Flux transfrontières de données et exigence de protection adéquate à l'épreuve de la surveillance de masse

De Terwangne, Cécile; GAYREL, Claire

Published in:
Cahiers de droit européen

Publication date:
2017

Document Version
le PDF de l'éditeur

DOCTRINE

FLUX TRANSFRONTIÈRES DE DONNÉES ET EXIGENCE DE PROTECTION ADÉQUATE À L'ÉPREUVE DE LA SURVEILLANCE DE MASSE. LES IMPACTS DE L'ARRÊT *SCHREMS*

PAR

Cécile DE TERWANGNE (1) et Claire GAYREL (2)

Protection des données à caractère personnel — Flux transfrontières de données — Protection adéquate — Droits fondamentaux — Surveillance de masse — État de droit — Privacy Shield

Dans son retentissant arrêt Schrems*, la Cour de justice a établi que pour qu'un État tiers puisse être reconnu comme garantissant une protection adéquate des données à caractère personnel arrivant sur son territoire en provenance de l'UE, il fallait que cet État offre une protection des libertés et droits fondamentaux substantiellement équivalente à celle instaurée sur le sol européen par la directive 95/46 lue à la lumière de la Charte. La présente contribution s'attache à dessiner les nouveaux contours de l'exigence de protection adéquate, tels qu'ils découlent de cette jurisprudence et du nouveau règlement général sur la protection des données (RGPD). L'analyse porte ensuite sur le niveau de protection offert par le Privacy Shield négocié avec les États-Unis au regard de ce nouveau standard. Enfin, les auteures envisagent les conséquences que ce nouveau standard pourrait avoir au-delà des décisions d'adéquation que la Commission peut adopter à l'égard d'un État tiers ou d'une organisation internationale, et suggèrent un renouvellement de l'ensemble de la politique européenne des flux transfrontières.*

In its landmark Schrems *decision, the Court of justice has established that in order to be considered as providing an adequate protection of personal data*

(1) Cécile de Terwangne est professeur à la Faculté de Droit de l'Université de Namur et directrice de recherches au CRIDS.

(2) Claire Gayrel, précédemment chercheuse au CRIDS, est juriste auprès du Contrôleur européen de protection des données (CEPD). Les opinions exprimées dans cet article appartiennent exclusivement à son auteure et ne représentent en aucun cas celles du CEPD.

transferred from the Union, a third State should ensure a level of protection of fundamental rights and freedoms essentially equivalent to that guaranteed within the European Union by virtue of directive 95/46 read in the light of the Charter. The present contribution addresses this renewed requirement of adequate protection, as derived from the case-law of the Court and from the General Data Protection Regulation (GDPR). The Privacy Shield is then analysed in the light of this new standard. Finally, the authors address the consequences of this standard beyond adequacy decisions adopted by the Commission with respect to third States or international organizations, and suggest a renewal of the whole transborder data flow policy.

Introduction (3)

Les données à caractère personnel (4) bénéficient d'une protection spécifique au sein de l'Union européenne (5). La vie connectée d'aujourd'hui et l'intensification toujours plus grande des échanges électroniques de données dans les contextes économiques, sociaux, politiques et privés conduisent à ce que ces données ne restent pas confinées à l'intérieur du territoire européen. Elles sont appelées à franchir les frontières et à sortir ainsi de leur zone de protection (6). Le législateur européen, soucieux d'assurer la continuité du régime de protection au-delà des frontières, a posé comme principe que les données personnelles ne pouvaient faire l'objet de transferts que vers des pays qui assurent « un niveau de protection adéquat » (7).

(3) Le présent article a été rédigé en tenant compte des informations disponibles jusqu'en février 2017.

(4) Soit toute information se rapportant à un individu identifié ou identifiable.

(5) Cette protection est assurée aujourd'hui par 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, *J.O.C.E.*, n° L 281, 23 novembre 1995. À partir du 25 mai 2018, elle découlera du règlement (UE) n° 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 (règlement général sur la protection des données ou RGPD).

(6) La zone protégée couvre en fait les 28 États de l'Union européenne auxquels s'ajoutent les 3 États de l'Espace économique européen : la Norvège, le Lichtenstein et l'Islande.

(7) Art. 25 de la directive 95/46. Ce principe est repris dans les mêmes termes dans le règlement général sur la protection des données, son article 45 précisant toutefois que ce niveau de protection pouvait être offert par « [un] pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou [une] organisation internationale ».

Entre 2000 et 2015, les échanges de données à caractère personnel de l'Union européenne vers les États-Unis ont pu être réalisés conformément à cette exigence de niveau de protection adéquat, grâce à la « sphère de sécurité (*Safe Harbor*) » mise en place par les deux partenaires (8). Cette sphère de sécurité était une construction juridique originale, réconciliant l'approche européenne de la question qui lie celle-ci à un enjeu de droits fondamentaux et l'approche américaine qui y voit d'abord un aspect de la vie économique et des marchés. Le résultat a débouché sur un système co-régulatoire, dans lequel une série de principes de protection ont été établis par les autorités mais auxquels les acteurs économiques américains pouvaient choisir de souscrire, se soumettant par là au contrôle de leur respect de ces contraintes librement consenties. Tous ceux qui s'engageaient à respecter les principes édictés entraient dans la sphère de sécurité et pouvaient dès lors recevoir sans entrave des données personnelles en provenance de l'Union européenne. Cette formule a séduit des milliers de destinataires américains de données européennes, parmi lesquels Facebook, Google, Amazon, Apple, Coca-Cola, Deloitte, Gallup, McKinsey, Boeing, Airbnb, Hilton, Tupperware, etc. (9).

Par son arrêt *Schrems* du 6 octobre 2015 (10), la Cour de justice a mis un terme spectaculaire à cette situation juridiquement sécurisée et efficace pour les acteurs économiques européens et américains. Ce sont les révélations d'Edward Snowden sur les pratiques de surveillance généralisée de l'Agence de Sécurité Nationale (NSA — *National Security Agency*) qui sont à l'origine de ce formidable coup d'arrêt qui a beaucoup agité l'industrie du numérique. Cette affaire *Schrems contre Data Protection Commissioner* soulevait la question du niveau de protection conféré aux données transférées depuis l'Europe vers les États-Unis dans le cadre du *Safe Harbor* si l'on prenait en considération le sort réservé aux données au vu des activités de la NSA. Pouvait-on encore parler de protection adéquate ?

(8) Décision 2000/520/CE de la Commission européenne, du 26 juillet 2000, conformément à la directive 95/46, 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, *J.O.C.E.*, n° L 215, p. 7.

(9) Sur l'importance de cet instrument dans les transferts de données transatlantiques, voy. J. P. Meltzer, « Examining the EU Safe Harbor decision and impacts for Transatlantic data flows », *The Brookings Institution*, Nov. 3, 2015, www.brookings.edu/research/testimony/2015/11/03-eu-safe-harbor-decision-transatlantic-data-flows-meltzer ; G. Maldoff et O. Tene, « Privacy Shield backgrounder », p. 9, https://iapp.org/resources/article/privacy-shield-backgrounder/.

(10) CJUE (GC), arrêt du 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14, EU:C:2015:650.

La Cour a répondu en apportant un important éclairage sur cette condition de protection adéquate pour libéraliser les flux transfrontières de données. Elle a ainsi estimé que la protection par l'État étranger des libertés et droits fondamentaux devait être « substantiellement équivalente » à celle instaurée sur le sol européen par la directive 95/46 lue à la lumière de la Charte. Au terme de son analyse, la Cour ne dira pas que les États-Unis n'apportent pas une protection substantiellement équivalente, mais plutôt que la décision de la Commission qui constatait l'adéquation de la protection offerte par le *Safe Harbor* n'apporte pas la motivation argumentée de cette constatation. Elle invalidera en conséquence cette décision mettant en place le *Safe Harbor*.

Ce coup de théâtre jurisprudentiel laissera les acteurs économiques dans un grand désarroi et conduira les autorités européennes et américaines à renégocier dans l'urgence un nouvel accord tenant compte des critiques formulées par la Cour. Le *Privacy Shield* (Bouclier de protection des données) a vu le jour en juillet 2016 et six mois plus tard il abrite plus de quinze cents organisations désireuses d'échanger à nouveau des données à travers l'Atlantique de manière juridiquement sécurisée.

Si les excès en matière de surveillance ont ainsi eu une incidence sur l'évaluation du caractère adéquat ou non de la protection offerte par un pays tiers, dans quelle mesure cette jurisprudence fracassante de la Cour de justice ne doit-elle pas dépasser la notion de protection adéquate pour être appliquée aux autres instruments juridiques permettant de transférer des données hors des frontières de l'UE ? En définitive, dans quelle mesure la décision *Schrems* n'oblige-t-elle pas à un renouvellement de la politique européenne des flux transfrontières *dans son ensemble* ?

Dans les pages qui suivent, nous reviendrons en premier lieu sur les nouveaux contours de l'exigence de protection adéquate, tels qu'ils découlent de la jurisprudence de la Cour et du nouveau règlement (I). Nous analyserons ensuite le niveau de protection offert par le *Privacy Shield* au regard de ce nouveau standard (II). Enfin, nous verrons en quoi les conséquences de ce nouveau standard pourraient bien porter leurs effets au-delà des transferts fondés sur une décision d'adéquation et entraîner un renouvellement de l'ensemble de la politique européenne de flux transfrontières (III).

On signalera, avant l'entame de cette analyse, que la présente contribution s'attache aux transferts de données traitées et générées par le secteur privé et susceptibles de faire l'objet d'une surveillance ultérieure et non aux transferts de données entre autorités de police.

I. — Les nouveaux contours de l'exigence de protection adéquate

Dans la décision *Schrems*, la Cour de justice s'est penchée pour la première fois sur l'interprétation de l'article 25, paragraphe 1, de la directive 95/46/EC, relatif à l'exigence de protection adéquate des données personnelles lorsque celles-ci sont transférées dans des pays tiers. La Cour, à cette occasion, a considéré que «l'expression "niveau de protection adéquat" doit être comprise comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la Charte» (11). Cet éclairage apporté par la Cour met l'accent sur les objectifs du droit à la protection des données à caractère personnel, en tant que droit instrumental, au service du respect et du renforcement de l'ensemble des droits fondamentaux (12). À côté du critère «classique» de la protection des données, la Cour consacre le critère, jusqu'ici implicite, de «l'État de droit». Le RGPD, quant à lui, reprend explicitement ce critère dans les éléments devant être pris en considération par la Commission européenne lorsqu'elle évalue le caractère adéquat ou non de la protection offerte par un pays tiers ou une organisation internationale (13).

Bien qu'absents des développements de la Cour dans l'arrêt *Schrems*, nous allons revenir sur les critères de protection des données à caractère personnel dans le cadre de l'évaluation d'adéquation, tels qu'ils découlent de la pratique existante et sont repris dans le nouveau règlement (A). Nous discuterons ensuite du critère de l'État de droit ou de l'exigence de protection substantiellement équivalente des droits fondamentaux (B). Ces deux types de critères dessinent les nouveaux contours de l'exigence de protection adéquate en droit européen de la protection des données à caractère personnel.

A. — Les critères de protection des données à caractère personnel

Ainsi qu'on l'a dit, tant la directive 95/46 que le RGPD exigent que les transferts de données à caractère personnel ne s'effectuent qu'en direction

(11) CJUE (GC), arrêt *Schrems*, précité, points 73 et 96.

(12) A. Rouvroy et Y. Poullet, «The Right to Informational Self-determination and The Value of Self-Development: Reassessing the Importance of Privacy for Democracy», in *Reinventing Data Protection*, Springer, 2009, pp. 45-76.

(13) Art. 45.2, a), du RGPD.

de pays (ou d'organisations internationales (14)) qui assurent « un niveau de protection adéquat » (15). Il est à noter que ces textes ne spécifient pas expressément sur quoi doit porter cette protection. La directive évoque plus loin les cas où la Commission peut constater qu'un pays tiers « assure un niveau de protection adéquat, en raison de sa législation interne ou de ses engagements internationaux, […] en vue de la *protection de la vie privée et des libertés et droits fondamentaux des personnes* » (16). On retrouve cet objectif de protection des droits fondamentaux des personnes concernées dans le RGPD (17). Mais les deux textes évoquent aussi la « protection des personnes » (18) et le règlement ajoute que la Commission peut décider qu'un pays tiers, un secteur déterminé dans un pays tiers, ou une organisation internationale offre un niveau adéquat de protection « des données » (19). La protection adéquate qui doit être assurée au-delà des frontières européennes est donc celle qui est accordée aux personnes concernées, à leurs droits fondamentaux ou à leurs données à caractère personnel.

On verra dans le point suivant que c'est la protection des droits fondamentaux des personnes concernées qui est au cœur des débats soulevés autour de l'affaire *Schrems*. Mais il est clair que l'évaluation de la protection offerte de l'autre côté des frontières européennes doit commencer par porter sur les instruments de protection des données.

La directive ne précise pas les critères qui doivent guider l'évaluation de la protection offerte par un pays tiers. Elle se contente d'énoncer que le caractère adéquat du niveau de protection offert doit s'apprécier au regard de toutes les circonstances relatives à un transfert de données ou à une catégorie de transferts (20). Parmi ces circonstances à prendre en considération figurent la nature des données, la finalité et la durée du traitement envisagé, les pays d'origine et de destination finale. C'est à une approche ouverte que la directive invite en appelant à analyser les règles de droit en vigueur

(14) Les organisations internationales ne sont visées comme destinataires de données que par le RGPD.

(15) Art. 25, paragraphe 1, de la directive 95/46 ; art. 45.1 du RGPD.

(16) Art. 25, paragraphe 6, de la directive 95/46 (c'est nous qui soulignons).

(17) Considérant 102, *in fine*, du RGPD : « Les États membres peuvent conclure des accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales dans la mesure où ces accords n'affectent pas le présent règlement ou toute autre disposition du droit de l'Union et prévoient un niveau approprié de protection des droits fondamentaux des personnes concernées ».

(18) Considérant 56 de la directive 95/46 ; considérant 101 du RGPD.

(19) Considérant 103 du RGPD.

(20) Art. 25, paragraphe 2, de la directive 95/46.

dans le pays tiers en cause, mais également les règles professionnelles et les mesures de sécurité qui y sont respectées (21).

