Vie du droit

La nouvelle décision d'adéquation (*Privacy Shield*) pour les transferts des données personnelles de l'Union européenne vers les États-Unis

Serena Crespi(*)

- **L'invalidation par l'arrêt *Schrems* du 6 octobre 2015 du *Safe Harbor* a créé une situation de forte incertitude**
- **La Commission a adopté un nouvel instrument — le *Privacy Shield* — qui présente d'importantes nouveautés**
- **Les principaux changements sont le rôle des autorités publiques des États-Unis et les mécanismes de recours offerts aux citoyens de l'Union européenne**

1 Nature et fonction du *Privacy Shield*

Le 2 février 2016, la Commission européenne a annoncé la conclusion d'un accord de principe entre l'Union européenne et les États-Unis relatif aux conditions dans lesquelles les données personnelles UE peuvent être transférées à cet État tiers. Cet accord a été suivi, le 29 février 2016, par la présentation par la Commission d'une proposition de décision d'adéquation UE/US. Cette décision — le *Privacy Shield*[1] — a finalement été adoptée le 12 juillet dernier,[2] après la réouverture des négociations sur certains points, afin de répondre notamment à certaines critiques formulées par les autorités nationales de protection des données.

Cette décision trouve sa base juridique en l'article 25 de la directive 95/46/CE relatif à la protection des personnes physiques à l'égard du traitement des données personnelles[3] (ci-après, la « directive »), en voie d'être remplacée par le règlement 2016/679 (ci-après, « le règlement »). Ce dernier, approuvé par les co-législateurs le 27 avril 2016 sur la base de l'article 16 TFUE[4], sera en effet pleinement applicable en mai 2018 à l'issue d'une période de transposition de deux ans[5].

En ce qui concerne les transferts des données de l'Union à des pays tiers, le nouveau règlement ne s'éloigne, toutefois, pas des principes fondateurs de la directive 95/46/CE. Afin de concilier, d'une part, le haut niveau de protection des données personnelles voulu par le Traité UE surtout après l'entrée en vigueur du Traité de Lisbonne (articles 8 de la Charte et 16 TFUE) avec, d'autre part, la nécessité dans un monde toujours plus interconnecté de permettre les transferts internationaux, y compris vers des systèmes différents de celui de l'Union européenne (et souvent très diffèrent de celui-ci), l'article 25 de la directive et, dans les mêmes termes, l'article 45 du règlement, subordonnent ces transferts à une série de conditions. Tout d'abord, les transferts sont permis vers des États tiers assurant un niveau de protection « adéquat » qui, selon la Cour de justice dans l'arrêt *Schrems*[6], doit être entendu comme « substantiellement équivalent » à celui garanti dans l'Union européenne[7]. Ce niveau de protection est constaté par une décision de la Commission (dite d'adéquation) après un avis des autorités nationales de protection des données réunies au sein du groupe de travail dit de l'« Article 29 » et à la suite d'une procédure de comitologie requérant un vote favorable des représentants des États membres[8]. En l'absence d'un tel niveau de protection et en vertu des articles 26 de la directive et 46-47 et 49 du règlement, les transferts vers des pays « non adéquats » peuvent s'opérer sur la base d'instruments alternatifs à la décision d'adéquation, comme, par exemple, lorsque les entreprises en cause utilisent des clauses contractuelles type approuvées au niveau de l'Union européenne et prévoyant un certain nombre de « garanties appropriées », ou lorsque la personne concernée a

