COMMISSION
EUROPÉENNE

Bruxelles, le 6.11.2015
COM(2015) 566 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

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)

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

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)

1. INTRODUCTION: L'INVALIDATION DE LA DECISION CONCERNANT LA SPHERE DE SECURITE RELATIVE A LA PROTECTION DES DONNEES

L'arrêt de la Cour de justice de l'Union européenne (ci-après: «la Cour de justice» ou «la Cour») du 6 octobre 2015 dans l'affaire C-362/14 (Schrems)[1] souligne l'importance du droit fondamental à la protection des données à caractère personnel qui est garanti par la charte des droits fondamentaux de l'UE, y compris lorsque ces données sont transférées vers des pays tiers.

Les transferts de données à caractère personnel sont un élément essentiel de la relation transatlantique. L'UE et les États-Unis sont le principal partenaire commercial l'un de l'autre, et les transferts de données font de plus en plus partie intégrante de leurs échanges.

Afin de faciliter ces flux de données tout en assurant un niveau élevé de protection des données à caractère personnel, la Commission a reconnu, par l'adoption de la décision de la Commission 2000/520/CE du 26 juillet 2000, la pertinence de la protection assurée par les principes de la sphère de sécurité (ci-après: «la décision "sphère de sécurité"»). Dans cette décision, qui se fonde sur l'article 25, paragraphe 6, de la directive 95/46/CE[2], la Commission avait reconnu que les «principes de la "sphère de sécurité" relatifs à la protection de la vie privée» et les «questions souvent posées» («Frequently asked questions» — FAQ) publiées par le Department of Commerce des États-Unis assurent un niveau adéquat de protection pour le transfert de données à caractère personnel à partir de l'UE[3]. Les données à caractère personnel pouvaient ainsi être transférées librement des États membres de l'UE vers des entreprises établies aux États-Unis qui adhéraient à ces principes, malgré l'absence d'un instrument général régissant la protection des données aux États-Unis. Le fonctionnement de l'accord sur la sphère de sécurité se fondait sur les engagements et l'autocertification des entreprises qui y avaient adhéré. L'adhésion aux principes de la sphère de sécurité et au FAQ est volontaire, mais en vertu de la législation américaine, les règles y afférentes deviennent

[1] Arrêt du 6 octobre 2015 dans l'affaire C-362/14, Maximilian Schrems c/Data Protection Commissioner, EU:C:2015:650 (ci-après également: «l'arrêt» ou «l'arrêt Schrems»).

[2] 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, JO L 281 du 23.11.1995, p. 31 (ci-après: «directive 95/46/CE» ou «la directive»).

[3] Aux fins de la présente communication, le terme «UE» couvre également l'EEE. Dès lors, les références aux «États membres» sont réputées englober également les pays membres de l'EEE.

contraignantes dès lors qu'une entreprise y adhère, sous le contrôle de la Federal Trade Commission (FTC, Commission fédérale du commerce)[4].

Dans son arrêt du 6 octobre 2015, la Cour a déclaré la décision relative à la sphère de sécurité invalide. Dans ce contexte, la présente communication a pour but de présenter des outils alternatifs pour l'exécution des transferts transatlantiques de données conformément à la directive 95/46/CE en l'absence de décision concernant le caractère adéquat du niveau de protection. Elle traite aussi succinctement des conséquences que l'arrêt aura sur d'autres décisions de la Commission concernant le caractère adéquat du niveau de protection. Dans l'arrêt, la Cour a précisé que de telles décisions ne peuvent être prises en vertu de l'article 25, paragraphe 6, de la directive 95/46/CE que si la Commission a constaté que le pays tiers concerné offre un niveau de protection des données à caractère personnel qui, sans être forcément identique, est substantiellement équivalent à celui garanti au sein de l'UE en vertu de la directive lue à la lumière de la charte des droits fondamentaux. S'agissant spécifiquement de la décision sur la sphère de sécurité, la Cour a conclu qu'elle avait été adoptée sans que la Commission ait constaté un nombre suffisant de limitations en ce qui concerne l'accès par les autorités publiques américaines aux données transférées sur la base de cette décision et l'existence d'une protection juridique efficace contre de telles ingérences. En particulier, la Cour a précisé qu'il y a lieu de considérer que la législation permettant aux autorités publiques d'avoir accès au contenu de communications électroniques de manière généralisée porte atteinte au contenu essentiel du droit fondamental au respect de la vie privée. La Cour a en outre confirmé que même si une décision concernant le caractère adéquat du niveau de protection avait été prise au titre de l'article 25, paragraphe 6, de la directive 95/46/CE, les autorités chargées de la protection des données (DPA) dans les États membres restent investies des pouvoirs et de l'obligation de s'assurer, en toute indépendance, que les règles relatives aux transferts de données vers un pays tiers sont conformes aux exigences fixées dans la directive 95/46/CE lue à la lumière des articles 7, 8 et 47 de la charte des droits fondamentaux. La Cour a toutefois également rappelé qu'elle seule dispose du pouvoir d'annuler un acte de l'UE tel qu'une décision de la Commission concernant le caractère adéquat du niveau de protection.