1. — *Les critères du WP 12*

Le Groupe de l'article 29, groupe instauré par la directive 95/46 et rassemblant les représentants des autorités nationales de protection des données, a apporté un éclairage capital sur la portée du caractère adéquat de la protection devant être assurée pour permettre les transferts de données hors Europe. Il ne s'agissait pas en effet de rechercher dans l'État de destination une protection identique à celle mise en place dans l'UE (22). Il a fallu dès lors établir les critères permettant de qualifier un système de protection d'« adéquat » (23). Cet exercice d'identification des principes et règles considérés comme le noyau dur de la protection des données (24) a débouché sur le document n° 12 (WP 12) adopté par le Groupe de l'article 29 (25).

Ce document a servi de base à toutes les études d'adéquation qui ont été effectuées pour permettre à la Commission de faire figurer ou non un État sur sa liste blanche (26) des pays garantissant une protection adéquate et pouvant dès lors recevoir librement les données en provenance de l'Europe.

---

(21) Art. 25, paragraphe 2, de la directive 95/46.

(22) Y. Poullet et B. Havelange (avec la collaboration de M.-H. Boulanger, H. Burkert, C. de Terwangne), *Élaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement des données à caractère personnel*, Étude réalisée pour la Commission européenne, février 1997. Voy. aussi European Commission, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data*, Luxembourg, Office for Official Publications of the EC, 1998.

(23) Le RGPD, quant à lui, tout en reprenant le terme de niveau « adéquat » de protection, ajoute cette précision au considérant 104 : « pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union ». Le régime juridique évalué doit donc présenter un niveau de protection « essentiellement équivalent » au niveau européen, voy. *infra*.

(24) Y. Poullet et B. Havelange, *Élaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement des données à caractère personnel*, *op. cit.* « Ce qui est recherché c'est une similarité fonctionnelle, loin de tout impérialisme européen » (Y. Poullet, « Pour une justification des articles 25 et 26 de la directive 95/46/CE en matière de flux transfrontières et de protection des données », *Communication commerce électronique*, 2003, Chronique n° 29, pp. 10 et 13).

(25) Groupe de l'article 29, Document de travail « Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données », WP 12 adopté le 24 juillet 1998, http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_fr.pdf.

(26) Art. 25, paragraphe 6, de la directive 95/46.

Selon ce document, « toute analyse sérieuse du niveau de protection adéquat doit porter sur les deux éléments fondamentaux suivants : le contenu des règles applicables et les moyens d'assurer leur application efficace ». En effet, outre l'analyse des règles régissant la protection des données dans l'État tiers, il convient de prendre la mesure de l'application de ces règles dans la pratique. Il est donc nécessaire d'examiner non seulement le contenu des règles applicables aux données personnelles transférées vers un pays tiers (point a ci-dessous) mais également le dispositif mis en place pour garantir l'efficacité de ces règles (point b).

a) Règles de contenu (27)

Au titre des règles de contenu fondamentales figure tout d'abord le principe de finalité. Tout transfert de données doit être limité à une finalité spécifique. Les données transférées ne peuvent être utilisées ultérieurement que dans la mesure où cela n'est pas incompatible avec la finalité du transfert.

Le principe de qualité et de proportionnalité des données doit également être présent dans le régime de l'État tiers. Ainsi, ce dernier doit exiger que les données soient adéquates, pertinentes et non excessives au regard des finalités liées au transfert. Elles doivent être exactes et, au besoin, actualisées.

La transparence des traitements de données doit être exigée, conduisant à ce que les personnes physiques soient informées sur les finalités des traitements et sur l'identité du responsable des traitements dans le pays tiers ainsi que sur d'autres aspects dès lors que cela est nécessaire pour assurer un traitement loyal des données. Les personnes concernées doivent aussi se voir reconnaître des droits d'accès à leurs données, de rectification de celles qui sont inexactes et d'opposition au traitement de leurs données.

Le régime juridique de l'État destinataire doit exiger des responsables de traitement qu'ils prennent des mesures de sécurité, sur les plans technique et organisationnel, qui soient appropriées au regard des risques.

Des garanties additionnelles à ces exigences de base doivent être prévues pour les catégories de données dites « sensibles » (celles qui sont répertoriées à l'article 8 de la directive (28)).

Enfin, le système juridique doit apporter des restrictions aux transferts ultérieurs des données qui ne peuvent être autorisés que lorsque le desti-

(27) Groupe de l'article 29, WP 12, *op. cit.*, pp. 6 et 7.

(28) C'est-à-dire les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que les données relatives à la santé et à la vie sexuelle, et les données relatives aux infractions, aux condamnations pénales ou aux mesures de sûreté.

nataire du transfert ultérieur est également soumis à des règles offrant un niveau de protection adéquat.

b) Règles procédurales/d'application

Ces principes doivent être concrètement appliqués dans un pays afin que celui-ci soit reconnu comme offrant une protection adéquate. Aussi, l'évaluation de la protection offerte doit-elle tenir compte du respect des règles dans la pratique (29). Par ailleurs, les personnes concernées doivent être en mesure de faire valoir leurs droits « rapidement et efficacement sans avoir à subir des coûts prohibitifs ». (30) Pour ce faire, il faut qu'il existe une sorte d'instance indépendante qui puisse apporter soutien et assistance aux personnes concernées et qui instruise leurs plaintes. Enfin, l'État destinataire des données doit fournir des voies de recours appropriées à la partie lésée en cas de non-respect des règles : « une instance d'arbitrage indépendante doit pouvoir être saisie permettant le versement d'une indemnisation et, au besoin, l'adoption de sanctions » (31).

2. — *L'officialisation des critères dans le RGPD*

Le règlement énonce désormais expressément les critères qui doivent être pris en compte par la Commission pour évaluer le caractère adéquat ou non de la protection offerte de l'autre côté de la frontière européenne (32). Il est à noter que le règlement envisage que cette évaluation porte non seulement sur la situation d'États tiers (33) mais aussi sur celle d'organisations internationales (telles que le CICR, par exemple, ou l'AMA — l'Agence Mondiale Anti-dopage). En outre, le règlement précise que les constats d'adéquation peuvent être restreints à un territoire (34) ou à un ou plusieurs secteurs déterminés dans le pays tiers. Ce type d'adéquation partielle a en fait déjà

(29) « Aucun système ne peut garantir qu'elles seront respectées à 100 %, mais certains sont meilleurs que d'autres. On reconnaît en général la qualité d'un système à la conscience aiguë qu'ont les responsables du traitement de leurs obligations et les personnes concernées de leurs droits et des moyens de les exercer. L'existence de sanctions efficaces et dissuasives est importante pour garantir ce respect des règles, de même que, bien entendu, les systèmes de vérification directe par les autorités, les commissions de contrôle ou les responsables indépendants chargés de la protection des données » (WP 12, p. 8).

(30) WP 12, p. 8.

(31) *Ibid.*

(32) Art. 45 du RGPD.

(33) Pour rappel, il s'agit d'États tiers à l'UE mais également à l'Espace économique européen.

(34) L'attention de la Commission a ainsi été attirée sur la situation du Québec qui est actuellement toujours l'objet d'analyse.

été reconnu pour le Canada où seule la protection mise en place pour le secteur privé a été estimée adéquate (35).

Les critères énumérés par le règlement pour évaluer le caractère adéquat du niveau de protection comprennent ceux appliqués jusqu'ici et issus du WP 12. Ainsi, l'article 45.2 du règlement invite la Commission à tenir compte des «règles en matière de protection des données, des règles professionnelles et des mesures de sécurité». Le texte ajoute des éléments plus précis comme les règles relatives aux transferts ultérieurs de données à caractère personnel vers un deuxième pays tiers ou vers une autre organisation internationale ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées.

Outre ces éléments issus des règles de contenu vues au point précédent, l'article 45.2 reprend des éléments provenant des règles de procédure vues au même point. Ainsi, le caractère adéquat de la protection dépend des recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées. De même, l'existence d'une ou de plusieurs autorités de contrôle indépendantes chargées d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits entre dans l'évaluation. Sur ce dernier point, que le RGPD met particulièrement en évidence (36), des compléments sont ajoutés par rapport au WP 12 : l'article 45.2, alinéa b, du RGPD précise qu'il est tenu compte de l'existence d'une ou de plusieurs autorités de contrôle indépendantes dans le pays ou au sein de l'organisation destinataire de données (dont le fonctionnement doit être effectif, il ne peut s'agir d'une autorité de façade), chargées, outre d'aider les personnes concernées à exercer leurs droits, d'assurer le respect des règles en matière de protection des données et de les faire appliquer, ainsi que de coopérer avec les autorités de contrôle des autres États membres. Le texte ne fournit pas d'éclairage sur les critères à prendre en compte pour vérifier l'indépendance des autorités en question. Selon nous, il ne s'agit pas d'appliquer aux autorités extérieures les mêmes critères particulièrement stricts d'indépendance que ceux qui ont été énoncés par la Cour de justice pour les autorités européennes

(35) Décision 2002/2/CE de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, *J.O.C.E.*, n° L 2, 4 janvier 2002.

(36) Ce point fait l'objet d'un alinéa autonome (b) du paragraphe 2 de l'article 45 du RGPD.

de protection des données (37). Cette position s'inscrit dans la ligne de la recherche d'une protection hors UE qui soit « essentiellement équivalente » et non identique au régime de l'Union.

On notera en effet que le RGPD complète la notion de niveau adéquat de la protection offerte au-delà des frontières européennes, par des termes empruntés à l'arrêt *Schrems* : le niveau adéquat de protection doit être *essentiellement équivalent* (38) au niveau européen. Ainsi, le considérant 104 précise que « [l]e pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union ». Cela ne signifie pas que le niveau de protection offert par le régime juridique évalué doive être identique au niveau européen (39). Ce qui est recherché à travers la notion de protection *essentiellement équivalente* c'est la continuité du niveau élevé de protection en cas de transfert de données vers un pays tiers (40). Les moyens auxquels ce pays tiers a recours pour assurer la protection peuvent être différents de ceux mis en œuvre au sein de l'Union mais ils doivent s'avérer, en pratique, effectifs (41).

On verra au point B ci-dessous que d'autres critères sont ajoutés par le règlement, liés au respect de l'État de droit, au respect des droits de l'homme et des libertés fondamentales, à la législation relative à la sécurité publique, la défense, la sécurité nationale et le droit pénal. À cela a été ajouté en fin de parcours législatif un critère découlant directement de l'arrêt *Schrems* : l'ampleur de l'accès des autorités publiques aux données à caractère personnel.

(37) CJUE, 9 mars 2010, *Commission c. Allemagne*, aff. C-518/07, EU:C:2010:125 ; CJUE, 16 octobre 2012, *Commission c. Autriche*, aff. C-614/10, EU:C:2012:631 ; CJUE, 8 avril 2014, *Commission c. Hongrie*, aff. C-288/12, EU:C:2014:237.

(38) L'arrêt *Schrems*, au point 73, évoque un niveau de protection qui doit être « substantiellement équivalent » mais la version anglaise de l'arrêt utilise les termes « *essentially equivalent* ». Ce sont ces derniers termes qui sont repris dans la version anglaise du RGPD, cette fois traduits en français par « essentiellement équivalent ». Il n'y a donc aucune différence à voir entre « essentiellement » et « substantiellement ».

(39) « Certes, le terme "adéquat" figurant à l'article 25, paragraphe 6, de la directive 95/46 implique qu'il ne saurait être exigé qu'un pays tiers assure un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union » (CJUE (GC), 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14, EU:C:2015:650, point 173).

(40) CJUE, arrêt *Schrems*, précité, points 172 et 173.

(41) *Ibid.*

B. — L'exigence de protection substantiellement équivalente des droits fondamentaux ou le critère de l'État de droit

Tandis que la régulation des flux transfrontières de données à caractère personnel est longtemps restée une matière très politique, où la marge d'appréciation de la Commission était importante en raison des enjeux économiques considérables qu'elle soulève, le critère de l'État de droit, implicite jusqu'alors (42), prend aujourd'hui toute sa signification. La Cour a considéré que l'exigence de protection adéquate de l'article 25, paragraphe 1, de la directive 95/46 implique un niveau de protection des libertés et droits fondamentaux *substantiellement équivalent* à celui garanti au sein de l'Union *en vertu de la directive 95/46, lue à la lumière de la Charte*. Selon nous, ce n'est pas l'exigence de protection substantiellement équivalente de l'ensemble des droits et libertés fondamentaux tels qu'ils sont protégés par la Charte qui est visée ici. Ce que la Cour exige est une protection substantiellement équivalente des droits et libertés fondamentaux qui sont susceptibles d'être directement concernés, voire compromis par des activités de traitement de données à caractère personnel.

Certains droits et libertés fondamentaux, autres que le droit à la protection des données à caractère personnel, ont donc vocation à faire partie intégrante de l'exigence d'adéquation. Nous pensons naturellement au droit à la protection de la vie privée, au droit à la liberté d'expression, au droit à la non-discrimination et au droit à une protection juridictionnelle effective (43). Mais l'exigence de protection substantiellement équivalente ne s'applique pas, selon nous, pour d'autres droits et libertés fondamentaux qui n'entretiendraient aucun lien avec des activités de traitement de données. En effet, soulignons que la Cour n'a fait aucune référence à l'application de la

(42) En tant qu'auteures d'une dizaine d'études d'adéquation réalisées à la demande de la Commission européenne entre 2000 et 2012, nous pouvons affirmer que ce critère de l'état de droit était, dans toute la mesure du possible et des moyens impartis, pris en compte dans nos analyses.

(43) Sur le droit à une protection juridictionnelle effective, la Cour a été très explicite au paragraphe 95 de l'arrêt *Schrems*, précité : « une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte. En effet, l'article 47, premier alinéa, de la Charte exige que toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés, ait droit à un recours effectif devant un tribunal dans le respect des conditions prévues à cet article. À cet égard, l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence d'un État de droit […] ».

peine de mort dans certains États fédérés alors qu'il s'agit pourtant d'une des divergences les plus fondamentales de protection du droit à la vie entre les systèmes européen et américain des droits de l'homme.

Le RGPD, quant à lui, dresse une liste d'éléments que la Commission est tenue de prendre en compte pour établir et motiver une décision d'adéquation : « [l]orsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tient compte, en particulier, des éléments suivants : a) l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation […] ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées […] b) les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel » (44). De ces éléments nous retenons qu'une attention particulière doit être portée aux engagements internationaux de l'État, aux ingérences des autorités publiques dans les domaines régaliens et plus largement au respect de l'État de droit.

