L'avenir incertain des flux de données transatlantiques

Par Florence G'SELL
Professeure de droit privé à l'Université de Lorraine, titulaire de la chaire Digital, Gouvernance et Souveraineté à Sciences Po Paris, Professeure invitée à l'Université de Stanford (Cyber Policy Center)

La légalité des transferts de données entre l'Union européenne et les États-Unis constitue une problématique de longue date compte tenu des approches très différentes de la protection de données personnelles de part et d'autre de l'Atlantique. Les accords permettant d'encadrer et légaliser les flux de données transatlantiques – *Safe Harbor*, puis *Privacy Shield* – ont été successivement annulés. Le nouveau mécanisme mis en place, le récent *Data Privacy Framework*, est d'ores et déjà contesté, ce qui laisse planer une réelle incertitude sur la possibilité, pour les entreprises, de transférer effectivement des données aux États-Unis.

Bien qu'essentiels à tous les secteurs de l'économie, les flux de données entre l'Europe et les États-Unis se font aujourd'hui dans une grande insécurité juridique, alors même que les grandes entreprises technologiques américaines implantées en Europe transfèrent massivement les données des utilisateurs européens vers les États-Unis. Originellement, toutefois, la protection des données n'était pas exclusivement une préoccupation européenne. Dès 1973, un rapport du ministère fédéral de la Santé, de l'éducation et du bien-être américain avait énoncé des principes en matière de collecte des données personnelles[1], qui ont ensuite été publiés, sous forme de lignes directrices, par l'OCDE en 1980[2] et eu une grande influence internationale.

Il reste que c'est en Europe que les premiers cadres contraignants ont été imposés avec l'adoption des lois allemandes[3] et françaises[4], puis la conclusion, sous l'égide du Conseil de l'Europe, de la Convention sur la protection des données, également connue sous le nom de Convention 108, qui a fourni une première définition de la notion de « donnée personnelle » comme « toute information concernant une personne physique identifiée ou identifiable ». L'adoption, en 1995, de la directive 95/46/CE relative à la protection des données a permis à l'Union européenne de se doter d'un cadre global de protection des données personnelles et d'encadrer les transferts de données en direction des pays tiers.

Dans le même temps, les États-Unis n'ont pas adopté de règlementation d'ensemble destinée à garantir une protection effective des données personnelles. À partir du début

[1] "Records, computers and the rights of citizens", report of the Secretary's advisory committee on automated personal data systems, US Department of Health, Education & Welfare, July 1973.

[2] Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel, adoptées le 23 septembre 1980.

[3] Loi du 21 janvier 1977 portant protection contre l'emploi abusif de données d'identification personnelle dans le cadre du traitement des données.

[4] Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

des années 2000 et de l'adoption du *Patriot Act*[5], des programmes de surveillance ont été mis en place qui ont consisté à permettre aux agences de renseignement américaines de collecter en masse les informations circulant sur les réseaux. Dans un tel contexte, les garanties très sommaires offertes aux citoyens américains en matière de protection des données personnelles sont très insuffisantes aux yeux des Européens, alors même que les entreprises établies aux États-Unis y transfèrent massivement les données collectées en Europe.

Dans ce cadre, les autorités américaines et européennes ont tenté de pallier le décalage entre les approches européennes et américaines en se mettant d'accord sur des cadres permettant de faire en sorte que les transferts se font dans des conditions jugées satisfaisantes par les européens. Plusieurs mécanismes se sont succédés : la « sphère de sécurité » (*Safe Harbor*), le « bouclier de protection des données » (*Privacy Shield*), et désormais le *Data Privacy Framework* qui vient d'être adopté.

Le *Safe Harbor*, première tentative d'encadrement des flux de données transatlantiques

Dès 1990, la Commission européenne, craignant que la disparité des législations nationales nuise au marché intérieur, a proposé un texte relatif à la protection des données personnelles qui est devenu, en 1995, la directive 95/46/CE relative à la protection des données[6]. L'article 25 de cette directive prévoyait, en particulier, que les données à caractère personnel ne pouvaient être transférées vers un pays extérieur à l'UE que si ce pays assurait un niveau de protection « adéquat », c'est-à-dire équivalent à la protection garantie par le droit de l'Union.