L'arrêt de la Cour se réfère à la communication de la Commission de 2013 concernant le fonctionnement de la sphère de sécurité du point de vue des citoyens de l'UE et des entreprises établies dans l'UE[5], où la Commission a relevé plusieurs lacunes et formulé treize recommandations. Se fondant sur ces recommandations, la Commission négocie avec les

[4] Pour obtenir des informations plus précises sur l'accord «Sphère de sécurité», voir la communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, COM/2013/847 final.

[5] Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire, COM/2013/847 final, 27.11.2013. Voir également la communication de la Commission au Parlement européen et au Conseil, «Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique», COM(2013) 846 final, 27.11.2013, et le mémo associé «Restaurer la confiance dans les flux de données entre l'Union européenne et les États-Unis — Foire aux questions», MEMO/13/1059, 27.11.2013.

autorités américaines depuis janvier 2014 afin de mettre en place un nouvel accord plus solide pour les échanges transatlantiques de données.

Suite à l'arrêt, la Commission maintient son objectif d'établir un nouveau cadre solide pour les transferts transatlantiques de données à caractère personnel. Elle a, à cette fin, immédiatement repris et intensifié ses négociations avec le gouvernement américain afin que tout nouvel accord concernant les transferts transatlantiques de données à caractère personnel soit totalement conforme aux critères établis par la Cour. Il est dès lors essentiel qu'un tel cadre comporte des limites, des garanties et des mécanismes de contrôle judiciaire suffisants pour garantir que les données à caractère personnel des citoyens de l'UE resteront protégées, y compris en ce qui concerne l'éventualité de l'accès des pouvoirs publics pour des motifs tenant au respect des lois et à la sécurité nationale. Entre-temps, le secteur professionnel a fait part de ses préoccupations quant aux possibilités de maintien des transferts de données[6]. Il apparaît donc nécessaire de clarifier les conditions dans lesquelles ces transferts peuvent se poursuivre. Ceci a amené le groupe de travail «Article 29», l'organe consultatif indépendant qui réunit des représentants de toutes les autorités chargées de la protection des données (DPA) des États membres, ainsi que le contrôleur européen de la protection de données, à publier, le 16 octobre, une déclaration[7] sur les premières conclusions à tirer du jugement. Cette déclaration contenait, entre autres, les orientations suivantes concernant les transferts de données:

- les transferts ne peuvent plus être basés sur la décision «Sphère de sécurité» de la Commission, qui est désormais invalide;

- des clauses contractuelles types (ci-après également: «CCT») et des règles d'entreprise contraignantes (ci-après également: «REC») peuvent entre-temps servir de base aux transferts de données, bien que le groupe de travail «Article 29» ait également déclaré qu'il poursuivra son analyse de l'impact de l'arrêt sur ces outils alternatifs.

Dans sa déclaration, le groupe de travail a en outre invité les États membres et les institutions de l'UE à discuter avec les autorités américaines dans le but de trouver des solutions juridiques et techniques pour les transferts de données; selon le groupe de travail «Article 29», les négociations visant à instaurer une nouvelle sphère de sécurité pourraient faire partie de cette solution.