Soulignons que le règlement insiste sur la « mise en œuvre » des législations, ce qui implique de prendre en compte le niveau de protection des droits et libertés conférés *en théorie* et *en pratique* dans l'État tiers concerné.

Selon nous, l'exigence de protection substantiellement équivalente des droits fondamentaux telle qu'exprimée dans l'arrêt *Schrems* et le GDPR demande d'examiner la réception des engagements internationaux en droit interne (1), le respect de « garanties essentielles » en matière de surveillance (2) et de dresser un portrait général de l'État de droit et de l'état de la démocratie dans le pays évalué (3).

1. — *Réception des engagements internationaux en droit interne*

L'examen des engagements internationaux de l'État constitue un critère incontournable. Il permet de connaître les engagements pris par l'État en

(44) Art. 45.1 du RGPD.

matière de droit à la protection des données, mais aussi en matière de droits fondamentaux plus largement. La question de savoir si un État a ratifié des instruments internationaux de protection des droits de l'homme tels que le Pacte international relatif aux droits civils et politiques (45) offre un premier outil de mesure du degré d'engagements de l'État à respecter les droits et libertés directement concernés par les activités de traitement de données. Le RGPD fait aussi référence à la participation du pays tiers ou de l'organisation internationale à des systèmes multilatéraux ou régionaux, notamment en ce qui concerne la protection des données à caractère personnel. La Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (46) et son protocole additionnel (47), qui constitue à ce jour le seul instrument international (48) contraignant en matière de protection des données, devrait compter parmi les engagements internationaux les plus pertinents pour tout État candidat à l'adéquation (49). Parmi les engagements internationaux non contraignants qui devraient aussi être pris en compte, il y a les lignes directrices relatives à la vie privée (50) de l'Organisation de Coopération et de Développement Économiques (OCDE) ou le *Privacy Framework* de l'*Asia Pacific Economic Cooperation* (APEC) (51).

Toutefois, la portée de ces engagements, en particulier les engagements contraignants, et leur pertinence aux fins d'une analyse d'adéquation dépendront de la réception du droit international dans l'État évalué. La place dans la hiérarchie des normes du droit international et l'option pour un système dualiste ou moniste sont des éléments essentiels permettant de mesurer l'importance des engagements internationaux de l'État dans la protection de la vie privée et des données à caractère personnel.

---

(45) Résolution 2200 A (XXI) du 16 décembre 1966 de l'Assemblée Générale des Nations Unies relative au Pacte international relatif aux droits civils et politiques, entrée en vigueur le 23 mars 1976.

(46) Convention STE n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

(47) Protocole additionnel STE n° 181 à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, concernant les autorités de contrôle et les flux transfrontières de données.

(48) La convention et le protocole sont ouverts à ratification par des États tiers au Conseil de l'Europe. À ce jour, l'Uruguay, Maurice et le Sénégal ont signé et ratifié la Convention n° 108.

(49) Voy. la référence explicite à la Convention 108 au considérant 95 du RGPD.

(50) Lignes directrices de l'OCDE régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel du 23 septembre 1980, telles que révisées le 9 octobre 2013.

(51) APEC Privacy Framework, November 2004.

2. — *Les « Garanties essentielles » en matière de surveillance*

L'évaluation du niveau de protection des droits et libertés fondamentaux garanti dans le cadre des activités de surveillance d'un État tiers devient un critère d'adéquation particulièrement déterminant. La méthodologie développée pour l'analyse d'adéquation du niveau de protection des données et expliquée au point (A) doit donc être complétée par un ensemble de critères spécifiques applicables aux activités de surveillance.

Faisant suite à l'arrêt *Schrems*, le Groupe de l'article 29 s'est accordé sur quatre « garanties essentielles » pour évaluer le niveau de protection garanti par un pays tiers dans le cadre de ses activités de surveillance (52). Ces garanties sont dégagées de la jurisprudence de la Cour européenne des droits de l'homme et de la Cour de justice et ne doivent pas seulement être prises en compte au cours d'une évaluation d'adéquation, mais aussi, et nous y reviendrons dans notre dernière partie, lorsque des données sont transférées dans le cadre d'autres instruments de transferts tels que les règles d'entreprise contraignantes ou les clauses contractuelles types (53). Elles ont vocation à servir de lignes directrices pour les autorités nationales et les responsables de traitement lorsqu'ils transfèrent des données en dehors du territoire européen, mais constituent bien sûr des critères hautement pertinents pour la préparation d'une décision d'adéquation.

La première de ces garanties est que « les traitements de données devraient s'opérer dans le cadre de règles claires, précises et accessibles » (54). C'est essentiellement l'exigence de légalité des articles 8, § 2, de la CEDH et 52, § 1, de la Charte qui est visée ici. Le Groupe de l'article 29 rappelle que, selon la jurisprudence de la Cour EDH, il n'y a aucune raison de soumettre les règles gouvernant l'interception de communications individuelles et les dispositifs de surveillance plus généraux à des critères d'accessibilité et de clarté différents (55).

La deuxième garantie est que « la nécessité et proportionnalité des mesures au regard des objectifs légitimes poursuivis soient démontrées » (56). Sur ce

(52) Working Document 01/2016 on the justification of interferences with the fundamental rights to privacy and data protection through surveillance measures when transferring personal data (European Essential Guarantees) of 13 April 2016, WP 237.

(53) WP 237, p. 3.

(54) Guarantee A — "Processing should be based on clear, precise and accessible rules", WP 237, p. 7.

(55) Cour EDH, arrêt du 1er juillet 2008, *Liberty et autres c. Royaume-Uni*, req. no 58243/00, § 63.

(56) Guarantee B — "Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated", WP 237, pp. 7-9.

point, les décisions récentes de la Cour de justice relative à la conservation des données de trafic sont particulièrement pertinentes. La Cour avait commencé par annuler la directive européenne de 2006 qui imposait une conservation systématique des données liées aux communications électroniques, considérant que les garanties étaient insuffisantes au regard des articles 7 et 8 de la Charte, mais laissé en suspens la question de savoir si la « surveillance indiscriminée » ou « de masse » posait, dans son principe même, un problème de légalité (57). Dans sa décision *Tele2 Sverige* du 21 décembre 2016, la Cour a condamné sans ambages, et contre l'avis exprimé par l'avocat général (58), le principe de la conservation généralisée et indifférenciée de l'ensemble des données de trafic et de localisation, comme étant contraire aux articles 7, 8 et 11 de la Charte (59). Cette décision ouvre la voie à une remise en cause d'autres instruments impliquant le traitement ou transfert de quantités « massives » de données, en premier lieu duquel le projet d'accord UE-Canada sur le transfert de données et le traitement de données des dossiers passagers (données dites « PNR — *Passenger Name Records* ») (60) pour lequel la Cour doit rendre un avis très prochainement (61). Si cet avis s'avérait négatif, les accords PNR existants conclus avec les États-Unis et l'Australie, ainsi que la directive PNR européenne adoptée dans la foulée des attentats de Paris de 2015 (62), ou encore l'accord UE-US « TTFP » (*Terrorist Tracking Financing Program*) portant sur les transferts de don-

(57) CJUE (GC), arrêt du 8 avril 2014, *Digital Rights Ireland*, aff. jointes C-293/12 et C-594/12, EU:C:2014:238.

(58) Conclusions de Henrik Saugmandsgaardøe dans les affaires jointes *Tele2 Sverige et Secretary of State for the Home Department*, C-203/15 et C-698/15, EU:C:2016:572.

(59) CJUE (GC), 21 décembre 2016, *Tele2 Sverige AB*, aff. jointes C-203/15 et C-698/15, EU:C:2016:970.

(60) Proposition de décision du Conseil relative à la conclusion de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, COM(2013) 528 final.

(61) Voy. les conclusions de Paolo Mengozzi présentées le 8 septembre 2016 dans l'avis 1/15 concernant le projet d'accord entre le Canada et l'UE sur le transfert et le traitement de données des dossiers passagers. Au moment de mettre sous presse, la Cour de justice a rendu l'avis attendu, le 26 juillet 2017 : « L'accord PNR ne peut pas être conclu sous sa forme actuelle en raison de l'incompatibilité de plusieurs de ses dispositions avec les droits fondamentaux reconnus par l'Union ».

(62) Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, *J.O.U.E.*, n° L 119, 4 mai 2016.

nées relatives aux transactions financières internationales (63), pourraient être remis en question (64).

La troisième garantie essentielle est « l'existence d'un mécanisme de supervision indépendant ». À cet égard, s' « il est en principe souhaitable que le contrôle soit confié à un juge, car le pouvoir judiciaire offre les meilleures garanties d'indépendance, d'impartialité et de procédure régulière » (65), le standard européen n'exclut pas qu'un autre organisme puisse être chargé de cette mission de contrôle « à condition que cet organe soit suffisamment indépendant de l'exécutif » (66) et qu'il soit investi de pouvoirs et attributions suffisants pour exercer un contrôle efficace et permanent (67).

Enfin, la quatrième garantie porte sur le droit à une protection juridictionnelle effective et exige que des voies de recours effectives soient disponibles aux individus (68).

3. — *État de droit et état de la démocratie*

Si les « garanties essentielles » proposées par le Groupe de l'article 29 ou les engagements internationaux pris par l'État sont des critères indubitablement pertinents pour compléter la méthodologie d'évaluation de l'adéquation du niveau de protection des données offert dans un pays tiers, ceux-ci doivent nécessairement s'inscrire dans un contexte général favorable au maintien d'un État de droit. Cette évaluation peut sembler évidente, voire inutile, pour des États où les principes fondamentaux de la démocratie sont fortement ancrés, mais peut se révéler tout à fait pertinente, voire déterminante, pour des États démocratiques plus récents ou moins avancés. Évaluer le niveau « démocratique » constitue une tâche particulièrement complexe.

---

(63) Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, *J.O.U.E.*, nº L 195, 27 juillet 2010.

(64) Voy. Fr. Boehm & M. D. Cole, « Data Retention after the Judgement of the Court of Justice of the European Union », 30 juin 2014, étude commandée par l'eurodéputé J.P. Albrecht suite à l'arrêt *Digital Rights Ireland*, www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf.

(65) Cour EDH, arrêt du 6 septembre 1978, *Klass et autres c. Allemagne*, req. nº 5029/71, § 54.

(66) Cour EDH, arrêt du 26 avril 2007, *Dumitru Popescu c. Roumanie*, req. nº 71525/01, § 71 ; Cour EDH, arrêt du 4 décembre 2015, *Roman Zakharov c. Russie*, req. nº 47143/06, § 258.

(67) Cour EDH, arrêt *Klass et autres c. Allemagne*, précité, § 56.

(68) Guarantee C — "Effective remedies need to be available to the individual", WP 237, *op. cit.*, p. 11.

Dans le même temps, rapporter une vision globale du niveau démocratique d'un État tiers n'est pas complètement impossible. Nous ne saurions proposer ici une liste exhaustive de critères auxquels toute étude d'adéquation devrait être attentive, mais plutôt quelques pistes à considérer qui ressortent de notre expérience d'évaluation du niveau de protection des données offert dans des pays tiers situés sur tous les continents.

Tout d'abord, l'exigence de contrôle indépendant décrite ci-dessus, fût-elle parlementaire ou judiciaire, ne saurait être satisfaite si le principe de séparation des pouvoirs ne se trouve pas suffisamment reflété dans les normes, de rang constitutionnel ou autre rang élevé de la hiérarchie des normes, d'un État tiers. De même, la garantie que l'État offre une protection juridictionnelle effective ne saurait être valablement constatée si l'indépendance du pouvoir judiciaire n'est pas expressément reconnue. Un aperçu du système juridique sur lequel l'État tiers repose, de la structure politique de cet État, de la forme de gouvernement et une analyse générale des règles de rang constitutionnel ou équivalent permet d'identifier des limites structurelles à l'effectivité des droits et libertés fondamentaux dans un État.

Cette vision globale du système politique et juridique de l'État tiers peut être complétée grâce à différents index globaux publiés par des Organisations non gouvernementales. Nous pensons à l'index annuel relatif à l'État de droit dans le monde publié par l'Organisation non gouvernementale *World Justice Project* (69), au baromètre mondial relatif à la corruption publié par l'ONG *Transparency International* (70) ou encore au *Global Open Data Index* qui mesure le niveau de transparence gouvernemental (71).

Cette évaluation est indispensable pour les transferts de données opérés dans le cadre des décisions d'adéquation adoptées sous l'empire du RGPD, mais aussi pour les transferts de données à des fins de coopération policière

(69) Voy. *World Justice Project (WJP) Rule of Law Index* 2016, http://worldjusticeproject.org/rule-of-law-index. Le WJP Index repose sur plus de 100.000 enquêtes d'opinions et avis d'experts exprimant leur expérience dans la vie quotidienne du respect de l'État de droit dans le monde. 47 indicateurs sont regroupés sous les 8 facteurs suivants : contraintes sur le gouvernement, absence de corruption, ordre et sécurité, droits fondamentaux, transparence du gouvernement, application de la réglementation, justice civile et justice pénale.

(70) Voy. *Global Corruption Barometer* and *Perceptions Corruption Index*, Transparency International, www.transparency.org/cpi2015/. Voy. par exemple le rapport récent relatif à l'Europe et à l'Asie, *People and Corruption, Europe and Central Asia 2016*, www.transparency.org/whatwedo/publication/7493.

(71) *Global Open Data Index* 2015, http://index.okfn.org/about/.

et judiciaire internationale qui seront fondées sur des décisions d'adéquation adoptées dans le cadre de la directive (72).

II. — Le *Privacy Shield*, une protection adéquate ?

Après avoir mis au jour les critères d'évaluation du caractère adéquat exposés au point précédent, la Cour de justice a relevé que « la Commission n'a pas fait état, dans la décision 2000/520, de ce que les États-Unis d'Amérique "assurent" effectivement un niveau de protection adéquat en raison de leur législation interne ou de leurs engagements internationaux » (73) alors qu'elle aurait dû justifier que ce pays assure effectivement « un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti dans l'ordre juridique de l'Union » (74). La Cour a dès lors invalidé la décision 2000/520 de la Commission instaurant le *Safe Harbor*.