(*) L'auteur est Professeur agrégé de droit de l'Union européenne à l'Université de Milano-Bicocca, Italie. Elle peut être contactée à l'adresse suivante : serena.crespi@unimib.it. (1) http ://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf (8 juillet 2016) (2) Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, *J.O.* L 207 du 1er août 2016, pp. 1 et s. (3) Directive du Conseil et du Parlement européen, du 24 octobre 1995, *J.O.*, L 281, p. 31. (4) *J.O.*, L 119, p. 1. En doctrine, voy. notamment E. Degrave, « La protection des données à caractère personnel enfin reformée », *J.D.E.*, 2016, pp. 136 et s. À la même date, le législateur de l'Union européenne a également adopté la directive 2016/680 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, *J.O.*, L 119, pp. 89 et s., Cette directive abroge et remplace la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008, *J.O.*, L 350, pp. 60 et s. (5) Article 99 du règlement 2016/679/UE. (6) C-362/14, ECLI:EU:C:2015 :650, point 74. *Ex multiis*, A. Debet, « L'invalidation du *Safe Harbor* par la C.J.U.E. : tempête sur les transferts de données vers les États-Unis », *La Semaine juridique*, éd. gén. 2015, pp. 2108 et s. ; M. Griguer, « Invalidation du *Safe Harbor* : quel impact pour les entreprises ? », Cahiers dr. entreprise, 2015, pp. 70 et s. ; M. Quéméner, « La fin du *Safe Harbor* au nom de la protection des données personnelles : enjeux et perspectives », *Droit de l'immatériel : informatique, médias, communication*, 2015, pp. 22 et s. ; E. Derieux, « Encadrement du transfert de données personnelles de l'Union européenne vers les États-Unis d'Amérique », *ibidem*, pp. 25 et s. ; Y. Padova, « Le *Safe Harbor* est invalide - Et après ? Analyse des fondements de l'arrêt de la C.J.U.E. et de ses conséquences » *ibidem*, pp. 50 et s. (7) Cette interprétation jurisprudentielle a été depuis codifiée par le législateur de l'Union européenne au considérant 104 du nouveau règlement : « [...] Lors de l'adoption, à l'égard d'un territoire ou d'un secteur déterminé dans un pays tiers, d'une décision d'adéquation, il y a lieu de tenir compte de critères clairs et objectifs, telles que les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et de la législation en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union, en particulier quand les données à caractère personnel sont traitées dans un ou plusieurs secteurs spécifiques. Plus particulièrement, le pays tiers devrait assurer un contrôle indépendant effectif de la protection des données et prévoir des mécanismes de coopération avec les autorités de protection des données des États membres, et les personnes concernées devraient se voir octroyer des droits effectifs et opposables ainsi que des possibilités effectives de recours administratif et juridictionnel » (8) À ce jour, la Commission a adopté 11 décisions d'adéquation (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm [8 juillet 2016]).

Vie du droit

donné son consentement au transfert, ou encore lorsque le transfert est nécessaire pour des motifs importants d'intérêt public.

Le *Privacy Shield* se présente comme une décision d'adéquation, bien que d'une nature et d'une portée particulière. Du fait de l'absence aux États-Unis d'un instrument législatif général et horizontal en matière de vie privée comparable à la directive ou au règlement — le droit américain en la matière relève davantage de règles sectorielles couvrant la protection des données dans certains domaines sensibles comme le crédit ou le secteur médical — et d'une autorité de contrôle semblable à celles existant dans chaque État membre de l'Union européenne, la décision de la Commission ne propose pas de constater l'adéquation du système des États-Unis dans son ensemble, mais subordonne la reconnaissance de l'adéquation au respect par les entreprises américaines désirant profiter de la libre circulation des données de l'Union européenne d'exigences supplémentaires par rapport à celles s'appliquant en droit américain (en termes, par exemple, de transparence et information des utilisateurs UE, de limitation des finalités du traitement, de droits de l'individu d'obtenir l'accès à ses données et d'exiger le cas échant leur correction).

Le système du *Privacy Shield* repose ainsi sur un mécanisme proche de l'auto-certification auquel les entreprises américaines décident d'adhérer volontairement. Néanmoins, une fois que ces dernières déclarent y adhérer, elles sont tenues par ces règles de manière contraignante et leur violation peut être sanctionnée notamment par la *Federal Trade Commission*. En d'autres termes, sans le modifier, cet instrument complète le système américain.