---

6 Les représentants des associations professionnelles ont notamment formulé ces préoccupations lors d'une réunion qui a été organisée par le vice-président Ansip et les commissaires Jourová et Oettinger peu après la publication de l'arrêt Schrems, le 14 octobre. Voir le Daily News du 14.10.2015 (MEX/15/5840). Voir aussi: *Open letter on the implementation of the CJEU Judgement on Case C-362/14 Maximillian Schrems v Data Protection Commissioner*, lettre ouverte datée du 13 octobre 2015 adressée au président de la Commission, Jean-Claude Juncker, et signée par diverses associations professionnelles et entreprises européennes et américaines: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=1045&PortalId=0&TabId=353

7 Déclaration du groupe de travail «Article 29», disponible sur Internet à l'adresse: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf

Le groupe de travail «Article 29» a fait savoir que si aucune solution adéquate n'est trouvée avec les autorités américaines d'ici fin janvier 2016 et en fonction de l'évaluation des outils alternatifs pour les transferts de données, les DPA prendront toutes les mesures jugées nécessaires et appropriées, y compris des mesures coercitives coordonnées.

Enfin, le groupe de travail «Article 29» a souligné que la recherche de solutions durables permettant d'appliquer l'arrêt de la Cour relève de la responsabilité conjointe des DPA, des institutions de l'UE, des États membres et des entreprises. Il a en particulier vivement encouragé les entreprises à envisager de mettre en place toute solution juridique et technique permettant d'atténuer les risques éventuels qu'elles rencontrent lors du transfert de données.

La présente communication est sans préjudice des obligations incombant aux DPA d'examiner la légalité de ces transferts en toute indépendance et des pouvoirs dont ils sont investis à cette fin[8]. Elle ne fixe aucune règle contraignante et respecte pleinement la compétence dont sont investies les juridictions nationales d'interpréter le droit applicable et, le cas échéant, de saisir la Cour de justice en vue d'obtenir une décision préjudicielle. La présente communication ne peut être utilisée aux fins de faire valoir un quelconque droit légal individuel ou collectif.

2. AUTRES BASES POSSIBLES POUR LES TRANSFERTS TRANSATLANTIQUES DE DONNEES A CARACTERE PERSONNEL

Les règles concernant les transferts internationaux de données qui sont fixées dans la directive 95/46/CE s'appuient sur une distinction claire entre les transferts vers des pays tiers garantissant un niveau adéquat de protection (article 25 de la directive), d'une part, et les transferts vers des pays tiers qui n'offrent pas un tel niveau de protection (article 26 de la directive), d'autre part.

L'arrêt Schrems examine les conditions dans lesquelles, en vertu de l'article 25, paragraphe 6, de la directive 95/46/CE, la Commission peut constater qu'un pays tiers assure un niveau de protection adéquat.

Lorsqu'il appert que le pays tiers vers lequel les données à caractère personnel doivent être exportées en provenance de l'UE n'offre pas ce niveau de protection adéquat, l'article 26 de la directive 95/46/CE prévoit un nombre de motifs alternatifs sur la base desquels les transferts peuvent néanmoins avoir lieu. Des transferts peuvent en particulier être exécutés lorsque l'entité chargée de déterminer les finalités et les moyens du traitement de données à caractère personnel (le «responsable du traitement»):

– offre des garanties suffisantes, au sens de l'article 26, paragraphe 2, de la directive 95/46/CE, au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants.

[8] Voir l'article 8, paragraphe 3, de la charte des droits fondamentaux et l'article 16, paragraphe 2, du TFUE. Cette indépendance a également été soulignée par la Cour dans l'arrêt Schrems.

Ces garanties peuvent notamment être offertes au moyen de clauses contractuelles appropriées liant l'exportateur et l'importateur des données (voir points 2.1 et 2.2 ci-dessous). Il peut notamment s'agir de CCT émises par la Commission et, en ce qui concerne les transferts entre les différentes entités d'un groupe multinational, de REC autorisées par les DPA; ou

– se fonde sur l'une des dérogations expressément énumérées à l'article 26, paragraphe 1, points a) à f), de la directive 95/46/CE (voir point 2.3 ci-dessous).

Par comparaison avec les décisions concernant le caractère adéquat du niveau de protection qui sont prises après avoir évalué globalement le système d'un pays tiers donné et qui peuvent, en principe, couvrir tous les transferts vers ce système, ces autres bases possibles pour les transferts ont à la fois un champ d'application plus limité (puisqu'elles ne s'appliquent qu'à des flux de données spécifiques) et une couverture plus large (puisqu'elles ne se limitent pas forcément à un pays spécifique). Elles concernent les flux de données d'entités particulières qui ont décidé de recourir à l'une des possibilités offertes par l'article 26 de la directive 95/46/CE. De plus, dès lors qu'ils fondent leurs transferts sur ces motifs et ne s'appuient donc pas sur une décision de la Commission concernant le caractère adéquat du niveau de protection, il appartient aux exportateurs et aux importateurs de données de veiller à ce que les transferts soient conformes aux exigences de la directive.