Cet arrêt ayant rendu inopérant l'instrument de référence qui permettait les échanges de données avec les États-Unis, il s'est tout de suite révélé impératif d'élaborer un nouvel accord qui viendrait remplacer le défunt *Safe Harbor* en répondant aux exigences énoncées par la Cour.

Les négociations entreprises entre la Commission et le gouvernement américain (75) aboutirent le 2 février 2016 à un accord politique sur un

(72) Art. 36 de la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, n° L 119, 4 mai 2016.

(73) Point 97 de l'arrêt *Schrems*, précité.

(74) Point 96 de l'arrêt *Schrems*, précité.

(75) En fait, un round de négociations UE-États-Unis avait déjà été entamé à la suite des révélations d'Edward Snowden. La Commission avait exposé dans sa communication COM(2013) 846 final et COM(2013) 847 final du 27 novembre 2013 que le régime du *Safe Harbor* devait être réexaminé en vue d'un renforcement de la protection pour tenir compte de la croissance exponentielle des flux de données liés à l'économie transatlantique, ainsi que de l'ampleur et de la portée de certains programmes de renseignement américains. Dans sa communication COM(2013) 847, la Commission a formulé 13 recommandations devant guider ce réexamen. « Ces recommandations portaient principalement sur le renforcement des principes de fond protégeant la vie privée et une plus grande transparence des politiques de confidentialité des entreprises américaines autocertifiées, sur un contrôle, un suivi et une mise en œuvre améliorés, par les autorités américaines, du respect de ces principes, sur la mise en place de mécanismes de règlement des litiges abordables et sur la nécessité de limiter le recours à la dérogation pour raison de sécurité nationale,

nouveau cadre pour les échanges transatlantiques de données à des fins commerciales, baptisé le « bouclier de protection des données » (« *Privacy Shield* ») (76). Le 29 février, la Commission présenta un projet de décision qui a fait l'objet de commentaires critiques de la part du Groupe de l'article 29 (77) et du Contrôleur européen de protection des données (78) avant la résolution adoptée par le Parlement européen à ce propos (79). La décision définitive, ajustée en tenant compte de ces commentaires, a été adoptée le 12 juillet 2016 (80) et le nouveau mécanisme est entré en vigueur dès le 1er août.

Nous présentons ici les éléments clés du *Privacy Shield*. Nous verrons dans un premier temps qu'il apporte des garanties complémentaires bienvenues en matière de protection des données traitées par le secteur privé (A). Toutefois, nous tâcherons d'expliquer pourquoi les engagements pris par le gouvernement américain en matière de surveillance nous apparaissent insuffisants pour satisfaire l'exigence de protection adéquate (B).

---

prévue par la décision 2000/520/CE, à ce qui est strictement nécessaire et proportionné » (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, considérant 8).

(76) Communiqué de presse de la Commission européenne du 2 février 2016, « La Commission européenne et les États-Unis s'accordent sur un nouveau cadre pour les transferts transatlantiques de données, le "bouclier vie privée UE-États-Unis" », Document IP/16/216. L'accord est baptisé « *Privacy shield* », traduit dans un premier temps par « bouclier vie privée » avant d'être traduit par « bouclier de protection des données » dans les textes ultérieurs. On notera que l'expression finale française correspond mieux au vocabulaire utilisé désormais pour évoquer la matière dans l'UE où le droit à la protection des données a une existence propre, détachée du droit à la vie privée.

(77) Groupe de travail article 29, avis 01/2016 du 13 avril 2016 sur le projet de décision concernant le caractère adéquat du « bouclier de protection des données UE-États-Unis », WP 238.

(78) CEPD, Opinion 4/2016 on the EU-US Privacy Shield Draft Adequacy Decision, 30 May 2016.

(79) Résolution du Parlement européen du 26 mai 2016 sur les flux de données transatlantiques (2016/2727(RSP)).

(80) Décision d'exécution (UE) 2016/1250 de la Commission européenne 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.U.E.*, no L 207, 1er août 2016.

A. — Un régime de protection des données amélioré

1. — *Un système co-régulatoire*

Le système mis en place en remplacement du défunt *Safe Harbor* est resté dans la ligne de ce dernier : il s'agit d'un mécanisme de co-régulation dans lequel les organisations américaines destinataires de données personnelles en provenance de l'UE décident librement de souscrire aux principes de protection (*Privacy Principles*) établis d'un commun accord par les autorités américaines et européennes. L'adhésion au système est donc entièrement volontaire mais le respect de ses règles est obligatoire une fois qu'on a franchi le pas. Comme auparavant, les organisations doivent s'engager à adhérer au système auprès du ministère américain du Commerce (*U.S. Department of Commerce*). Ce dernier publie la liste des entreprises ayant adhéré au *Privacy Shield* (81) et est chargé de veiller au respect de leurs engagements. Pour pouvoir obtenir leur certification, les entreprises doivent avoir une politique de protection des données conforme aux *Privacy Principles*, politique qu'elles doivent rendre publique sur leur site Web. Elles doivent par ailleurs renouveler tous les ans leur adhésion au bouclier de protection des données.

Les principes de protection énoncés dans le *Privacy Shield* reflètent ceux qui étaient établis dans le cadre du *Safe Harbor* tout en étant amplifiés et renforcés par rapport au modèle passé (82). Les modifications portent sur les éléments suivants.

2. — *Des obligations de transparence*

Les organisations participantes voient peser sur elles des obligations plus lourdes qu'auparavant surtout en termes de *transparence*. Au-delà de l'obligation évoquée ci-dessus de rendre publique leur politique en matière de protection des données, elles doivent ainsi fournir aux personnes concernées des informations sur un certain nombre d'éléments essentiels en rapport avec le traitement de leurs données à caractère personnel (tels que le type de données recueillies, la finalité du traitement, le droit d'accès et de choix, les conditions applicables aux transferts ultérieurs et la responsabilité du traitement). Les organisations doivent aussi afficher sur leur site Web des hyperliens vers le site du *Department of Commerce* (qui donne davantage

(81) Voy. la *Privacy Shield List* sur le site internet du ministère du Commerce à l'adresse www.privacyshield.gov/welcome.

(82) G. Maldofff, « We read Privacy Shield so you don't have to », *Privacy Tracker*, Westin Research Center, March 7, 2016, https://iapp.org/news/a/we-read-privacy-shield-so-you-dont-have-to.

d'informations sur l'autocertification, les droits des personnes concernées et les mécanismes de recours disponibles), vers la liste du *Privacy Shield* et vers le site web d'un organe approprié de règlement extrajudiciaire des litiges (83).

3. — *Des utilisations limitées des données*

Un des *Privacy principles*, le principe 2 intitulé « choix », a été remodelé sur un point particulièrement important, répondant à une faiblesse du *Safe Harbor* qui avait été dénoncée jusque-là (84). Alors qu'auparavant les données traitées aux États-Unis en provenance d'Europe pouvaient être utilisées *dans un but incompatible* avec l'objectif pour lequel elles avaient été initialement collectées (85), à moins que les personnes concernées ne s'y soient opposées, à présent, sauf opposition, les données « peuvent être utilisées *dans un but matériellement différent* du ou des objectifs pour lesquels les données ont été initialement collectées ou du ou des objectifs approuvés ultérieurement par la personne concernée » (86). Le principe 5, dont l'intitulé « Intégrité des données » a été complété par « … et limitation des finalités », apporte une clarification importante sur l'utilisation des données qui est admise dans un but matériellement différent. Ainsi, si on accepte une telle utilisation, une organisation ne peut toutefois *pas traiter les données d'une manière incompatible* avec les objectifs pour lesquels elles ont été collectées ou avec les objectifs approuvés ultérieurement par la personne concernée. Il y a donc là un renforcement clair de la protection et un rapprochement avec le régime européen. La décision d'adéquation de la Commission apporte aussi cette clarification : « Lorsqu'une nouvelle finalité (modifiée) est sensiblement différente de la finalité initiale, mais qu'elle

(83) Considérant 20 de la 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 (ci-après « Décision Privacy Shield »).

(84) Notamment, Y. POULLET, « Les "Safe Harbor Principles" : une protection adéquate ? », IFCLA 2000, Actes du colloque « Le droit de l'Informatique au tournant du Millénaire », organisé à Paris par la Chambre de Commerce et d'Industrie de Paris, 10 juillet 2000, www.crid.be/pdf/public/4415.pdf.

(85) Par l'application des principes « *Notice* » et « *Choice* » du *Safe Harbor* : il suffisait à l'organisme américain d'informer la personne qu'il traitait ses données et s'autorisait à les utiliser dans un but incompatible avec celui annoncé initialement, pour être autorisé à le faire si la personne concernée ne manifestait pas son opposition à un tel détournement de finalité.

(86) Annexe II de la décision *Privacy Shield*, intitulée « Principes du cadre "Bouclier de protection des données UE-États-Unis" publiés par le ministère américain du Commerce », Principe 2 a. « Choix ».

reste compatible avec celle-ci, le principe "choix" donne aux personnes concernées le droit de s'opposer au traitement (refus). Le principe "choix" ne se substitue pas à l'interdiction expresse de procéder à des traitements incompatibles» (87).

Les conditions applicables au *transfert ultérieur de données à des tiers* sont par ailleurs durcies. Le même niveau de protection doit être assuré en cas de transfert de ce type par une entreprise participante (88).

4. — *Des contrôles et sanctions en cas de non-respect des obligations*

Le *Department of Commerce* procédera à des *contrôles réguliers* afin de vérifier que les entreprises observent les règles auxquelles elles ont souscrit. En cas de non-respect de ces règles, des sanctions seront prises à l'encontre de l'entreprise non conforme qui pourra en certains cas être radiée de la liste des entreprises adhérant au dispositif (89).

5. — *Recours pour les personnes concernées*

Le point des voies de recours ouvertes aux personnes concernées a occupé une grande place dans les négociations. Au final, plusieurs mécanismes sont offerts aux personnes dont les données ont fait l'objet d'une utilisation abusive dans le cadre du bouclier de protection des données (90). Les négociateurs ont veillé à ce que ces voies de règlement des litiges soient accessibles et abordables pour les citoyens européens. Les organisations américaines traitant des données transférées doivent elles-mêmes veiller à proposer des systèmes de recours indépendants et aisément accessibles,

(87) Considérant 22 de la décision *Privacy Shield*. Des exemples de ce qui peut être considéré comme compatible ont été apportés pour faciliter l'application du principe : «Selon les circonstances, les finalités de traitement compatibles peuvent par exemple comprendre celles qui ont raisonnablement pour objectif les relations avec la clientèle, le respect de la réglementation et les considérations juridiques, l'audit, la sécurité et la prévention de la fraude, la préservation ou la défense des droits de l'organisation reconnus par la loi, ou d'autres finalités conformes aux attentes d'une personne raisonnable compte tenu du contexte dans lequel s'inscrit la collecte».

(88) Annexe II de la décision *Privacy Shield*, Principe 3 «Responsabilité en cas de transfert ultérieur».

(89) Annexe II de la décision *Privacy Shield*, Chap. I «Vue d'ensemble», par. 3 et 4. Voy. égal. G. Maldoff, «We've got a finalized Privacy Shield agreement: What's new?», *Privacy Tracker*, July 12, 2016.

(90) Principe 7 «Voies de recours, application et responsabilité» des Principes du Bouclier de protection des données UE-États-Unis. Voy. égal. les nombreux considérants (38 à 63) de la décision *Privacy Shield* réservés à ce point.

pouvant être saisis gratuitement de toute plainte ou tout litige. Les personnes concernées peuvent aussi s'adresser à leur autorité nationale de protection des données, qui collaborera avec la *Federal Trade Commission* pour l'examen des plaintes déposées par les citoyens de l'UE. Lorsqu'une réclamation n'est pas tranchée par l'une de ces voies, un mécanisme d'arbitrage est disponible, en dernier ressort : l'arbitrage contraignant du mécanisme de règlement des litiges offert par le Comité du bouclier de protection des données (*Privacy Shield Panel*). Quant aux recours dans le domaine de la sécurité nationale, on verra ci-dessous qu'une nouvelle voie est offerte aux citoyens de l'UE, passant par un médiateur indépendant des services de renseignement des États-Unis (partie II.B.4).

6. — *Accès des autorités publiques à des fins d'ordre public et de sécurité nationale : limitations et recours*

Les négociateurs du *Privacy Shield* ont bien sûr répondu au point qui était au cœur de l'action en justice portée par Maximilian Schrems contre le *Data Protection Commissioner* irlandais, c'est-à-dire la question de l'accès des pouvoirs publics américains à des fins d'ordre public et de sécurité nationale aux données transférées outre-Atlantique. Cet accès est désormais soumis à des limitations, des conditions et des mécanismes de surveillance définis (91). Les États-Unis ont officiellement exclu toute surveillance de masse systématique des données transférées vers leur territoire dans le cadre du *Privacy Shield*. « Le cabinet du directeur du renseignement national a également précisé que le recours à la collecte de données en vrac serait soumis à certaines conditions préalables et que cette collecte devrait être aussi ciblée et précise que possible. Il a détaillé les garanties mises en place pour l'utilisation de données dans de telles circonstances exceptionnelles » (92).

Par ailleurs, un élément de protection totalement nouveau est issu de la négociation entre représentants de la Commission européenne et autorités américaines : tous les citoyens de l'UE dont les données à caractère personnel sont transférées aux États-Unis dans le cadre du *Privacy Shield* bénéficient désormais d'une voie de recours dans le domaine du renseignement national. Le secrétaire d'État américain a effectivement instauré un

(91) Voy. considérants 67 à 110 de la décision *Privacy Shield*.

(92) Communiqué de presse de la Commission européenne du 12 juillet 2016, « La Commission européenne lance le bouclier de protection des données UE-États-Unis : une protection renforcée pour les flux de données transatlantiques ».

mécanisme de médiation (*Ombudsperson*) pour les citoyens européens au sein du département d'État (93).

Nous reviendrons sur les limites de ces mesures tant concernant la surveillance de masse que concernant le mécanisme de recours mis en place (voy. notre analyse critique des faiblesses du système aux points B.2. et B.4. ci-dessous).

7. — *Réexamen annuel*

Un mécanisme de réexamen annuel conjoint mené par la Commission européenne et le *Department of Commerce* a été prévu, devant permettre de contrôler le fonctionnement du bouclier de protection des données, et notamment le respect des engagements et des assurances concernant l'accès aux données à des fins d'ordre public et de sécurité nationale (94).