2 L'importance de l'adoption du *Privacy Shield*

L'adoption du *Privacy Shield* était particulièrement attendu, car il vise à combler le vide juridique créé par l'annulation, totale et *ex tunc*, de la précédente décision d'adéquation UE/US (*Safe Harbor*[9]) par la Cour de justice dans l'arrêt *Schrems* pour incompatibilité avec l'article 8 (droit à la protection des données personnelles) de la Charte des droits fondamentaux UE.

L'annulation, sans aucune période de transition, de l'outil traditionnellement utilisé par de nombreuses entreprises au cours des quinze dernières années (plus de 4.000 d'entre elles y avaient adhéré entre 2000 et 2015) pour transférer des données personnelles outre-Atlantique a naturellement suscité de nombreuses préoccupations, notamment dans le monde économique[10], exigeant une réponse rapide de la Commission. Immédiatement après l'invalidation du *Safe Harbor*, celle-ci a alors intensifié les négociations avec les autorités américaines, en réalité déjà entamées avant le prononcé de l'arrêt *Schrems*. Dès 2013, la Commission avait, en effet, identifié certaines faiblesses et insuffisances du système pouvant compromettre le niveau de protection assuré par ladite décision d'adéquation[11] et avait alors initié des pourparlers avec les États-Unis en vue du renforcement du *Safe Harbor*.

Les points critiques relevés par la Commission concernaient aussi bien la manière dont cet instrument était administré par les autorités américaines (notamment insuffisance de contrôle par le département du Commerce de la manière dont les entreprises se conformaient aux conditions *Safe Harbor*), que des développements de la législation et des pratiques US hors *Safe Harbor*, mais qui avaient fini par avoir des conséquences sur le niveau de protection censé être assuré par celui-ci. En particulier, à la suite des révélations Snowden sur les programmes de surveillance américains, se posait la question d'un accès qu'on a pu décrire comme de masse et indifférenciée des agences de renseignement US aux données des utilisateurs UE transférées vers les États-Unis dans le cadre d'opérations commerciales. C'est précisément sur ce point que se concentre la position d'invalidité de la Cour : selon les juges de Luxembourg, dans les arrêts *Digital Rights Ireland*[12] et *Schrems*, l'accès des autorités publiques tant des États membres (*Digital Rights Ireland*) que des pays tiers (*Schrems*) devrait n'avoir lieu que dans la mesure où cela est strictement nécessaire et proportionné par rapport aux objectifs, par exemple de sécurité nationale, poursuivis. Etant donné que le *Safe Harbor* manquait « de toute constatation quant à l'existence dans le système américain de garanties, limites et recours en matière d'accès des autorités publiques aux donnée transférées pour des motifs commerciaux depuis l'Europe vers les États-Unis »[13], la Cour a alors conclu à l'annulation de ladite décision.

Compte tenu de la nature de ces motifs d'invalidité, l'adoption d'une nouvelle décision d'adéquation paraît d'autant plus importante, que seul cet instrument est susceptible d'apporter des réponses aux critiques de la Cour. Les autres instruments de transfert prévus par la législation UE, notamment ceux de type contractuel, semblent, en effet, ne pouvoir aucunement limiter des possibles violations des règles en matière de protection des données d'origine étatique ou publique comme dans le cas de programmes de renseignement étrangers. Cette problématique est d'ailleurs au cœur d'une nouvelle affaire opposant à nouveau, devant les juridictions irlandaises, M. Schrems et Facebook, mais cette fois au sujet de l'utilisation des clauses contractuelles « types » pour des transferts de données vers les États-Unis.[14] En d'autres termes, la décision d'adéquation constitue l'outil le plus complet, simple et moins coûteux pour effectuer les transferts de données UE vers des pays tiers.

