révision annuelle,

2. Considère que l'accord gagnerait à être simplifié sous la forme d'un document unique et plus homogène,

3. Appelle à aller plus loin dans la clarification de la terminologie en veillant particulièrement à la cohérence de l'emploi des notions dans toutes les parties de l'accord, et en y adjoignant un glossaire,

4. Appelle à ce que la possibilité d'une surveillance massive et indiscriminée des données des citoyens européens soit plus clairement visée pour être écartée et à tout le moins limitée et proportionnée aux seuls objectifs de sécurité et de protection de l'ordre public clairement établis,

5. Demande à ce que l'ensemble des voies de recours pour les citoyens européens présente une architecture plus lisible, avec un rôle accru de point d'appui pour les autorités nationales européennes de protection des données,

6. Appelle à ce que le Médiateur américain prévu dans l'accord dispose de toutes les garanties pour assurer son office dans des conditions suffisantes d'indépendance,

7. Souligne que le transfert ultérieur des données à des pays tiers demeure en l'état un aspect problématique de l'accord,

8. Souhaite que soit introduite dans l'accord une clause de rendez-vous pour une renégociation, afin de prendre en compte les avancées permises par la réforme du cadre européen sur la protection des données personnelles.

MOTION FOR A EUROPEAN RESOLUTION

*On the '**Privacy shield' personal data protection agreement** between the **United States of America** and the **European Union**,*

The National Assembly,

In the light of Article 88-4 of the Constitution,

In the light of the Treaty on the Functioning of the European Union, and in particular its Article 16,

In the light of the Charter of Fundamental Rights of the European Union, and in particular its Articles 7 and 8,

In the light of the European Convention for the Protection of Human Rights, and in particular its Article 8,

In the light of Convention 108 of the Council of Europe,

In the light of directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data,

In the light of the proposal for a directive COM(2012) 10 of the European Parliament and of the Council of 25 January 2012 on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data,

In the light of the proposal for a regulation COM(2012) 11 of the European Parliament and of the Council of 25 January 2012 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation),

In the light of Commission decision 2000/520/EC of 26 July 2000 pursuant to directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce,

In the light of the Judgement of the Court of Justice of the European Union of 6 October 2015, in case C-362/14, M. Schrems v Data Protection Commissioner,

In the light of the communication COM(2015) 566 final from the Commission to the European Parliament and the Council of 6 November 2015 on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC, following the Judgement by the Court of Justice in Case C-362/14 (Schrems)

In the light of the communication COM(2016) 117 from the Commission to the European Parliament and the Council of 29 February 2016 'Transatlantic Data Flows: Restoring Trust through Strong Safeguards',

In the light of the draft agreement for a 'Privacy shield' between the European Union and the United States presented on 29 February 2016,

In the light of the opinion 01/2016 of the Article 29 Group, formed by national authorities for the protection of personal data, on the draft adequacy decision on the personal data privacy shield between the European Union and the United States,

Considering that data processing systems must respect people's fundamental rights and freedoms, especially privacy, and contribute to economic and social progress, the development of trade and the well-being of individuals,

Considering the large volume of exchanges of personal data with the United States, the EU's principal trading partner, and the need to create a protective framework for rights essentially equivalent to that of the European Union,

Considering the invalidation by the Court of Justice of the European Union of the Safe Harbour agreement introduced in 2000 between the EU and the United States, and the legal uncertainty which could arise,

1. Welcomes the significant improvements contributed by the new EU-US data transfer framework, the 'EU-US privacy shield', especially as regards the definition of key terms, its respect for the rights to correct or delete data and the introduction of an annual review mechanism,

2. Considers that the agreement should be simplified in the form of a single and more homogeneous document,

3. Calls for further clarification of the terminology by paying special attention to consistent use of notions in all parts of the agreement, and by attaching a glossary thereto,

4. Calls for the possibility of massive and indiscriminate surveillance of the data of European citizens to be more clearly stated so as to be ruled out and at the very least limited and proportionate to the sole clearly established goals of security and the protection of public order,

5. Demands that all the judicial remedies for European citizens should present a clearer structure, with a greater role as a cornerstone for the European national data protection authorities,

6. Demands that the American ombudsperson provided for in the agreement should have all the guarantees to fulfil his duties in a sufficiently independent manner,

7. Emphasises that the subsequent transfer of data to third countries remains as such a thorny aspect of the agreement,

8. Desires that a rendezvous clause for a renegotiation be included in the agreement so as to take account of advances allowed by the reform of the European personal data protection framework.

ANNEXES

PROJET D'ACCORD UNION EUROPÉENNE – ÉTATS-UNIS POUR LA PROTECTION DES DONNÉES

Le projet d'accord, et ses annexes, peuvent être consultés sur le site de la Commission européenne à l'adresse suivante :

http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

Annexes :
http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-1_en.pdf
http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-2_en.pdf
http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-3_en.pdf
http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-4_en.pdf
http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-5_en.pdf
http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-6_en.pdf
http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision-annex-7_en.pdf