8. — *Un texte comportant encore certaines faiblesses*

Si le *Privacy Shield* apporte donc indéniablement des améliorations au système antérieur qui méritent d'être saluées (95), on notera tout de même que certains défauts du *Safe Harbor* n'ont pas pu être corrigés ou que la protection mise en place présente certaines faiblesses.

Ainsi, le droit d'accès accordé aux personnes concernées par des données européennes transférées aux États-Unis connait une exception critiquée depuis la naissance du *Safe Harbor* : le droit d'accès peut être refusé dans « les cas où la charge de travail ou la dépense qu'occasionnerait le droit d'accès sont disproportionnées par rapport aux risques pesant sur la vie privée de la personne concernée » (96).

---

(93) Il est à noter que ce mécanisme de médiation n'est pas réservé aux seuls cas liés au *Privacy Shield* mais qu'il est aussi valable dans le cadre de transferts de données du continent européen ayant eu recours aux autres instruments juridiques (voy. Groupe de l'article 29, *Opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision*, 13 April 2016, WP 238, p. 45 : « *Despite its name, it is explained in the Memorandum that the Privacy Shield Ombudsperson will not only process requests relating to national security access to data transmitted from the EU to the U.S. pursuant to the Privacy Shield, but also those where the data has been transmitted pursuant to Standard Contractual Clauses, Binding Corporate Rules, Derogations (under Article 26 of Directive 95/46/EC)* »).

(94) Art. 4.4 de la décision *Privacy Shield*.

(95) Dans le même sens, voy. Groupe de l'article 29, Opinion 01/2016, précitée : « *The WP29 first of all welcomes the significant improvements brought by the Privacy Shield compared to the Safe Harbour decision* ».

(96) Principe 6 « Accès ». Voy. également le principe complémentaire 8.b, qui vise à circonscrire le recours à cette exception au droit d'accès.

Par ailleurs, le texte même du *Privacy Shield* met en exergue une lacune qui devra sans doute être comblée à l'avenir. Il s'agit de l'absence d'une protection générale dans le droit américain contre les décisions automatisées. Or, « compte tenu du recours accru au traitement automatisé (y compris au profilage) pour fonder des décisions concernant les personnes dans l'économie numérique moderne, ce domaine doit faire l'objet d'une étroite surveillance » (97).

Le Groupe de l'article 29 regrette en outre qu'un droit d'opposition à l'enregistrement, à l'utilisation ou à la communication des données ne soit pas accordé aux personnes concernées (98).

Enfin, ainsi qu'il a été dit au point 6) ci-dessus, sur le plan de l'accès aux données par les autorités publiques pour des motifs de sécurité nationale, des garanties plus solides auraient été les bienvenues à propos de l'engagement américain à ne pas effectuer de collecte massive et indiscriminée de données (99). Le point B ci-dessous s'attache à développer ces failles de la protection face aux pratiques de surveillance étatique, ainsi qu'aux mécanismes de supervision mis en place.

B. — Des garanties insuffisantes concernant la surveillance

Un certain nombre d'évolutions politiques, mais aussi législatives et règlementaires ont eu lieu aux États-Unis à la suite des révélations d'Edward Snowden (100). La décision d'adéquation relative au *Privacy Shield* se réfère explicitement à ces avancées afin d'établir l'adéquation du niveau de protection offert par les États-Unis quant aux mesures de surveillance secrète dont les citoyens et résidents européens sont susceptibles de faire l'objet (101).

(97) Considérant 25 de la décision *Privacy Shield*. Le Groupe de l'Article 29 a lui aussi relevé cette lacune dans le dispositif de protection mis en place avec le *Privacy Shield* (G29, 27 July 2016, Statement on the decision of the European Commission on the EU-U.S. *Privacy Shield*).

(98) Groupe de l'article 29, 27 July 2016, Statement on the decision of the European Commission on the EU-U.S. Privacy Shield.

(99) *Ibid.*

(100) Voy. P. Swire, « US Surveillance Law, Safe Harbor, and Reforms Since 2013 », White Paper submitted to the Belgian Privacy Commission for its December 18, 2015 forum on « The Consequences of The Judgement in The *Schrems* case », https://fpf.org/wp-content/uploads/2015/12/White-Paper-Swire-US-EU-Surveillance.pdf.

(101) Voy. en particulier l'Annexe VI de la décision *Privacy Shield* : « Lettre de M. Robert Litt, conseiller général Bureau du directeur du renseignement national ».

Nous l'avons dit, ces garanties ont reçu un accueil réservé du Groupe de l'article 29 (102) et du CEPD (103).

L'objet de cette section ne saurait être de proposer une analyse juridique détaillée du système de surveillance américain. En effet, les programmes de surveillance en œuvre aux États-Unis et révélés par les documents de Snowden sont très complexes (104). Une analyse approfondie des problèmes juridiques soulevés par de tels programmes sous l'angle de la protection des données en vue d'une analyse d'adéquation requiert la collaboration étroite de plusieurs experts informatiques et juristes des deux côtés de l'Atlantique. Comme cela a été souligné par le Groupe de l'article 29, il est d'ailleurs regrettable que le projet de décision d'adéquation du *Privacy Shield* ait été élaboré sans qu'une étude d'adéquation indépendante ait été préalablement conduite, contrairement à la pratique habituelle jusqu'ici (105).

Notre objectif sera ici plutôt de discuter les plus importantes faiblesses du système américain au regard des « garanties essentielles » évoquées dans notre première partie (I.B.). Puisque nous nous intéressons à la protection des données des Européens, nous choisissons de nous concentrer ici sur la principale base légale qui encadre la surveillance des non-Américains (106)

(102) Groupe de l'article 29, Opinion 01/2016, précitée.

(103) CEPD, Opinion 4/2016, précitée

(104) Ils incluent des programmes d'accès aux données des sociétés Internet, des programmes de surveillance du réseau câblé de fibres optiques, la collecte massive et généralisée de données de trafic auprès d'opérateurs nationaux, des écoutes téléphoniques et des collectes de textos, mais aussi de millions d'images (en particulier de visages), ou encore la mise en place de « trappes » pour contourner le cryptage et le recours à des logiciels malveillants permettant de prendre le contrôle d'un ordinateur à distance (y compris ses fonctionnalités audio et vidéo). Pour une présentation de l'ensemble des programmes de surveillance révélés par les principaux médias (*Washington Post*, *Guardian*, *Der Spiegel*, *Le Monde*) ayant eu accès à des documents de Snowden, voy. le rapport de P. Omtzigt pour le Conseil de l'Europe, Assemblée parlementaire, Commission des questions juridiques et des droits de l'homme, « Les opérations massives de surveillance », 26 janvier 2015, AS/Jur(2015)01. Voy. aussi la classification de plusieurs de ces programmes de surveillance sur une échelle des plus ciblés au plus massifs par M. Cayford, C. Van Gulijk et P.H.A.J.M. Van Gelder, « All swept up : An initial classification of NSA surveillance technology », in T. Nowakowski, M. Młyńczak, A. Jodejko-Pietruczuk et S. Werbińska-Wojciechowska (eds), *Safety and Reliability : Methodology and Applications*, CRC Press, 2014, pp. 643-650, www.crcnetbase.com/doi/abs/10.1201/b17399-90.

(105) Groupe de l'article 29, Opinion 01/2001, *op. cit.*

(106) Dans cet article, les « non-Américains » désignent les personnes qui n'ont pas la nationalité américaine et/ou qui ne sont pas des résidents permanents aux États-Unis et qui ne bénéficient pas d'une protection équivalente à celle assurée aux citoyens ou résidents américains en vertu du *Privacy Act* de 1974 et du Quatrième Amendement de la Constitution des États-Unis qui protège contre des perquisitions et saisies non motivées

par la NSA, à savoir la section 702 FISA (*Foreign Intelligence Surveillance Act*) (107). Cette disposition est particulièrement pertinente puisqu'elle sert de base juridique à la conduite des programmes *PRISM* et *Upstream* révélés par les documents de Snowden et ayant suscité de vives réactions du côté européen. Nous rappellerons brièvement le fonctionnement de ces programmes et leur base légale (1). Davantage que le risque d'une surveillance absolument indiscriminée, nous verrons que ce sont les finalités beaucoup trop larges des bases légales de ces programmes qui sont problématiques (2). Ensuite, nous verrons en quoi le système d'autorisation et de contrôle de telles mesures de surveillance secrète pose un problème de compatibilité avec le standard européen en la matière (3). Enfin, nous reviendrons sur les limites des mécanismes de recours offerts aux individus (4), l'ensemble de ces considérations contribuant à soulever des doutes sérieux quant à une protection *substantiellement équivalente* des droits fondamentaux aux États-Unis.

1. — *Fonctionnement des programmes* PRISM *et* Upstream

Les programmes *PRISM* et *Upstream* trouvent leur base légale dans la section 702 FISA introduite en 2008 (108). En bref, cette disposition permet au Procureur général des États-Unis et au Directeur de la NSA d'autoriser conjointement l'interception des communications 1) de personnes étrangères, 2) dont il est raisonnable de croire qu'elles se trouvent en dehors du territoire des États-Unis, 3) au moyen de la participation contrainte des fournisseurs de services électroniques, 4) en vue d'acquérir des renseignements étrangers (*foreign intelligence information*) (109). La NSA a développé au moins deux programmes pour intercepter ces communications, organisant une collecte en aval et en amont des communications étrangères.

La collecte en aval consiste à requérir la coopération (contrainte) des grandes entreprises américaines fournisseurs de services de communications électroniques (Google, Apple, Facebook, Yahoo, Skype, etc.). Les premières révélations relatives au programme *PRISM* faisaient état d'un accès direct

---

et requiert un mandat (et une sérieuse justification) pour toute perquisition. Voy. plus loin la Section II (B) (5) «Des voies de recours insuffisantes».

(107) 50 U.S. Code § 1881a — Procedures for targeting certain persons outside the United States other than United States persons.

(108) 50 U.S. Code § 1881a.

(109) Pour une analyse juridique détaillée des programmes de surveillance autorisés suivant la section 702, voy. Privacy and Civil Liberties Oversight Board (PCLOB), Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, 2 juillet 2014, www.pclob.gov/library/702-Report.pdf.

par la NSA aux serveurs des grandes entreprises numériques américaines lui permettant d'intercepter unilatéralement toutes les communications ou données qu'elle souhaitait (110). Ces allégations, immédiatement niées par les entreprises concernées, se sont avérées partiellement fausses. *PRISM* serait plutôt une sorte de programme qui aurait été développé en collaboration entre la NSA et les entreprises pour permettre à ces dernières de répondre efficacement aux ordres de surveillance des cibles envoyés par la NSA. Dans ce cadre, les cibles sont appelées des sélecteurs (adresse email, numéro de téléphone). Si la NSA ne dispose pas d'un accès direct aux serveurs privés, *PRISM* est le programme permettant de créer un miroir pour chaque sélecteur/compte ciblé et de fournir à la NSA l'accès à l'ensemble des comptes miroirs ciblés en temps réel (111).

Le deuxième programme repose sur l'interception des communications en amont, au niveau de l'infrastructure des télécommunications elle-même. Le programme *Upstream* consiste à scinder un câble de fibre optique afin que celui-ci envoie les signaux dans deux directions différentes, l'une vers le destinataire final, l'autre vers la NSA (112). En somme, il s'agit pour la NSA de faire une copie de l'ensemble des signaux transitant par un câble sur lequel elle a été en mesure d'installer le système d'interception. Une fois les données copiées, le programme *Upstream* vise l'interception des informations « à propos » (*about*) des sélecteurs ciblés afin de compléter la collecte de l'ensemble des données de communications qui concernent cette cible. Contrairement à *PRISM* qui permet la collecte des communications d'un sélecteur ciblé lorsqu'il est le destinataire ou l'expéditeur d'une information via un service de communications électroniques, *Upstream* permettra de collecter l'ensemble des informations circulant sur Internet « de », « à » et « à propos » de ce sélecteur, telles que les messages électroniques de tiers faisant référence à ce sélecteur. Une fois les données relatives aux sélecteurs filtrées, l'ensemble des autres données seraient supprimées.

Avant d'analyser plus en détails les garanties applicables à ces programmes, soulignons immédiatement que le *Privacy and Civil Liberties Oversight Board* (PCLOB) a considéré que, pour l'essentiel, ces programmes étaient valablement autorisés par le Congrès suivant la section 702 FISA

(110) Voy. M. Greenwald, « NSA PRISM program taps in to user data of Apple, Google and others », *The Guardian*, 7 juin 2013, www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

(111) M. Cayford, C. Van Gulijk & P.H.A.J.M. Van Gelder, « All swept-up: an initial classification of NSA surveillance technology », *op. cit.*, pp. 645-646.

(112) *Ibid.*, p. 644.

et compatibles avec le quatrième amendement de la Constitution (113). Il faut souligner que le rapport du PCLOB vise en premier lieu à analyser la légalité au regard du droit américain des programmes de surveillance. Ainsi l'accent y est légitimement mis sur les risques ou excès d'interceptions incidentes de communications domestiques de ressortissants américains et sur les limites et faiblesses des procédures de minimisation applicables en cas de telles interceptions incidentes. Le *Review Group* (114), mis sur pied par le Président des États-Unis dans la foulée des révélations, prend en compte dans son rapport, outre l'analyse légale, les conséquences politiques et diplomatiques néfastes que peuvent entraîner les programmes de surveillance des ressortissants étrangers de pays alliés (115).

2. — *Une surveillance de masse ? Des finalités trop larges*

Les programmes *PRISM* et *Upstream*, tous deux fondés sur la section 702 FISA, doivent être distingués. Le programme *PRISM* n'est pas celui d'une collecte de masse et indiscriminée de communications électroniques. En effet, les chiffres révélés par les rapports de transparence, conformément à l'*US Freedom Act* (116), montrent bien qu'il s'agit d'une interception ciblée (en moyenne 90.000 cibles par an) (117). Toutefois, *Upstream* soulève la question de savoir si l'interception provisoire de l'ensemble des signaux transitant par un câble de fibre optique en vue de l'interception ciblée de communications constitue une mesure que l'on pourrait qualifier de sur-

(113) PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, *op. cit.*

(114) Office of the Press Secretary of the White House, « Presidential Memorandum — Reviewing Our Global Signals Intelligence Collection and Communications Technologies », 12 August 2013.