La directive de 1995 a habilité la Commission à constater que certains pays tiers garantissent un niveau de protection adéquat du fait de leur législation ou de leurs engagements internationaux. Ces décisions d'adéquation s'imposent aux États membres et permettent de transférer légalement les données en direction des pays concernés. En revanche, lorsqu'aucune décision d'adéquation n'a été adoptée à propos du pays destinataire, les entreprises souhaitant y exporter des données personnelles doivent garantir par contrat qu'elles sont elles-mêmes en mesure de fournir un niveau de protection adéquat. C'est ainsi qu'a été consacré l'usage de « clauses contractuelles types », qui sont des clauses standards préapprouvées par les autorités qui permettent aux exportateurs de données de transférer celles-ci vers des pays pour lesquels aucune décision d'adéquation n'a été adoptée. Des clauses contractuelles types sont ainsi publiées par la Commission européenne et reprises par les entreprises qui le souhaitent.

S'agissant des États-Unis, le caractère adéquat de la législation américaine, peu protectrice des données personnelles, n'allait pas de soi. Les États-Unis et l'Union européenne se sont alors mis d'accord sur un mécanisme devant permettre aux entreprises américaines d'offrir un niveau de protection adéquat. En 2000, le Département du Commerce américain a publié sept *Safe Harbor Privacy Principles* que les entreprises devaient s'engager à respecter si elles voulaient pouvoir transférer des données depuis l'Europe vers les États-Unis. Ces entreprises devaient certifier chaque année, dans une lettre adressée au Department of Commerce, qu'elles adhéraient à ces principes, dont le respect effectif devait être contrôlé par la Federal Trade Commission. Le caractère « adéquat » de la protection ainsi

[5] Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) of 2001.

[6] 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, Journal officiel n°L 281 du 23/11/1995, pp. 31-50.

offerte fut reconnu par la Commission européenne dans une décision d'adéquation du 26 juillet 2000[7], qui fondait juridiquement les transferts de données personnelles vers les États-Unis. Plus de 5 000 entreprises ont ainsi adhéré au *Safe Harbor*.

Cet accord n'a toutefois pas résisté au scandale provoqué par les révélations d'Edward Snowden qui a, en 2013, divulgué au grand public l'existence de programmes de surveillance de masse menés par les autorités américaines[8]. La section 702 du *Foreign Intelligence Surveillance Act* (FISA) permet, en effet, aux services de renseignement américains de procéder à une surveillance ciblée de personnes étrangères situées en dehors des États-Unis en contraignant les fournisseurs américains de services de communication électronique à leur communiquer des données[9]. Il leur suffit simplement d'obtenir annuellement l'autorisation de principe d'une juridiction spéciale, la Foreign Intelligence Surveillance Court (FISC), qui approuve les programmes de surveillance de manière globale mais n'est pas consultée sur la détermination des personnes ciblées. Par ailleurs, l'*Executive Order* 12333, adopté en 1980, autorise les activités de surveillance menées hors des États-Unis et autorise notamment la « collecte en vrac » des données sans aucun contrôle judiciaire, ce qui permet l'acquisition de quantités massives de données. Dans ce cadre, les informations divulguées par Edward Snowden ont permis de montrer que la National Security Agency (NSA) avait obtenu un accès quasi illimité aux données collectées par des grandes entreprises technologiques américaines, notamment dans le cadre d'un programme appelé PRISM. Ironie du sort, les entreprises impliquées dans PRISM participaient toutes également au *Safe Harbor*.

Dans la foulée de ces révélations, la Commission européenne a publié, le 27 novembre 2013, treize recommandations destinées à améliorer le fonctionnement du *Safe Harbor*[10]. Au même moment, Maximilian Schrems, un étudiant en droit autrichien utilisateur de Facebook, déposait plainte contre Facebook auprès de l'autorité de protection des données irlandaise pour avoir massivement transféré ses données personnelles vers les États-Unis tout en participant au programme PRISM. Saisie d'une question préjudicielle par les juridictions irlandaises, la Cour de justice de l'Union européenne a invalidé, le 6 octobre 2015, la décision d'adéquation relative au *Safe Harbor*[11]. La CJUE a jugé que la Commission européenne aurait dû davantage examiner les lois et les engagements internationaux des États-Unis avant d'adopter la décision d'adéquation. Elle a par ailleurs estimé que l'accès généralisé, par les services de renseignement américains, aux données des utilisateurs et l'absence de recours efficaces contre cet accès compromettait l'essence du droit fondamental au respect de la vie privée, tel qu'il est garanti par l'article 7 de la Charte des droits fondamentaux de l'Union européenne.