3 Les différences entre le *Safe Harbor* de 2000 et le *Privacy Shield* de 2016

Selon la Commission, le *Privacy Shield* se présente comme un instrument substantiellement renforcé par rapport au *Safe Harbor* et conforme aux exigences posées par la Cour de justice dans l'arrêt *Schrems*. Par rapport au *Safe Harbor* — qui, comme relevé par la Cour[15], contenait une motivation très réduite et lacunaire — la nouvelle proposition se caractérise, tout d'abord, par sa motivation particulièrement détaillée.

L'effort de la Commission pour répondre aux critères énoncés par la Cour ne s'est toutefois pas limité uniquement à la dimension formelle de la décision, mais s'étend à ses aspects substantiels. Le

(9) Décision 2000/520 de la Commission, du 26 juillet 2000, *J.O.*, L 215, p. 7. **(10)** Communication de la Commission, du 16 octobre 2015, COM(2015)566. **(11)** Communication de la Commission, du 27 novembre 2013, COM(2013)846. **(12)** C-293/12 et C-594/12, ECLI:EU:C:2014 :238. **(13)** Arrêt *Schrems*, points 88 et 89. **(14)** http://www.reuters.com/article/us-eu-privacy-facebook-idUSKCN0YG2DL (9 juillet 2016). **(15)** Arrêt *Schrems*, points 79-98.

Privacy Shield relève, en premier lieu, le niveau général des engagements applicables aux entreprises américaines qui souhaitent importer des données UE, rapprochant ainsi davantage ces obligations des standards européens. Sont, par exemple, renforcées les obligations des entreprises relatives à l'information des particuliers (conditions de notification) ou la possibilité pour ces derniers de s'opposer au traitement des données UE à des fins autres que celles pour lesquelles elles ont été collectées (conditions de choix). En outre, la décision limite les cas dans lesquels les entreprises des États-Unis peuvent effectuer des transferts de données à des tiers (condition de transfert ultérieur) et assouplit les conditions dans lesquelles la responsabilité de ces entreprises peut être mise en cause par les particuliers européens en cas de tels transferts[16].

En deuxième lieu, afin de remplir les conditions énoncées au point 81 de l'affaire *Schrems* selon lesquelles un système fondé sur l'auto-certification, comme le demeure le *Privacy Shield*, est admissible seulement à la condition qu'il soit soumis à des « mécanismes efficaces de détection et de contrôle permettant d'identifier et de sanctionner » les violations des règles applicables, le nouveau régime prévoit un système de contrôle plus strict du respect des engagements souscrits par les entreprises membres du *Privacy Shield*. Cela passe, en particulier, par un traitement mieux encadré, et qui devrait alors se révéler plus effectif, d'éventuelles plaintes introduites par des utilisateurs européens, qu'il s'agisse de l'obligation pour les entreprises d'y répondre dans un délai de 45 jours[17] ou de l'accès gratuit des individus européens aux mécanismes extra-judiciaires de règlement des différends[18]. Ces derniers peuvent également se tourner vers leur autorité nationale de protection des données, qui devra coopérer avec la *Federal Trade Commission* et le département du Commerce américain pour assurer un traitement efficace de la plainte[19]. Enfin, si un particulier considère que les autorités américaines n'ont pas répondu de façon satisfaisante à sa plainte, il pourra saisir, y compris avec l'aide de son autorité nationale, un tribunal arbitral spécifique au *Privacy Shield*, dont la décision sera contraignante et exécutoire[20]. En dehors même des cas de plaintes individuelles, les autorités américaines se sont engagées à instituer un système de vérification continu du respect des engagements de la part des entreprises du *Privacy Shield*, passant ainsi du système de contrôle essentiellement réactif du *Safe Harbor* à un système plus (pro)actif[21].