2.1. Solutions contractuelles

Comme le souligne le groupe de travail «Article 29», afin d'offrir un niveau de protection adéquat au sens de l'article 26, paragraphe 2, de la directive 95/46/CE, des clauses contractuelles «doivent compenser, de manière satisfaisante, l'absence d'un niveau général adéquat de protection, en incluant les éléments essentiels de protection manquants dans une situation particulière donnée»[9]. Afin de faciliter l'utilisation de ces instruments lors de transferts internationaux, la Commission a approuvé, conformément à l'article 26, paragraphe 4, de la directive, quatre séries de CCT qui sont réputées satisfaire aux exigences de l'article 26, paragraphe 2, de la directive. Deux séries de clauses types se rapportent aux transferts entre responsables de traitement[10], les deux autres concernant les transferts entre un responsable de traitement et un sous-traitant agissant selon les instructions du premier[11].

[9] Voir le groupe de travail «Article 29», 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), 24 juillet 1998, p. 16.

[10] Décision 2001/497/CE de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE, JO L 181, 4.7.2001, p. 19, et décision 2004/915/CE de la Commission du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers, JO L 385, 29.12.2004, p. 74.

[11] Décision 2002/16/CE de la Commission du 27 décembre 2001 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, JO L 6, 10.1.2002, p. 52, et décision de la Commission 2010/87/UE 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, JO L 39, 12.2.2010, p. 5. La première décision, qui a été révoquée par la seconde, s'applique uniquement aux contrats conclus avant le 15 mai 2010.

Chacune de ces séries de clauses types énonce les obligations respectives des exportateurs et des importateurs de données. Celles-ci prévoient des obligations concernant, entre autres, les mesures de sécurité, les informations à communiquer à la personne concernée en cas de transfert de données sensibles, la notification à l'exportateur des données de demandes d'accès formulées par des autorités répressives des pays tiers et de tout accès accidentel ou non autorisé, et les droits dont disposent les personnes concernées à l'égard de leurs données à caractère personnel en ce qui concerne leur accès, leur rectification et leur effacement, ainsi que les règles d'indemnisation de la personne concernée en cas de dommage découlant d'une violation par l'une des parties aux CCT. Les modèles types requièrent également que les personnes concernées dans l'UE aient la possibilité de faire valoir devant un DPA et/ou une juridiction de l'État membre dans lequel l'exportateur des données est établi les droits que leurs confèrent clauses contractuelles en tant que tiers bénéficiaires[12]. Ces droits et obligations doivent être fixés dans des clauses contractuelles, car, contrairement à la situation où la Commission a fait une constatation concernant le caractère adéquat du niveau de protection, il n'est pas possible de présumer que l'importateur de données dans le pays tiers est soumis à un système adéquat de contrôle et de bonne exécution des règles en matière de protection des données.

Les décisions de la Commission étant obligatoires dans tous leurs éléments dans les États membres, l'intégration des CCT dans un contrat signifie que les autorités nationales sont, en principe, soumises à l'obligation de les accepter. Elles ne peuvent dès lors refuser le transfert des données vers un pays tiers en se fondant uniquement sur l'argumentation que ces CCT n'offrent pas suffisamment de garanties. Leur pouvoir d'examiner ces clauses à la lumière des exigences énoncées par la Cour dans l'arrêt Schrems n'en est pas diminué pour autant. En cas de doutes, elles doivent saisir une juridiction nationale, laquelle peut, à son tour, se tourner vers la Cour de justice pour obtenir une décision préjudicielle. Si, dans la plupart des législations des États membres transposant la directive 95/45/CE, il n'existe pas d'obligation d'obtenir une autorisation nationale préalable pour procéder au transfert, certains États membres maintiennent toutefois un système de notification ou d'autorisation préalable pour l'utilisation des CCT. Dans pareille situation, le DPA national doit comparer les clauses réellement contenues dans le contrat avec les CCT et s'assurer qu'aucune modification n'y a été apportée[13]. Si les clauses sont utilisées sans modification[14], l'autorisation est en principe[15]

---

12 Voir par exemple le considérant 6 de la décision 2004/915/CE de la Commission et la clause V de son annexe; clause 7 de l'annexe de la décision 2010/87/UE de la Commission.