L'intermède du *Privacy Shield*

À la suite de l'invalidation du *Safe Harbor*, les autorités européennes et américaines se sont rapidement mises d'accord sur un nouveau mécanisme appelé « bouclier de la

[7] Décision 2000/520/CE : Décision 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 », Journal officiel n°L 215 du 25/08/2000 pp. 7-47.

[8] "NSA Files: Decoded", *The Guardian*, November 1, 2013.

[9] G'SELL F., « Quel avenir pour les transferts transatlantiques de données après la sanction de Meta par l'autorité de protection des données irlandaise ? », Blog de la Chaire Digital, Gouvernance et Souveraineté, Sciences Po, 1er juin 2023.

[10] Recommandation de la Commission du 27 novembre 2013 relative à des garanties procédurales en faveur des personnes vulnérables soupçonnées ou poursuivies dans le cadre des procédures pénales, Journal Officiel n°C 378/8 du 24/12/2013, pp. 8-10.

[11] CJUE 6 octobre 2015, affaire C-362/14.

protection des données » (*Privacy Shield*). Dès le 12 juillet 2016, la Commission européenne a adopté une nouvelle décision d'adéquation[12] justifiée par les nouvelles garanties fournies dans le cadre du *Privacy Shield*. Les autorités américaines se sont, en particulier, engagées à s'abstenir de pratiquer une surveillance de masse et indiscriminée sur les données transférées aux États-Unis. Il a également été convenu qu'un médiateur (*ombudsman*) indépendant des autorités américaines traiterait des recours formés par les européens dont les données personnelles sont transférées aux États-Unis.

Pendant que la Commission européenne et les autorités américaines négociaient le *Privacy Shield*, les instances européennes rédigeaient le Règlement général sur la protection des données (RGPD), qui a été définitivement adopté en 2016 pour une entrée en vigueur le 25 mai 2018[13]. Le RGPD a renforcé et uniformisé les principes de protection des données personnelles figurant dans la directive de 1995. Comme celle-ci, il prévoit que les transferts de données vers des pays extérieurs à l'UE ne sont possibles que si ces transferts sont fondés sur une décision d'adéquation adoptée par la Commission ou, à défaut, lorsque les entreprises se livrant aux transferts offrent des garanties appropriées, par exemple grâce à des clauses contractuelles types (article 46). Il faut, en ce cas, que les personnes concernées disposent de droits opposables et de voies de recours effectives. C'est sur ce point que le contentieux relatif aux transferts de données réalisés par Facebook (devenu Meta) s'est poursuivi, Max Schrems ayant maintenu son opposition au transfert de ses données après l'invalidation du *Safe Harbor*. Selon Schrems, les clauses contractuelles types, qui ne sont pas contraignantes pour les services de renseignement américains, ne peuvent constituer une base juridique valable pour les transferts vers les États-Unis.

C'est dans le cadre de ce contentieux que le 16 juillet 2020, la Cour de justice de l'Union européenne a invalidé la décision d'adéquation relative au *Privacy Shield*[14]. La Cour a, en effet, rappelé que la législation des États-Unis, en ce qu'elle permet largement l'accès des services de renseignement américains aux données personnelles n'offre pas de garanties suffisantes aux européens dont les données sont transférées. Elle a, en outre, jugé que les mesures prévues par le *Privacy Shield* n'étaient pas suffisantes, notamment dans la mesure où elles ne garantissaient pas un droit de recours effectif aux citoyens européens. Elle a, enfin, confirmé que les clauses contractuelles types peuvent offrir un fondement juridique approprié aux transferts des données hors de l'Union, en précisant que les responsables de traitement et les autorités de protection des données doivent suspendre ou interdire les transferts de données en cas de conflit entre les obligations prévues par ces clauses et les législations des pays destinataires des données. C'est donc principalement sur le fondement de clauses contractuelles types que les transferts de données vers les États-Unis ont été réalisés depuis la décision du 16 juillet 2020.