En troisième lieu, contrairement à la décision *Safe Harbor* qui — comme l'a relevé l'arrêt *Schrems*[22] — ne comportait aucune constatation quant aux limitations régissant l'accès aux données UE par les autorités US pour des raisons d'intérêt général comme la sécurité nationale, le *Privacy Shield* contient des dispositions précises à cet égard. Se fondant sur les réformes des programmes de surveillances menées depuis 2014 par l'administration Obama (*Presidential Policy Directive 28*), les autorités américaines ont ainsi fourni, pour la première fois, des garanties écrites sur les limites, sauvegardes et mécanismes de contrôle s'appliquant aux conditions d'accès et d'utilisation des données US par les agences de renseignement nord-américaines[23]. Ces limitations devraient être en mesure d'empêcher l'accès massif et indifférencié aux données personnelles transférées depuis l'Union européenne. Les autorités américaines se sont également engagées à introduire un mécanisme de recours (administratif) spécifique en la matière, à travers la création d'un *Ombudsperson*[24]. Ce nouvel organe, bien que créé au sein du département d'État US, sera indépendant des agences de renseignement américaines et traitera les plaintes des individus UE relatives à l'accès à leurs données pour raisons de sécurité nationale. Il devra notamment assurer qu'un remède approprié est apporté en cas d'irrégularité et fournir une réponse au plaignant. C'est la première fois qu'un tel mécanisme de traitement des plaintes individuelles est introduit au niveau international, ces questions relevant normalement des relations purement intergouvernementales.

Enfin, le *Privacy Shield* sera soumis à une procédure de réexamen conjoint annuel afin de contrôler le respect des engagements souscrits tant par les entreprises que par les autorités publiques américaines, y compris en ce qui concerne les conditions auxquelles celles-ci peuvent avoir accès aux données transférées aux États-Unis[25]. L'introduction de ce mécanisme d'évaluation du fonctionnement du *Privacy Shield* répond à l'exigence posée par la Cour dans l'arrêt *Schrems* selon laquelle, étant donné que « le niveau de protection assuré par un pays tiers est susceptible d'évoluer », « il incombe à la Commission, après l'adoption d'une décision [d'adéquation] de vérifier de manière périodique si la constatation relative au niveau de protection adéquat assuré par le pays tiers en cause est toujours justifiée en fait et en droit »[26]. Afin de souligner l'importance de la dimension « dynamique » de la décision d'adéquation, la Commission a expressément lié les résultats de cette évaluation annuelle à un possible déclenchement de la procédure de suspension de l'arrangement, notamment si l'évaluation devait révéler un niveau insuffisant de conformité aux règles du *Privacy Shield* de la part des entreprises ou des autorités des États-Unis ou si ces autorités ne devaient pas répondre de manière satisfaisante aux questions soulevées par leurs interlocuteurs de l'Union européenne[27]. Ce lien entre la procédure de réexamen et la procédure de suspension devrait, à tout le moins, inciter au respect des exigences posées par le *Privacy Shield*, également à la lumière du fait que les résultats de cette évaluation seront communiqués au Parlement et au Conseil.

L'arrangement décrit ci-dessus a été partiellement modifié en raison des avis, pour le moins mitigé, rendu entre avril et mai 2016 sur le *Privacy Shield* par le groupe de travail « Article 29 »,[28] le Parlement européen[29] et le Contrôleur européen de la protection des données[30]. Afin de répondre à ces observations, en avril 2016 la Commission a rouvert les négociations avec les États-Unis sur certains éléments du *Privacy Shield.* Ces discussions ont mené à des améliorations et des clarifications portant sur les règles s'appliquant tant aux entreprises (à travers notamment un renforce-