(115) R. A. Clarke, M. J. Morell, G. R. Stone, C. R. Sunstein & P. Swire, *Liberty and Security in a Changing World*, Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 12 December 2013, www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

(116) USA Freedom Act to reform the authorities of the Federal Government to require the production of certain business records, conduct electronic surveillance, use pen registers and trap and trace devices, and use other forms of information gathering for foreign intelligence, counterterrorism, and criminal purposes, and for other purposes (US Freedom act), June 2, 2015.

(117) Office of the Director of National Intelligence, Statistical Transparency Report Regarding use of National Security Authorities, Calendar year 2013 (89138 Section 702 FISA targets), Calendar year 2014 (92707 Section 702 FISA targets), Calendar year 2015 (94368 Section 702 FISA targets), www.dni.gov/index.php/newsroom/press-releases/215-press-releases-2016/1371-odni-releases-third-annual-statistical-transparency-report-regarding-use-of-national-security-authorities.

veillance massive (118). Quoi qu'il en soit, tant pour le programme *PRISM* que pour *Upstream*, il nous apparaît que les finalités pour lesquelles une interception des communications des non-Américains est possible, en ce compris leur contenu, sont trop larges.

La section 702 organise l'interception des communications des ressortissants étrangers raisonnablement présumés se trouver en dehors du territoire des États-Unis en vue de l'acquisition de « renseignements étrangers ». Comme cela a été souligné par le Groupe de l'article 29, cela couvre un champ très large (119), tel que « toute information concernant une puissance étrangère ou un territoire étranger relative à : a) la défense ou la sécurité nationales des États-Unis ; b) ou à la conduite des affaires étrangères des États-Unis » (120). Cette notion de « renseignements étrangers » dépasse des enjeux sécuritaires directs pour inclure tous renseignements utiles à la définition et conduite de la politique étrangère des États-Unis.

En matière de surveillance secrète des communications, le standard de la CEDH requiert que les États fournissent des indications appropriées sur les circonstances dans lesquelles les pouvoirs publics peuvent recourir à des mesures de surveillance secrète, en particulier en énonçant clairement *la nature des infractions* susceptibles de donner lieu à une interception et en définissant *les catégories de personnes* susceptibles d'être mises sur écoute (121).

Concernant les *personnes*, la Cour a jugé que les mesures d'interception visant une personne non soupçonnée d'une infraction mais susceptible de détenir des informations sur une telle infraction pouvaient être justifiées au regard de l'article 8 de la Convention (122). Toutefois, la loi doit pou-

(118) Voy. la classification du programme *Upstream* parmi les programmes de surveillance de masse par M. Cayford, C. Van Gulijk et P.H.A.J.M. Van Gelder, « All swept up : An initial classification of NSA surveillance technology », *op. cit.* L'opinion contraire est défendue par un des membres du *Review Group* de la Maison Blanche, P. Swire, « US Surveillance Law, Safe Harbor, and Reforms Since 2013 », *op. cit.*, p. 19 : « *the second view, which I share, is that processing the signal only for filtering purposes does not constitute mass surveillance. Access only to the filtered results, under rules such as those in Section 702, means that the communications of an individual are only retained if there is a match with a selector such as an email address* ».

(119) Groupe de l'article 29, WP 238, précité, p. 36.

(120) 50 U.S. Code § 1801 — Définition e), traduction non officielle.

(121) Cour EDH, arrêt du 24 avril 1990, *Kruslin c. France*, req. nº 11801/85, § 35 ; Cour EDH, arrêt du 24 avril 1990, *Huvig c. France*, req. nº 11105/84, § 34.

(122) Cour EDH, déc. du 19 mars 2002, *Petronella Greuter v. The Netherlands*, req. nº 40045/98 ; Cour EDH, arrêt du 4 décembre 2015, *Roman Zakharov c. Russie*, req. nº 47143/06, § 245.

voir définir clairement quelles sont les personnes, autres que les suspects, susceptibles de détenir de telles informations et pouvant faire l'objet d'une mesure de surveillance secrète (123). Le standard européen exige donc qu'un lien soit établi entre la personne surveillée et la prévention ou répression d'une infraction pénale. Dans l'arrêt *Digital Rights Ireland*, la Cour de justice avait d'ailleurs insisté sur le fait que la directive 2006/24 relative à la rétention de données de trafic n'exigeait nulle part un tel lien puisqu'elle s'appliquait même à des personnes « pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves » (124). Dans sa décision *Tele2 Sverige*, la Cour relève qu'« une telle réglementation ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique », notamment en ce qu'elle n'est pas limitée « aux personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave [ou à] des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité » (125). Dans ce cadre, la finalité d'acquisition de « renseignements étrangers », en ce qu'elle inclut toute information utile à « la conduite des affaires étrangères des États-Unis », nous semble beaucoup trop floue. Un lien, *même indirect ou lointain*, entre les personnes surveillées et la prévention, répression ou poursuite d'infractions pénales n'est en tout cas pas exigé.

Pour ce qui est des *infractions* susceptibles de justifier une interception des communications, la Cour européenne des droits de l'homme a considéré que la base légale permettant l'interception de communications d'une personne « en raison de faits ou d'activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique de la Fédération de Russie », sans davantage de précisions sur les circonstances pouvant conduire à une interception, confère aux autorités une latitude quasi illimitée d'interprétation, susceptible d'entraîner des abus (126). En ce qui concerne les États-Unis, les documents révélés par Edward Snowden ont d'ailleurs permis de démontrer qu'une partie des activités de surveillance de la NSA dans le cadre de *PRISM* ne pouvait être associée à la lutte contre le terrorisme ou les infractions graves, mais avait en effet servi à surveiller les communications

(123) Cour EDH, arrêt du 10 février 2009, *Iordachi et autres c. Moldavie*, req. n° 25198/02, § 44 ; arrêt *Roman Zakharov c. Russie*, précité, § 245.

(124) CJUE (GC), arrêt du 8 avril 2014, *Digital Rights Ireland Ltd*, précité, § 58.

(125) CJUE (GC), arrêt du 21 décembre 2016, *Tele2 Sverige AB*, précité, point 106.

(126) Cour EDH, *Zakharov c. Russie*, précité, § 248.

de personnes militantes pour les droits humains, des journalistes, ou encore de nombreuses entreprises pour des motifs d'espionnage économique (127).

La *Presidential Policy Directive* 28 (PPD-28) (128) adoptée dans la foulée du scandale provoqué par les documents de Snowden et suivant les recommandations du *Review Group* vise à apporter des garanties contre les abus révélés dans la presse. La PDP-28, qualifiée de document historique par certains (129), apporterait des précisions permettant de prévenir ces abus. Il y est spécifié que « les États-Unis ne doivent pas collecter de renseignements en vue de supprimer ou réprimer des voix critiques ou dissidentes, ou en vue de désavantager certaines personnes en raison de leurs origines ethniques, raciales, de leur genre, orientation sexuelle ou religion », ou encore que « la collecte d'informations d'origine étrangère à caractère commercial ou autres secrets commerciaux n'est autorisée qu'en vue de la protection de la sécurité nationale des États-Unis ou de ses partenaires et alliés » (130). Ces engagements de la part des États-Unis ont une valeur politique certaine et contribuent à éclairer les activités de surveillance organisées dans le cadre de la section 702 FISA. Toutefois, cette disposition est insuffisante à garantir que des militants, dignitaires religieux, journalistes ou autres personnalités n'ayant aucun lien avec une entreprise criminelle ne soient injustement surveillés. En effet, si les États-Unis s'engagent à ne pas collecter d'informations en vue de « supprimer ou réprimer des voix critiques ou dissidentes », la PPD-28 n'interdit pas aux agences exécutives de collecter des informations en vue de *se tenir informées de telles voix critiques ou dissidentes*, précisément afin de mieux définir leur politique étrangère, qui est une des finalités légales du FISA. Pareillement, si les États-Unis s'engagent à ne pas collecter d'information en vue de « désavantager » certaines personnes en raison d'une de leurs caractéristiques, la PPD-28 n'écarte pas la possibilité de collecter de telles informations en vue simplement de produire du renseignement utile à la définition de la politique

(127) Rapport de P. Omtzigt pour le Conseil de l'Europe, « Les opérations massives de surveillance », précité, p. 17.

(128) Office of the Press Secretary of the White House, Presidential Policy Directive 28 / PPD 28 — Signals Intelligence Activities of 17 January 2014, www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. Il faut souligner qu'une PPD ne crée aucun droit pour les individus et ne peut être invoquée devant le juge mais est toutefois contraignante pour l'ensemble des agences administratives à qui elle s'adresse.

(129) P. Swire, « US Surveillance Law, Safe Harbor, and Reforms Since 2013 », *op. cit.*, p. 33.

(130) Presidential Policy Directive/PPD-28 — Signals Intelligence Activities, Section 1. Principles Governing the Collection of Signals Intelligence, traduction non officielle.

étrangère des États-Unis. Autrement dit, la PPD-28 comporte des engagements bienvenus de la part des États-Unis quant à certaines utilisations préjudiciables pour les individus qu'ils pourraient faire des renseignements obtenus, mais ne contient aucune limite à la collecte de données relatives à des personnes n'ayant aucun lien, même indirect ou ténu avec la prévention ou répression d'une infraction pénale, tant que ces données peuvent s'avérer utiles à la définition de la politique étrangère des États-Unis.

L'ensemble de ces considérations nous conduisent à conclure que le *FISA Act* et la PPD-28 ne sont pas compatibles avec la garantie essentielle selon laquelle la collecte et le traitement d'informations à des fins de sécurité nationale doivent s'opérer dans le cadre de *règles, claires, précises et accessibles* à même de démontrer *la nécessité et proportionnalité des mesures au regard des objectifs légitimes poursuivis*.

3. — *Un système d'autorisation et de contrôle problématique*

Dans sa jurisprudence relative aux mesures de surveillance secrète, la Cour européenne des droits de l'homme rappelle que la condition de nécessité qui découle de l'article 8, § 2, de la Convention exige un contrôle indépendant, efficace et permanent à même de prévenir les abus (131). Si l'absence de contrôle judiciaire *ex ante* peut être considérée comme admissible (132), la Cour EDH considère que l'existence d'un contrôle indépendant *a posteriori*, «tant dans les cas individuels qu'à titre général» revêt alors une importance particulière (133). Or, un des problèmes majeurs que soulèvent les programmes *PRISM* et *Upstream* au regard des standards européens réside dans le système d'autorisation des interceptions et celui du contrôle de ces interceptions mis en place.

Contrairement au standard applicable pour l'interception des communications des ressortissants américains, qui consiste en une interception judiciaire décidée sur une base individuelle, les programmes de surveillance

(131) Cour EDH, arrêt *Klass et autres c. Allemagne*, précité, §§ 55 et 56.

(132) Voy. Cour EDH, arrêt du 18 mai 2010, *Kennedy c. Royaume-Uni*, req. n° 26839/05. Dans cette affaire, la Cour a considéré comme admissible un système d'interceptions des communications qui s'appuyait sur des autorisations d'interceptions au cas par cas émises par le pouvoir exécutif, puis soumises à un contrôle *ex post* régulier et indépendant portant sur un échantillon de ces autorisations.

(133) Cour EDH, arrêt du 12 janvier 2016, *Szabó and Vissy c. Hongrie*, req. n° 37138/14, §§ 77-79 : «*it is in this context that the external, preferably judicial,* a posteriori *control of secret surveillance activities, both in individual cases and as general supervision, gains its true importance, by reinforcing citizens' trust that guarantees of the rule of law are at work even in this sensitive field and by providing redress for any abuse sustained*».

tels que *PRISM* et *Upstream* s'appuient sur des certifications générales par la Cour FISA d'une validité d'un an. Cette dernière doit en effet délivrer des certifications pour chaque catégorie de renseignements recherchés, qui s'apparente à une validation des finalités pour lesquelles l'interception des communications peut être ordonnée par un analyste de la NSA. Ainsi, la Cour FISA délivre chaque année plusieurs certificats, autorisant sur une base générale la conduite des programmes de surveillance pour certaines finalités de renseignements contenus dans la certification. L'absence de contrôle *ex ante* des décisions d'interceptions, comme c'est le cas ici, rend d'autant plus importantes les conditions de la supervision et de contrôle du programme.

Or, les décisions de ciblage des analystes sont contrôlées en interne par des services appartenant au pouvoir exécutif. La Division Sécurité Nationale du *Département de la Justice* (*National Security Division* — NSD) contrôlerait *a posteriori* chaque décision de ciblage, tandis que le Bureau du Directeur du Renseignement (*Office of the Director of National Intelligence* — ODNI) procèderait à des contrôles par échantillons de décisions (134). Le PCLOB rapporte que le contrôle opéré par la NSD et l'ODNI porte essentiellement sur l'exigence d'extranéité des sélecteurs ciblés, c'est-à-dire la condition que ce sont des cibles non américaines qui sont visées (135). Sur cette question, l'ensemble des procédures de ciblage et de minimisation s'avèrent en effet très strictes en vue de limiter la collecte intentionnelle ou incidente de communications domestiques ou impliquant un ressortissant américain qui seraient soumises au régime d'autorisation judiciaire. En revanche, en ce qui concerne les non-Américains, le PCLOB affirme que les analystes sont seulement tenus de se référer à la catégorie de « renseignements étrangers ». Ils n'ont pas à exposer les raisons particulières pour lesquelles l'interception des communications de cette cible permettra la collecte de « renseignements étrangers » utiles à l'une des finalités certifiées par la Cour FISA (136). Le contrôle interne par la NSD et l'ODNI des décisions de ciblage quant à l'exigence de « renseignements étrangers » se trouve inévitablement limité.

Afin de renforcer le contrôle *ex post*, le PCLOB avait recommandé la révision des procédures de ciblage pour assurer que chaque décision prise par un analyste puisse être spécifiquement reliée à l'une des certifications de la Cour FISA et que l'évaluation interne par la NSD et l'ODNI porte, en sus du contrôle déjà exercé quant au respect de la condition d'extranéité,

(134) PCLOB Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, *op. cit.*, p. 70.

(135) *Ibid.*, pp. 72-73.