Vers un nouveau cadre de transferts des données ? Le *Data Privacy Framework*

Au printemps 2022, l'Union européenne et les États-Unis ont conclu un nouvel accord politique en vue de mettre sur pied un nouveau mécanisme permettant de faciliter les transferts des données outre-Atlantique. Dans ce cadre, les États-Unis se sont engagés à faire en sorte que les activités des services de renseignement soient « nécessaires et

[12] Décision d'exécution de la Commission 2016/1250 du 12 juillet 2016 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, Journal Officiel 2016, L 207, p. 1).

[13] 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, Journal Officiel 2016, L 119, p. 1.

[14] CJUE, 16 juillet 2020, affaire C-311/18.

proportionnées », deux garanties auxquelles les Européens sont attachés. Ils se sont également engagés à créer une autorité indépendante chargée d'encadrer et contrôler la manière dont les données sont collectées et traitées aux États-Unis, et notamment par les services de renseignement américains.

Dans la foulée de cet accord, le Président américain Joe Biden a signé, le 7 octobre 2022, le décret présidentiel (*Executive Order*) on *Enhancing Safeguards for United States Signals Intelligence Activities* (EO 14086) destiné à mieux encadrer les activités de surveillance. Le texte prévoit que les autorités ne peuvent collecter des données que pour un objectif de sécurité nationale, lorsque cela est nécessaire en vue d'un objectif expressément défini et seulement d'une manière proportionnée à cette priorité. Les exigences de « nécessité » et de « proportionnalité » sont explicitement mentionnées dans le texte. Les services de renseignement devront, dans ce cadre, modifier leurs procédures afin de respecter les nouvelles garanties, sous le contrôle d'un nouveau Conseil de surveillance de la vie privée et des libertés civiles qui réalisera un audit annuel de ces procédures.

Par ailleurs, le décret prévoit un mécanisme de recours au profit des personnes concernées devant le responsable de la protection des libertés civiles du bureau du directeur du renseignement national (Civil Liberties Protection Officer). Les décisions du CLPO pourront elles-mêmes être contestées devant une nouvelle Cour de contrôle de la protection des données (Data Protection Review Court). Toutes les décisions prises par ces autorités seront contraignantes pour les services de renseignement. Destinées à répondre aux préoccupations européennes, ces possibilités de recours constituent la seule véritable nouveauté du *Data Privacy Framework*. Il faut toutefois souligner que ce droit au recours n'est offert qu'aux citoyens des pays désignés comme « États éligibles » par l'*attorney general* des États-Unis. Celui-ci doit donc décider si la législation des pays concernés en matière de collecte de données et de surveillance respecte suffisamment le droit à la vie privée des citoyens américains. Le 30 juin 2023, Merrick Garlan, *attorney general* des États-Unis, a désigné l'Union européenne ainsi que l'Islande, la Norvège et le Liechtenstein (l'Espace Économique Européen) comme États éligibles à ce titre.

Par ailleurs, dans la foulée de la publication de l'*Executive Order* 14086, la Commission européenne a publié, le 13 décembre 2022, un projet de décision d'adéquation prenant en considération les garanties supplémentaires désormais accordées. Comme cela avait été le cas lors de la publication du projet de *Privacy Shield*, ce projet de décision d'adéquation a fait immédiatement l'objet de critiques. En particulier, le Comité européen de protection des données (CEPD), composé de représentants de l'ensemble des autorités nationales de protection des données, a rendu, le 28 février 2023, un avis réservé[15]. Certes, le CEPD relève les améliorations substantielles apportées par le nouveau cadre. Cependant, il estime souhaitable de clarifier un certain nombre de dispositions relatives, par exemple, à la conservation des données. Le CEPD regrette, en outre, que la collecte de masse ne soit pas soumise à l'exigence d'une autorisation préalable par un organe indépendant. Le CEPD insiste, par ailleurs, sur le fait que la procédure d'autorisation fondée sur la section 702 FISA n'est en rien modifiée dans le nouveau mécanisme : la FIS Court ne fait qu'autoriser globalement les programmes de surveillance sans être sollicitée sur la détermination des cibles, ce dont il découle qu'il n'y a pas de véritable contrôle effectif des programmes de surveillance par une autorité judiciaire indépendante. D'ailleurs, la section 702 du *Foreign Intelligence Surveillance Act* (Fisa), qui doit expirer au 31 décembre 2023, devrait probablement être reconduite par le Congrès sans modification, ce qui est, du reste, le souhait de l'administration Biden. Enfin, si la création de la nouvelle Data Protection Review Court (DPRC) est bienvenue, les conditions de sa saisine doivent, selon le CEPD, être clarifiées, notamment la condition selon laquelle le demandeur doit démontrer que ses droits ont été atteints (*adversely affected*).