13 Il convient de souligner que la proposition de règlement général de protection des données (COM(2012) 11 final) prévoit que les transferts fondés sur des CCT ou des REC, dans la mesure où elles ont été adoptées par la Commission ou conformément au mécanisme de contrôle de la cohérence envisagé, ne requièrent pas d'autre autorisation.

14 L'utilisation de CCT n'empêche toutefois pas les parties d'accepter d'ajouter d'autres clauses tant que celles-ci ne contredisent pas directement ou indirectement les clauses approuvées par la Commission et ne portent pas préjudice aux libertés et aux droits fondamentaux des personnes concernées. Voir Commission européenne, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries* (FAQ B.1.9), p. 28 (disponible sur l'Internet à l'adresse: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf).

15 Si un DPA a des doutes concernant la compatibilité des CCT avec les exigences de la directive, il devrait soumettre la question à une juridiction nationale qui peut ensuite introduire une demande de décision préjudicielle auprès de la Cour de justice (cf. points 51, 52, 64 et 65 de l'arrêt Schrems).

automatiquement accordée[16]. Comme expliqué ci-dessous (voir point 2.4), cela n'affecte en rien les mesures supplémentaires que l'exportateur de données pourra devoir prendre, en particulier sur la base des informations qu'il reçoit de l'importateur de données concernant les changements apportés au système juridique du pays tiers qui sont susceptibles de le mettre dans l'impossibilité de s'acquitter des obligations lui incombant en vertu du contrat. Lors de l'application des CCT, tant les exportateurs que les importateurs de données (ces derniers en vertu du contrat auquel ils sont parties) relèvent du contrôle des DPA.

L'adoption des CCT n'interdit pas aux entreprises de se fonder sur d'autres instruments tels que des accords contractuels ponctuels afin de démontrer que les modalités de leurs transferts offrent des garanties suffisantes au sens de l'article 26, paragraphe 2, de la directive 95/46/CE. Conformément à l'article 26, paragraphe 2, de la directive, ces transferts doivent être approuvés individuellement par les autorités nationales. Certains DPA ont également développé des orientations dans ce domaine, notamment sous la forme de contrats standardisés ou de règles détaillées à suivre pour la rédaction des clauses de transferts de données. La plupart des contrats actuellement utilisés par les entreprises en vue d'exécuter leurs transferts internationaux de données reposent toutefois sur les CCT approuvées par la Commission[17].

2.2. Transferts intragroupes

Afin de transférer des données à caractère personnel de l'UE vers des filiales établies en dehors de l'UE tout en respectant les exigences énoncées à l'article 26, paragraphe 2, de la directive 95/46/CE, une multinationale peut adopter des REC. Ce type de codification des pratiques ne peut servir de base qu'aux transferts effectués au sein du groupe d'entreprises.

L'utilisation de REC permet donc de faire circuler les données à caractère personnel librement entre les diverses entités d'un groupe partout dans le monde en les dispensant de l'obligation de passer des accords contractuels entre elles, tout en garantissant que le même niveau élevé de protection de données à caractère personnel est respecté dans l'ensemble du groupe grâce à un ensemble unique de règles contraignantes et exécutables. Le fait de n'avoir qu'un seul ensemble de règles crée un système plus simple et plus efficace dont la mise en œuvre par le personnel et la compréhension par les personnes concernées sont facilitées. Afin d'aider les entreprises à rédiger des REC, le groupe de travail «Article 29» a élaboré des exigences de fond (par exemple limitation de l'objet, sécurité de traitement, informations transparentes pour les personnes concernées, restrictions concernant les transferts ultérieurs en dehors du groupe, droit individuel d'accès, de rectification et d'effacement) et procédurales (par exemple

[16] Le groupe de travail «Article 29» a établi une procédure de coopération spécifique entre les DPA pour l'approbation des clauses contractuelles qu'une entreprise souhaite utiliser dans différents États membres. Voir le groupe de travail «Article 29», *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on 'Contractual clauses' Considered as compliant with the EC Model Clause*, (WP 226), 26 novembre 2014. Voir également la clause VII de l'annexe de la décision 2004/915/CE de la Commission et la clause 10 de l'annexe de la décision 2010/87/UE de la Commission.