(16) Section II « Principes », Annexe II. **(17)** Considérant 44 de la décision de la Commission et *lit.* i), point d), section 11 « Résolution des litiges et application des décisions » de l'Annexe II. **(18)** Considérant 45 de la décision de la Commission et principe « Voies de recours, application et responsabilité ». **(19)** Considérant 48 de la décision de la Commission et annexe I-1. **(20)** Annexe I-2 — Modèle d'arbitrage. **(21)** Considérants 34, 36 et 37 de la décision de la Commission et annexe I-1. **(22)** Arrêt *Schrems*, points 92-95. **(23)** Considérants 67-90 de la décision de la Commission et annexe VI. **(24)** Considérants 116-122 de la décision de la Commission et annexe III. **(25)** Considérants 145-149 de la décision de la Commission et annexe II-1. **(26)** Arrêt *Schrems*, point 76. **(27)** Considérants 150-152 de la décision de la Commission. **(28)** http:ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (9 juillet 2016). **(29)** http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0233+0+DOC+PDF+V0//FR (9 juillet 2016) **(30)** https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf (9 juillet 2016).

ment des obligations s'appliquant en cas de transferts ultérieurs ou en matière de limites à la durée de conservation des données) qu'à la question de l'accès des autorités publiques des États-Unis aux données UE, y compris en précisant certains aspects du statut et du fonctionnement de l'*Ombudsperson*.

4 La compatibilité du *Privacy Shield* avec le droit de l'Union européenne

Tout en contenant des améliorations indéniables par rapport au *Safe Harbor*, il est difficile de prédire si le *Privacy Shield* est en mesure de surmonter le test de compatibilité avec l'article 8 de la Charte. Ce régime, tout comme le *Safe Harbor* et bien qu'il complète certains aspects du système des États-Unis, se fonde en effet sur celui-ci et n'élimine donc pas certaines différences « structurelles » entre les systèmes de protection des données des deux côtes de l'Atlantique.

Dans ces conditions, l'issue d'un recours — dont l'introduction semble probable — contre la nouvelle décision d'adéquation, dans le cadre d'un renvoi préjudiciel ou d'un recours d'annulation, dépendra avant tout de l'interprétation qui sera donnée par la Cour à la notion d'« adéquation », entendue désormais comme « équivalence substantielle ».

Les possibilités d'une issue positive sembleraient, en effet, plutôt réduites si la Cour devait attribuer au standard de « l'équivalence substantielle », qu'elle a posé dans *Schrems* et qui a été entretemps repris par le législateur européen dans le nouveau règlement, une interprétation s'approchant de la « quasi identité ». En revanche, les chances de survie de la décision devant les juges européens seraient plus grandes si ce test était interprété dans une perspective plus fonctionnelle consistant à vérifier si dans son ensemble le système étranger assure un niveau de protection adéquat par rapport aux standards européens. À notre avis, seul ce type d'interprétation semblerait pouvoir permettre de « naviguer » entre des systèmes protégeant les données personnelles de manière différente, tout en assurant un niveau élevé de protection.

L'issue d'un éventuel recours contre le *Privacy Shield* dépendra également du type de contrôle qu'exercera la Cour sur la nouvelle décision. Il est clair qu'une décision d'adéquation donne lieu à des appréciations complexes de la part de la Commission des règles et du fonctionnement d'un système juridique étranger. On pourrait alors s'attendre à ce que, comme c'est le cas dans d'autres domaines du droit de l'Union européenne (notamment en droit de la concurrence), une certaine marge d'appréciation soit reconnue à la Commission, marge d'appréciation à laquelle correspond un contrôle plus restreint du juge de l'Union européenne. Et certains éléments de l'arrêt *Schrems* sembleraient confirmer cette lecture. L'invalidation du *Safe Harbor* se fonde, avant tout, sur l'absence dans cette décision de « toute constatation » quant à l'existence dans le système américain de garanties, limites et recours en matière d'accès des autorités publiques aux donnée UE. Il convient également d'ajouter un certain embarras de la Commission qui — comme l'a relevé la Cour[31] — avait déjà elle-même soulevé, dans sa communication de 2013, des doutes sur le caractère nécessaire et proportionné de l'ingérence des programmes de surveillance américains à des fins de sécurité nationale dans le droit fondamental à la protection des données UE. En d'autres termes, le *Safe Harbor* aurait été essentiellement entaché d'un défaut de motivation, doublé en quelque sorte d'une potentielle contradiction de motifs. Si cette lecture se révélait correcte, le *Privacy Shield* pourrait alors passer l'examen de la Cour, car il apparaît, sous cet angle, radicalement différent du *Safe Harbor*. En particulier, en ce qui concerne l'accès des autorités américaines aux données UE, le *Privacy Shield* contient, comme on l'a déjà relevé, de nombreux développements analysant les garanties, les limites et les voies de recours en la matière.