(136) *Ibid.*, p. 71.

sur le respect de l'exigence de finalité de « renseignements étrangers » (137). Au moment de la rédaction de cet article, ces recommandations n'avaient été que partiellement suivies (138). Ces mesures nous semblent effectivement plus que nécessaires afin de contrôler les activités des analystes *à titre général*. Toutefois, elles ne contribuent pas à garantir un contrôle *ex post* indépendant *au cas par cas*.

En conclusion de ce point, il nous semble que le système de certification annuel des interceptions de communications, associé à l'absence de contrôle *ex post* indépendant et au *cas par cas* des interceptions réalisées par les analystes de la NSA ne satisfont pas l'exigence *d'un mécanisme de supervision indépendant*.

4. — *Des voies de recours insuffisantes*

Les limites à la protection juridictionnelle offerte aux non-Américains aux États-Unis en ce qui concerne les traitements de données par les autorités publiques constituent une divergence importante entre les systèmes européens et américains en matière de protection de la vie privée (139), qui a longtemps fait obstacle à la signature de l'accord transatlantique relatif à la protection des données traitées à des fins de coopération policière et

(137) PCLOB Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, *op. cit.*, pp. 134-135, Recommendation n° 1 : « *The NSA's targeting procedures should be revised to (a) specify criteria for determining the expected foreign intelligence value of a particular target, and (b) require a written explanation of the basis for that determination sufficient to demonstrate that the targeting of each selector is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court [...] Upon revision of the NSA's targeting procedures, internal agency reviews, as well as compliance audits performed by the ODNI and DOJ, should include an assessment of compliance with the foreign intelligence purpose requirement comparable to the review currently conducted of compliance with the requirement that targets are reasonably believed to be non-U.S. persons located outside the United States* ».

(138) PCLOB, Recommendations Assessment Report, 5 février 2016, pp. 14-15, www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf.

(139) Voy. notamment E. DE BUSSER, *Data Protection in EU and US Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters between Judicial and Law Enforcement Authorities*, Maklu Publishers, 2009 et Fr. BIGNAMI, « The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens », Study for the LIBE Committee of the European Parliament, 2015, www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU(2015)519215_EN.pdf.

judiciaire (140). Ces limites ont également été mises en exergue par les révélations relatives à l'accès aux données initialement collectées et traitées par le secteur privé à des fins commerciales par les agences de renseignements américaines. En effet, les garanties et protection conférées par le 4e amendement de la Constitution (141) et le *Privacy Act* de 1974 (142) s'appliquent principalement pour les Américains (143). Vu les critiques exprimées par la Cour dans l'arrêt *Schrems* (144), des garanties spécifiques devaient nécessairement être apportées en vue de se conformer aux exigences essentielles qui découlent de l'article 47 de la Charte. Elles sont principalement de deux ordres.

a) *Ombudsperson* et autres mécanismes de recours pour la surveillance électronique à des fins de sécurité nationale

Ainsi que dit précédemment, le *Privacy Shield* innove en établissant un mécanisme de recours spécifique pour les citoyens européens concernant les activités de « *signals intelligence* » opérées par les agences de renseignement américaines : le *Privacy Shield Ombudsperson* (145). Il y est précisé que l'*Ombudsperson* est indépendant de la communauté du renseignement et rapporte directement au Secrétaire d'État. Il est responsable du traitement de plaintes provenant d'individus exclusivement et portant sur l'accès par des agences de renseignement à des données transférées depuis l'Union vers les États-Unis en vertu du *Privacy Shield* ou d'autres instruments tels que des règles d'entreprise contraignantes ou des clauses contractuelles types (146). Les requêtes devront être transmises via les services compétents en matière

(140) Proposal for a Council Decision on the conclusion on behalf of the European Union, of an Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offences, COM(2016) 237 final.

(141) U.S. Supreme Court, *United States v. Verdugo-Urquidez*, 494 U.S. 1092 (1990) où la Cour suprême a considéré que le Quatrième Amendement ne s'appliquait pas à une saisie à l'étranger lorsque la personne invoquant le respect dudit amendement n'est ni citoyen ni résident américain.

(142) 5 U.S.C. Sec. 552a — Records maintained on individuals.

(143) Fr. Bignami, « The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens », *op. cit.*

(144) CJUE (GC), arrêt *Schrems*, précité, point 95 : « Une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte ».

(145) Annexe III (A) de la décision *Privacy Shield* « EU-U.S. Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence », pp. 51-59.

(146) *Ibid.*, p. 52.

de sécurité nationale des États membres (147). L'*Ombudsperson* est supposé procéder aux vérifications nécessaires auprès des services concernés mais ne pourra en aucun cas confirmer ou infirmer à l'individu que celui-ci a été la cible d'une mesure de surveillance (148).

Comme cela a été analysé par le Groupe de l'article 29, ce mécanisme est insatisfaisant à plusieurs égards (149). En premier lieu, si l'*Ombudsperson* est indépendant des agences de renseignement, son indépendance vis-à-vis du pouvoir exécutif n'est pas assurée compte tenu de sa subordination au Secrétaire d'État. En second lieu, des doutes sérieux subsistent quant aux conditions d'exercice de ses missions en pratique, et par conséquent sur l'effectivité de ses pouvoirs d'enquêtes et de réparation. En troisième lieu, l'*Ombudsperson* ne remplit pas les conditions d'un « Tribunal » au sens de la Charte des droits fondamentaux de l'UE et de la CEDH. Enfin, les décisions de l'*Ombudsperson* ne sont pas susceptibles d'appel.

b) *Judicial Redress Act* et traitements de données à des fins policières et judiciaires en matière pénale

En ce qui concerne les activités de traitement de données réalisées à des fins répressives par les autorités policières et judiciaires, les lacunes de la protection juridictionnelles des Européens sont supposées être comblées par le *Judicial Redress Act* adopté le 24 février 2016 (150) dont l'objet est d'étendre aux citoyens de certains États les voies de recours ouvertes aux citoyens et résidents américains en vertu du *Privacy Act*. Toutefois, cette extension de droits pour les Européens présente deux catégories de limites importantes (151).

Tout d'abord, les agences fédérales policières et judiciaires bénéficient d'un régime d'exemptions très large en vertu du *Privacy Act* (152). Puisque les droits d'accès (153), de rectification (154) et de recours administratif (155) contre les autorités policières et judiciaires fédérales ne sont pas disponibles la plupart du temps pour les Américains, ils ne le seront pas non

(147) *Ibid.*, p. 53.
(148) *Ibid.*, p. 55.
(149) Groupe de l'article 29, Opinion 01/2016, précitée, p. 45-5.
(150) « Judicial Redress Act of 2015 » adopté le 24 février 2016 « To extend Privacy Act remedies to citizens of certified states, and for other purposes ».
(151) E. Hasbrouck, « The limits of the US Judicial Redress Act », *Privacy Laws & Business International Report*, April 2016, pp. 21-23.
(152) 5 U.S.C. Sec. 552a (j) — General Exemptions & (k) — Specific Exemptions.
(153) 5 U.S.C. Sec. 552a (d)(1) — Access to Records.
(154) 5 U.S.C. Sec. 552a (d)(2).
(155) 5 U.S.C. Sec. 552a (d)(3), (d)(4).

plus pour les Européens. Le procédé d'extension des droits des Américains au bénéfice des Européens se révèle particulièrement artificiel. Ensuite, même avec l'entrée en vigueur du *Judicial Redress Act*, les citoyens ou résidents européens continueront à bénéficier d'une protection moindre que les Américains à deux égards. Premièrement, le *Judicial Redress Act* n'étend pas aux Européens la possibilité de saisir la justice lorsqu'une agence fédérale traite des données inexactes, inadéquates ou incomplètes (156). Ensuite, le *Judicial Redress Act* ne s'applique qu'aux données transférées par une autorité publique ou une entité privée depuis un État européen vers une autorité compétente fédérale américaine (157). Il ne s'applique pas aux données collectées par ces autorités via des États tiers ou des intermédiaires privés aux États-Unis.

En conclusion, tant le mécanisme de l'*Ombudsperson* que le *Judicial Redress Act* nous semblent insuffisants pour assurer aux citoyens et résidents européens la disponibilité de voies de recours effectives contre les mesures de surveillance dont ils sont susceptibles de faire l'objet.

Cela n'a pas échappé aux ONG qui ont déjà introduit deux recours en annulation contre la décision de la Commission en s'appuyant sur *l'inadéquation* du niveau de protection garanti par le *Privacy Shield* (158). Si le *Safe Harbor* a pu survivre une quinzaine d'années aux critiques récurrentes de la part de nombreux experts avant d'être finalement invalidé par la Cour, les révélations d'Edward Snowden ont durablement ouvert la voie à une période où les transferts internationaux de données feront l'objet d'une attention, voire d'une contestation accrue de la société civile en cas de défaut de protection. Cette nouvelle période devrait s'accompagner, selon nous, d'un nécessaire renouvellement de la politique européenne de flux transfrontières.

III. — Vers un nécessaire renouvellement de la politique européenne de flux transfrontières

Après avoir présenté les nouveaux contours de l'exigence de protection adéquate et appliqué cette exigence au *Privacy Shield*, nous revenons à l'arrêt *Schrems* sous un angle plus large que celui des rapports transatlantiques. En effet, si les États-Unis constituent incontestablement une des destinations

(156) E. Hasbrouck, «The limits of the US Judicial Redress Ac», *op. cit.*, p. 23.

(157) Judicial Redress Act, section 1 (h)(4) — Covered record.

(158) Recours introduit le 16 septembre 2016 — *Digital Rights Ireland c. Commission*, aff. T-670/16 et recours introduit le 25 octobre 2016 — *La Quadrature du Net e.a. c. Commission*, aff. T-738/16.

les plus importantes pour les transferts de données à caractère personnel en raison de l'importance de son industrie numérique, les transferts internationaux de données en provenance de l'Union européenne s'intensifient vers d'autres destinations, en particulier dans le contexte des activités des multinationales et de l'externalisation croissante des services de traitement de données. Aussi, la question de l'impact de l'arrêt *Schrems*, au-delà de la question de l'adéquation du niveau de protection offert aux transferts transatlantiques, doit être examinée (A). Nous expliquerons pourquoi, selon nous, cet impact invite à une nouvelle distinction entre destinataires *adéquats* et destinataires *sûrs* (B).

A. — L'IMPACT DE L'ARRÊT *SCHREMS* SUR LES AUTRES INSTRUMENTS DE TRANSFERTS INTERNATIONAUX

En dehors d'une décision d'adéquation de la Commission, les transferts internationaux de données peuvent avoir lieu dans le cadre de règles d'entreprise contraignantes (communément désignées sous leur acronyme anglais «BCRs» pour *Binding Corporate Rules*) approuvées, ou de garanties suffisantes, qui peuvent être apportées via des clauses contractuelles types (CCTs) ou *ad hoc* (159). En outre, la directive et le RGPD prévoient une liste de dérogations pouvant servir de base légale à des transferts de données vers des destinataires *non adéquats*. À ce titre, les transferts peuvent, entre autres, se fonder sur le consentement indubitable de la personne concernée, la nécessité d'exécuter un contrat entre la personne concernée et le responsable du traitement ou d'exécuter des mesures précontractuelles prises à la demande de la personne concernée (160). La question de l'impact de l'arrêt *Schrems* sur ces mécanismes alternatifs de transferts s'est immédiatement posée. Le vice-président de la Commission européenne Timmermans et la commissaire à la Justice ont déclaré en conférence de presse que l'ensemble de ces instruments étaient disponibles pour assurer la continuité des transferts transatlantiques dans l'attente d'une nouvelle décision d'adéquation (161), ce qui a été confirmé par voie de communication (162). Le Groupe de l'article 29 a réagi dans le

(159) Art. 26.2 de la directive 95/46 et art. 46 et 47 du RGPD.

(160) Art. 26.1 de la directive 95/46 et art. 49 du RGPD.

(161) Conférence de presse du Vice-Président Timmermans et de la Commissaire Jourová à la suite de l'arrêt de la Cour dans l'affaire C-362/14 (*Schrems*), 6 octobre 2015, http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm?locale=FR.

(162) Communication 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*), COM(2015) 566 final.

même sens tout en assurant poursuivre son analyse de l'impact de l'arrêt sur ces outils alternatifs (163).

Comme cela a été très justement souligné par le Groupe de l'article 29 «*fundamental rights apply across the board and not only depending on the legal basis for a data transfer*» (164). C'est aussi ce qu'affirme la Cour dans son raisonnement prenant largement appui sur la protection des droits fondamentaux garantie par la Charte : « [a]insi, l'article 25, paragraphe 6, de la directive 95/46 met en œuvre l'obligation explicite de protection des données à caractère personnel, prévue à l'article 8, paragraphe 1, de la Charte, et vise à assurer, comme l'a relevé M. l'avocat général […], la continuité du niveau élevé de cette protection en cas de *transfert de données à caractère personnel vers un pays tiers* » (165). Cette obligation d'assurer la continuité de protections conférée aux données lorsqu'elles sont transférées hors de l'Union ne saurait être valablement limitée aux transferts réalisés sur la base d'une décision d'adéquation. Selon nous, elle s'étend nécessairement à tous les cas de transferts quelle que soit leur base juridique (166). Jusqu'à aujourd'hui, ces garanties suffisantes sont apportées, pour ce qui est de la protection des données traitées dans le secteur privé, par des clauses spécifiques incluses dans des BCRs ou clauses contractuelles conclues entre le responsable de traitement et le destinataire (167). Or ces instruments souffrent des mêmes défauts que ceux du *Safe Harbor* en ce qui concerne les mesures de surveillance (168). Leurs clauses ne contiennent que des garanties limitées comparables à celles contenues dans le *Safe Harbor* et jugées insuffisantes par la Cour. Elles prévoient notamment une obligation pour le destinataire des données d'informer le responsable de traitement

(163) Statement of the Article 29 Working Party of 16 October 2015.

(164) WP 237, p. 4.

(165) C'est nous qui soulignons.

(166) Seuls les transferts basés sur une des exceptions listées à l'article 26, paragraphe 1, de la directive 95/46 et à l'article 49 du RGPD ne sont pas concernés au même titre par l'exigence de continuité de protection. Le Groupe de l'Article 29 a expliqué que ces dérogations concernent des cas dans lesquels les risques pour la personne en cause sont relativement faibles ou où d'autres intérêts peuvent être considérés comme primant le droit de la personne concernée au respect de la vie privée. Il a en outre précisé qu'elles appelaient une interprétation « stricte » et ne pouvaient servir, en principe, de base juridique pour des transferts massifs, répétitifs ou structurels. Voy. Groupe de l'article 29, Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995, 25 novembre 2005, WP 114.