[15] CEPD, Avis n°5/2023, 28 février 2023.

De son côté, le Parlement européen s'est prononcé, le 11 mai 2023, dans une résolution adoptée en séance plénière, qui conclut que le nouveau cadre de protection des données UE-États-Unis ne crée pas d'équivalence substantielle du niveau de protection et invite la Commission à poursuivre les négociations. Le texte relève, entre autres choses, que la collecte en masse de données personnelles est toujours permise dans certains cas et n'est pas soumise à une autorisation préalable indépendante. La résolution souligne également que la nouvelle DPRC rendra des décisions confidentielles, que les juges de la cour pourront être révoqués par le président des États-Unis, et que celui-ci pourra également annuler ses décisions, de sorte que la Cour n'est pas vraiment indépendante. Si la résolution du Parlement ne lie pas la Commission européenne, elle est toutefois importante politiquement.

Le 10 juillet 2023, la Commission européenne a adopté définitivement la décision d'adéquation relative au *Data Privacy Framework* (DPF)[16] après avoir constaté que les garanties prévues par l'Executive Order 14086 et la *Data Privacy Framework* UE-États-Unis offrent un niveau de protection adéquat pour les données à caractère personnel transférées depuis l'Union européenne. La décision détaille notamment les recours désormais possibles dans le nouveau cadre. Elle souligne également le nouveau système de certification prévu par le DPF, aux termes duquel les entreprises souhaitant transférer les données devront s'engager à respecter un certain nombre de principes établis par le Department of Commerce américain, et obtenir, sur cette base une certification qui pourra être retirée en cas de violation des règles du DPF.

Il était temps que le nouveau cadre entre en vigueur. Depuis l'invalidation du *Privacy Shield* le 16 juillet 2020, les transferts transatlantiques de données étaient majoritairement fondés sur des clauses contractuelles types, ce qui posait des difficultés de plus en plus insurmontables. Le 12 mai 2023, la Data Protection Commission irlandaise[17] a lourdement sanctionné Meta, à la demande du Comité Européen de Protection des Données, en condamnant l'entreprise à payer une amende de 1,2 milliard et à cesser à brève échéance de transférer des données aux États-Unis[18]. En l'état, ont dit les autorités européennes de protection des données, la législation américaine est telle qu'il n'est pas possible de garantir une protection adéquate avec des clauses contractuelles types. La nouvelle décision d'adéquation ne va toutefois apporter qu'une sécurité juridique relative aux entreprises se livrant à des transferts transatlantiques de données. La décision pourrait fort bien, en effet, faire l'objet d'une nouvelle décision d'invalidation, Max Schrems ayant d'ores et déjà annoncé vouloir contester le nouveau cadre. L'enjeu est de taille. À défaut d'un cadre juridique suffisamment sûr, les entreprises concernées pourraient être tentées de renoncer à transférer les données aux États-Unis pour les traiter exclusivement sur des serveurs situés en Europe. Une telle logique de localisation des données pourrait cependant avoir pour conséquence de rendre plus difficile le développement et le partage, en Europe, d'applications sophistiqués et ambitieuses. Il faut donc espérer que, malgré les critiques, le nouveau *Data Privacy Framework* puisse enfin aboutir à ce que les flux de données se fassent en toute sécurité et dans le respect des droits des personnes concernées.

[16] Commission implementing decision of 10.7.2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate level of protection of personal data under the EU-US Data Privacy Framework C(2023) 4745 final.

[17] Decision of the Data Protection Commission made pursuant to Section 111 of the Data Protection Act 2018 and Articles 60 and 65 of the General Data Protection Regulation.

[18] G'SELL F. (2023), « Quel avenir pour les transferts transatlantiques de données après la sanction de Meta par l'autorité de protection des données irlandaise ? », Blog de la Chaire Digital, Gouvernance et Souveraineté, Sciences Po, 1er juin.