Cela étant, il ressort aussi de la jurisprudence récente de la Cour de justice de l'Union européenne[32] que, lorsque les institutions de l'Union européenne interviennent dans une matière, comme la protection des données, relevant d'un droit fondamental, leur pouvoir d'appréciation est en principe réduit et est alors soumis à un contrôle strict de la Cour. Si cette ligne interprétative devrait être appliquée à un recours concernant le *Privacy Shield*, cela signifierait probablement que la Cour devrait se livrer — maintenant que la décision de la Commission inclut une riche motivation en la matière — à un examen concret du contenu des règles américaines sur l'accès des autorités publiques aux données personnelles et à l'évaluation de la conformité de ces règles à des principes du droit européen tels que les principes de proportionnalité et de nécessité. Bien que, dans l'affaire *Schrems*, le juge européen ait donné certaines indications quant à l'interprétation de ces principes aux règles applicables en matière d'accès pour raisons de sécurité nationale[33], l'absence de toute motivation dans le *Safe Harbor* lui a permis d'éviter de se livrer à un examen direct du droit des États-Unis. Il est intéressant de noter à cet égard que, de manière tout à fait inhabituelle, le président de la Cour a, au lendemain du prononcé de l'affaire *Schrems*, concédé une interview au *Wall Street Journal* dans laquelle il se défendait de toute portée « extraterritoriale » de l'arrêt, en affirmant que celui-ci n'avait exprimé aucun jugement sur le système US, mais uniquement sur la décision de la Commission[34]. Subtile distinction qui pourrait être plus difficile de maintenir maintenant que le *Privacy Shield* contient une analyse détaillée de ce droit.

Conclusion

Bien que reflétant certaines spécificités du système américain, l'adoption du *Privacy Shield* présente un intérêt allant bien au-delà de la seule question des transferts transatlantiques de données. Il s'agit, en effet, de la première décision d'adéquation prise par la Commission après l'arrêt *Schrems*, arrêt dont de nombreux éléments ont été entre temps codifiés dans la réforme de la législation européenne sur la protection des données personnelles adoptée en avril dernier. Les exigences que cet instrument pose tant du point de vue substantiel (par exemple, en matière d'accès des autorités publiques aux données pour motifs de sécurité nationale) que procédural (par exemple, mécanisme de réexamen

(31) Arrêt *Schrems*, point 90. **(32)** Arrêts *Schrems*, point 78 ; *Digital Rights Ireland*, points 47-48. **(33)** Arrêt *Schrems*, points 91-95. **(34)** www.wsj.com/articles/european-court-chief-defends-decision-to-strike-down-data-transfer-agreement-1444768419 (8 juillet 2016).

périodique) constituent alors d'importants précédents pour de possible futures décisions d'adéquation concernant d'autres pays tiers. À travers ces éléments, le *Privacy Shield* apporte une réponse pragmatique à la jurisprudence de la Cour, s'efforçant de concilier haut niveau de protection des données personnelles en cas de transfert hors de l'Union européenne et nécessaire prise en compte de la diversité des systèmes de protection de ces données dans le monde. À une époque où les échanges de données sont toujours plus cruciaux pour des raisons non seulement commerciales mais aussi de sécurité et, plus généralement, d'interactions sociales, il ne fait aucun doute que la recherche de cet équilibre demeure une question centrale au sujet de laquelle la Cour sera probablement appelée à se prononcer à nouveau prochainement.