[17] Voir le groupe de travail «Article 29», *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on 'Contractual clauses' Considered as compliant with the EC Model Clause*, (WP 226), 26 novembre 2014, p. 2.

audits, contrôle de la conformité, traitement des plaintes, coopération avec les DPA, responsabilité et juridiction) pour les REC en se fondant sur les normes de protection de données de l'UE[18]. Ces règles sont non seulement contraignantes pour les membres du groupe corporatif, mais elles sont aussi exécutables dans toute l'UE, à l'instar des CCT: en tant que bénéficiaires tiers, les personnes individuelles dont les données sont traitées par une entité du groupe ont la capacité, de faire respecter les REC en déposant une plainte devant un DPA et d'engager une action devant une juridiction d'un État membre. Les REC doivent en outre désigner au sein de l'UE une entité qui accepte d'assumer la responsabilité en cas de violations des règles par un membre du groupe en dehors de l'UE qui est lié par ces règles.

La plupart des législations des États membres transposant la directive prévoient que les transferts de données fondés sur des REC doivent être autorisés par le DPA de l'État membre à partir duquel la multinationale entend transférer des données. Afin de faciliter et d'accélérer le processus et de réduire la charge qui pèse sur les demandeurs, le groupe de travail «Article 29» a rédigé un formulaire de demande standardisé[19] et institué entre les DPA concernés une procédure de coopération spécifique[20] qui prévoit la désignation d'une «autorité-chef de file» chargée de la procédure d'approbation.

2.3. Dérogations

En l'absence de décision concernant le caractère adéquat du niveau de protection prise en vertu de l'article 25, paragraphe 6, de la directive 95/46/CE et indépendamment de l'utilisation de CCT et/ou de REC, les données à caractère personnel peuvent néanmoins être transférées vers des entités établies dans un pays tiers dans la mesure où l'une des dérogations alternatives énoncées à l'article 26, paragraphe 1, de la directive 95/46/CE s'applique:[21]

– la personne concernée a indubitablement donné son consentement au transfert envisagé;

[18] Voir groupe de travail «Article 29», Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes (WP 153), 24 juin 2008, Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes (WP 154), 24 juin 2008 et Document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes (WP 155), 24 juin 2008.

[19] Groupe de travail «Article 29», *Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data* (WP 133), 10 janvier 2007.

[20] Groupe de travail «Article 29», Document de travail relatif à une procédure de coopération en vue de l'émission d'avis communs sur le caractère adéquat de la protection offerte par les «règles d'entreprise contraignantes» (WP 107), 14 avril 2005.

[21] Comme l'a souligné le groupe de travail «Article 29», dans la mesure où d'autres dispositions de la directive 95/46/CE contiennent des exigences se rapportant à l'utilisation de ces dérogations (par exemple les limitations de l'article 8 concernant le traitement de données sensibles), celles-ci doivent être respectées. Voir groupe de travail «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 (WP 114), 25 novembre 2005, p. 9. Voir également Commission européenne, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries* (FAQ D.2), p. 50.

– le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée;

– le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers;

– le transfert est nécessaire ou rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important[22], ou pour la constatation, l'exercice ou la défense d'un droit en justice;

– le transfert est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée;

– le transfert intervient au départ d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime, dans la mesure où les conditions légales pour la consultation sont remplies dans le cas particulier.

Ces motifs permettent de déroger à l'interdiction générale de transferts de données à caractère personnel vers des entités établies dans un pays tiers qui n'offre pas un niveau adéquat de protection. En l'occurrence, l'exportateur de données n'est pas tenu d'offrir l'assurance que l'importateur de données fournira une protection adéquate et il ne devra généralement pas obtenir d'autorisation préalable pour le transfert auprès des autorités nationales compétentes. Néanmoins, compte tenu de leur caractère exceptionnel, le groupe de travail «Article 29» estime que ces dérogations doivent être interprétées de manière stricte[23].

Le groupe de travail «Article 29» a publié plusieurs documents d'orientation non contraignants concernant l'application de l'article 26, paragraphe 1, de la directive 95/46/CE[24], dont plusieurs règles de «meilleures pratiques» qui sont formulées de

---

22 Ceci peut inclure, par exemple, des transferts de données entre les autorités fiscales ou douanières ou entre des services compétents pour les questions de sécurité sociale (voir considérant 58 de la directive 95/46/CE). Les transferts entre les organes de supervision dans le secteur des services financiers peuvent également bénéficier de la dérogation. Voir groupe de travail «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), 24 juillet 1998, p. 25.