(167) Le destinataire pouvant être responsable de traitement ou sous-traitant.

(168) Chr. Kuner, « Reality and Illusion in EU Data Transfer Regulation Post Schrems », *Legal Studies Research Paper Series* No. 14/2016, March 2016, pp. 26-28, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346.

des requêtes gouvernementales d'accès sauf si le droit national applicable l'interdit. Elles prévoient aussi l'obligation pour le destinataire d'informer le responsable de traitement de toute modification du cadre légal interne applicable lorsqu'il est susceptible d'avoir « des conséquences négatives importantes » (« *substantial adverse effect* ») sur les garanties offertes par les clauses (169). Les BCRs, quant à elles, contiennent des obligations similaires pour les filiales d'une multinationale vis-à-vis de l'entité européenne désignée responsable de la protection des données. En cas de conflits, l'entreprise est tenue d'adopter une « décision responsable » et de consulter l'autorité de protection des données compétente en cas de doutes (170).

La Commission européenne s'est engagée à étudier les modifications nécessaires à apporter à ces instruments, ainsi qu'aux autres décisions d'adéquation, en vue de les rendre compatibles avec la décision de la Cour. Mais ces changements devraient surtout porter sur les pouvoirs de contrôle des autorités de protection des données tels qu'ils ont été reconnus par la Cour en matière de transferts, y compris en présence d'une décision d'adéquation (171). Comme nous l'avons mentionné dans notre première partie, le Groupe de l'article 29 a publié des lignes directrices relatives aux « garanties essentielles » applicables dans le domaine de la surveillance, devant être respectées dans tous les cas de transferts, quelles que soient leurs bases juridiques. Les autorités de protection des données se baseront sur ces lignes directrices pour autoriser l'usage de BCRs ou clauses contractuelles *ad hoc*.

Dans ce système, les autorités de protection des données peuvent intervenir à des stades différents. Au moment de l'adoption de BCRs ou de clauses contractuelles *ad hoc* soumises à approbation, elles pourront examiner dans les cas individuels, et au-delà du contenu des clauses de protection des données, les pays de destination concernés afin d'évaluer si les « garanties essentielles » sont respectées. Elles peuvent également, comme cela a été rappelé avec insistance par la Cour, examiner toute plainte en relation avec le niveau de protection conféré à des données transférées hors de l'Union. Lorsqu'elles ne seront pas convaincues du respect des garanties essentielles, ces autorités pourront suspendre des transferts ou catégories de transferts vers certaines destinations.

---

(169) Voy. notamment la Clause n° 5 de la décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil, *J.O.U.E.*, n° L 39, 12 février 2010.

(170) Groupe de l'article 29, Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes, 24 juin 2008, WP 154, p. 9.

(171) COM(2015) 566 final, précité, p. 16.

Le Groupe de l'Article 29, futur Comité Européen de la Protection des Données (CEPD), prend très au sérieux son rôle de supervision accru des transferts internationaux, où le respect des « garanties essentielles » va jouer un rôle important. Toutefois, ce modèle largement basé sur la supervision et le contrôle au *cas par cas* des transferts ou catégories de transferts a des limites. Tout d'abord, dans le régime actuel et à venir, l'usage des clauses contractuelles types n'est et ne sera soumis à aucune autorisation et/ou approbation préalable d'une autorité nationale de protection des données. Aussi l'usage de clauses types par les entreprises permet d'échapper au « viseur » des autorités de protection des données. En outre, l'ampleur de la tâche de supervision qui incombe aux autorités de contrôle nous paraît très complexe au regard de la multitude des transferts internationaux de données. Il faudra, au cas par cas, examiner les catégories de transferts de données concernées et les mesures de surveillance applicables dans le pays en question, que ces mesures soient plus générales (surveillance stratégique des activités numériques) ou sectorielles (surveillance des données bancaires ou financières, par exemple).

B. — Vers une distinction entre destinataires *adéquats* et destinataires *sûrs* ?

Nous l'avons expliqué dans notre première partie, l'exigence d'adéquation est, dans le cadre du RGPD et à la suite de l'arrêt *Schrems*, très élevée. Seul un nombre réduit de pays devraient pouvoir accéder à une reconnaissance d'adéquation et ainsi, faire partie intégrante de l'espace de libre circulation des données à caractère personnel mis en place par le droit de l'Union (172). Tout pays considéré comme adéquat bénéficie des mêmes privilèges que les États membres, c'est-à-dire l'absence de restrictions aux flux de données entre eux. Il n'est pas anormal que cette reconnaissance d'adéquation soit accordée avec une grande vigilance et se retrouve réservée à un nombre limité de pays satisfaisant tant au critère d'un niveau de protection des données élevé (*cf.* partie I.A), qu'à celui du respect de l'État de droit et de protection substantiellement équivalente des droits fondamentaux (*cf.* partie I.B). Dans le même temps, la Commission entend promouvoir le recours aux instruments alternatifs en vue de libéraliser les flux de données vers les autres destinations.

(172) La Commission a annoncé ses priorités dans ce domaine, évoquant le Japon et la Corée du Sud, voy. Communication from the Commission to the European Parliament and the Council on Exchanging and Protecting Personal Data in a Globalized World of 10 January 2017, COM(2017) 7 final.

Toutefois, puisque les risques posés par les pratiques de surveillance excessive en vigueur dans certains pays du monde pourront difficilement être levés dans des BCRs ou clauses contractuelles entre entreprises, de tels instruments alternatifs ne devraient pouvoir être utilisés, selon nous, que pour des transferts vers des *pays sûrs*. Par «*pays sûrs*», nous proposons d'entendre les pays qui, s'ils ne remplissent pas l'ensemble des conditions nécessaires à une reconnaissance d'adéquation, apportent la démonstration du respect des «garanties essentielles» énoncées par le Groupe de l'article 29 dans le domaine de la surveillance (*cf*. partie I.B.2). Tandis qu'il est désormais courant d'affirmer que les données personnelles constituent le pétrole du XXI^e^ siècle, alors qu'il s'agit dans l'ordre juridique européen d'une question de droits fondamentaux, nous croyons que la Commission européenne pourrait endosser, en première ligne, la responsabilité de l'identification de pays présumés *sûrs* pour les transferts de données dans le cadre de clauses contractuelles types ou de BCRs.

Une telle liste de pays *sûrs*, parallèle à celle de pays reconnus comme offrant une protection adéquate, permettrait aux entreprises européennes de déterminer dans quels États elles peuvent organiser leurs activités de traitement avec la plus grande sécurité juridique. Cette liste permettrait aux autorités de protection des données et futur Comité européen de préserver leurs ressources pour leurs activités de contrôle du respect des garanties suffisantes apportées par des BCRs ou clauses contractuelles. En outre, une liste de pays sûrs accroîtrait la transparence vis-à-vis des personnes concernées. En effet, selon le RGPD, celles-ci devront être informées des pays tiers vers lesquels leurs données sont susceptibles d'être transférées et des garanties appropriées mises en place par le responsable de traitement (173). Pour les citoyens européens, il serait donc particulièrement opportun de pouvoir vérifier si les pays de destination en question figurent soit sur la liste des pays «adéquats», soit au minimum sur celle des pays «sûrs».

Sur le plan méthodologique, si la Commission européenne réussit à juger de l'adéquation du niveau de protection des données conférée par un État tiers, évaluation qui porte notamment sur le respect des garanties essentielles par l'État en question, comme on l'a vu précédemment, il n'y aucune raison qu'une méthodologie ciblée sur le seul respect de ces garanties essentielles ne puisse être développée et testée. L'on pourrait objecter qu'une telle proposition est politiquement difficile à mettre en œuvre tant la question des pouvoirs des services de police et de renseignements est sensible pour les États nations. Aussi, certains États, pour des raisons de souveraineté, ne

(173) Art. 13.1, f), du RGPD.

seront pas intéressés de figurer sur une telle liste. Dans le même temps, ceux qui voudraient intensifier leurs relations économiques avec l'Union dans le domaine des services de traitement de données, pourraient voir dans le statut de «*pays sûr*» une alternative à l'adéquation leur permettant d'accroître l'attractivité de leur territoire pour ces services. Dans tous les cas, l'octroi de la qualification de *pays sûrs* devrait reposer sur la volonté étatique.

Au-delà des pays *adéquats*, pour lesquels aucune restriction n'est applicable, et des pays *sûrs*, pour lesquels les BCRs et clauses contractuelles apportant des garanties suffisantes pourraient être utilisées, les exceptions, qui n'ont pas vocation à s'appliquer pour les transferts massifs ou structurels, pourraient toujours être utilisées quelle que soit la destination.

Si une entreprise devait procéder à des transferts massifs ou structurels vers des pays autres que des pays sûrs, il lui reviendrait alors la responsabilité de s'assurer que la législation du pays tiers concerné ne portera pas atteinte au niveau de protection des données pour les transferts spécifiques envisagés. Dans la mesure où l'Union européenne représente l'un des plus grands marchés du monde de données à caractère personnel en raison de son niveau de vie élevé et de digitalisation de la société très avancé, la Commission européenne a les moyens politiques et diplomatiques d'inciter certains États tiers à s'engager à respecter des garanties essentielles en matière de surveillance.

Conclusion

L'arrêt *Schrems* aura eu un impact considérable sur les échanges de données entre l'Union européenne et les pays tiers. Il aura permis de mettre en lumière un critère crucial, même si délicat à vérifier, pour autoriser ces échanges : celui de la protection des libertés et droits fondamentaux dans le cadre des activités de surveillance de l'État tiers.

Les quatre «garanties essentielles» identifiées par le Groupe de l'article 29 offrent les clés pour évaluer le niveau de protection garanti par un pays tiers dans l'exercice de ses activités de surveillance. Il s'agit de l'exigence de légalité de telles activités qui doivent s'opérer dans le cadre de règles claires, précises et accessibles. Il faut ensuite démontrer la nécessité et la proportionnalité des mesures, l'existence d'un mécanisme de supervision indépendant et le droit à un recours effectif. À travers ces quatre garanties essentielles, auxquelles s'ajoute le respect de l'État de droit, c'est la protection substantiellement équivalente ou non des droits fondamentaux qui est mesurée.

Dans cette optique, la négociation du *Privacy Shield* a apporté d'indéniables améliorations au système du défunt *Safe Harbor*, malgré les défauts et faiblesses que nous avons relevés dans les pages qui précèdent. Cela étant,

les révélations d'Edward Snowden ont durablement ouvert la voie à une période où les transferts internationaux de données font l'objet d'une attention accrue de la société civile, illustrée notamment par les deux recours en annulation introduits par des ONG contre la décision *Privacy Shield* de la Commission. En outre, la volonté du président Donald Trump de remettre en cause toute protection de la vie privée pour les non-Américains en vertu du *Privacy Act* mérite d'être soulignée, tant elle montre que les garanties obtenues des États-Unis dans ce domaine peuvent être fragiles (174).

Mais la décision *Schrems* a des conséquences bien au-delà des rapports transatlantiques. Selon nous, c'est en fait dans tous les cas de transfert de données que les garanties essentielles doivent désormais être respectées, que ces transferts s'appuient sur une décision d'adéquation ou sur l'utilisation des instruments alternatifs que sont les clauses contractuelles et les BCRs. En effet, l'approche de la Cour dans l'arrêt *Schrems* replace le droit fondamental à la protection des données au cœur du dispositif des flux transfrontières. Or, les BCRs et les clauses contractuelles présentent les mêmes défauts que le *Safe Harbor* puisqu'ils n'offrent que des garanties très limitées en matière de surveillance.

À notre sens, le recours aux BCRs ou aux clauses contractuelles s'indique quand l'État destinataire des données n'offre pas de protection adéquate, mais n'est pas justifié en présence de pratiques de surveillance excessive. Seuls les flux de données encadrés par ces instruments à destination de ce que nous avons appelé ci-dessus les *pays sûrs,* c'est-à-dire démontrant le respect des « garanties essentielles », devraient être admissibles.

Cette politique, qui pourrait avoir pour effet de restreindre les flux transfrontières vers les États ni adéquats ni sûrs, aurait néanmoins le mérite de la cohérence avec la justification des restrictions au commerce international qui réside dans la protection de la vie privée et des données à caractère personnel (175). En outre, elle permettrait à la société civile, de plus en plus soucieuse du sort réservé aux données transférées, d'avoir une vision sur la politique de flux transfrontières de l'Union. En effet, en l'état actuel, les personnes concernées ignorent quels États tiers offrent ou non des garanties en matière de surveillance et surtout, elles ignorent vers quelles destina-

(174) Executive Order of the White House, Enhancing Public Safety in the Interior of the United States, Sec. 14. Privacy Act : « *Agencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information* », www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

(175) Article XIV de l'Accord général sur le commerce et les services.

tions les autorités de protection des données autorisent les transferts ou les refusent. Enfin, cette politique offrirait une sécurité juridique accrue aux entreprises en leur permettant de faire les choix stratégiques nécessaires quant aux pays de destination où elles choisissent d'organiser leurs activités de traitement de données.

Liste des principaux actes législatifs et autres cités

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, *J.O.C.E.*, nº L 281, 23 novembre 1995.

Règlement (UE) nº 2016/679 du Parlement 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, Règlement général sur la protection des données ou RGPD, *J.O.C.E.*, nº L 119, p. 1.

Décision 2000/520/CE de la Commission européenne, du 26 juillet 2000, conformément à la directive 95/46, 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, *J.O.C.E.*, nº L 215, p. 7. Décision *Safe Harbor*.

Décision d'exécution (UE) 2016 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, *J.O.C.E.*, nº L 207, 1er août 2016, pp. 1-112. Décision *Privacy Shield.*

Liste des principaux arrêts de la CJUE cités

CJUE (GC), arrêt du 8 avril 2014, *Digital Rights Ireland*, aff. jtes C-293/12, C-594/12, EU:C:2014:238.

CJUE (GC), arrêt du 6 octobre 2015, *Maximillian Schrems c. Data Protection Commissioner*, aff. C-362/14, EU:C:2015:650.

CJUE (GC), arrêt du 21 décembre 2016, *Tele2 Sverige AB*, aff. jtes C-203/15 et C-698/15, EU:C:2016:970.