23 Groupe de travail «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 (WP 114), 25 novembre 2005, p. 20.

24 Groupe de travail «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), 24 juillet 1998; 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 (WP 114), 25 novembre 2005. Voir également Commission européenne, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries* (FAQ D.9), p. 48-54.

manière à orienter l'intervention des DPA[25]. Le groupe de travail recommande en particulier que les transferts de données à caractère personnel qui pourraient être qualifiés de transferts répétés, massifs ou structurels bénéficient de garanties suffisantes et, dans la mesure du possible, soient effectués dans un cadre juridique spécifique tel que des CCT ou des REC[26].

Dans la présente communication, la Commission traitera uniquement les dérogations qui apparaissent particulièrement pertinentes pour les transferts dans un contexte commercial suite à la constatation d'invalidité de la décision concernant la sphère de sécurité.

2.3.1. Transferts nécessaires à l'exécution d'un contrat ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée (article 26, paragraphe 1, point b))

Cette dérogation pourrait s'appliquer, par exemple, dans le contexte d'une réservation d'hôtel ou lorsque les informations concernant un paiement sont transférées vers un pays tiers afin d'effectuer un virement bancaire. Cependant, dans chacun de ces cas, le groupe de travail «Article 29» considère qu'il doit exister un «lien étroit et important», un «lien direct et objectif» entre la personne concernée et la finalité du contrat ou de la mesure précontractuelle («critère de nécessité»)[27]. La dérogation ne peut pas s'appliquer non plus aux transferts d'informations supplémentaires qui ne sont pas nécessaires pour le transfert ou aux transferts requis à d'autres fins que l'exécution du contrat (par exemple action de relance auprès des clients prospectés)[28]. En ce qui concerne les mesures précontractuelles, le groupe de travail «Article 29» a estimé que seuls les contacts initiés par la personne concernée (par exemple, une demande d'informations concernant un service particulier) seraient couverts, à l'exclusion de ceux qui résultent de démarches commerciales engagées par le responsable des données[29].

---

25 Groupe de travail «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 (WP 114), 25 novembre 2005, p. 10-11.

26 Groupe de travail «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 (WP 114), 25 novembre 2005, p. 11. Selon le groupe de travail, les transferts massifs ou répétés ne peuvent être exécutés que sur la base d'une dérogation lorsqu'il est impossible, en pratique, de recourir à des CCT ou des CER et lorsque les risques pour les personnes concernées sont faibles (par exemple transferts internationaux de fonds). Voir également Commission européenne, *Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries* (FAQ D.1), p. 49.

27 Groupe de travail «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 (WP 114), 25 novembre 2005, p. 15. Voir également Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis (WP 66), 24 octobre 2002.

28 Groupe de travail «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), 24 juillet 1998, p. 25. 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 (WP 114), 25 novembre 2005, p. 13.

29 Groupe de travail «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), 24 juillet 1998, p. 25.

2.3.2. Transferts nécessaires à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et un tiers (article 26, paragraphe 1, point c))

Cette dérogation pourrait s'appliquer, par exemple, lorsque la personne concernée est la bénéficiaire d'un transfert bancaire international ou lorsqu'un agent de voyage communique les données d'une réservation de vol à une compagnie aérienne. À nouveau, le critère de nécessité s'applique et requiert, dans ce cas, un lien étroit et important entre l'intérêt de la personne concernée et l'objet du contrat.

2.3.3. Transferts nécessaires ou rendus juridiquement obligatoires pour la constatation, l'exercice ou la défense d'un droit en justice (article 26, paragraphe 1, point d))

Cette dérogation pourrait s'appliquer, par exemple, lorsqu'une entreprise doit transférer des données en vue de se présenter en justice comme plaignant ou comme défendeur, ou de se défendre devant une autorité publique. Comme pour les deux précédentes, cette dérogation-ci est aussi soumise au critère de nécessité[30]: un lien étroit doit exister avec le litige ou la procédure juridique (ou administrative).

D'après le groupe de travail «Article 29», la dérogation ne peut s'appliquer que si les règles internationales concernant la coopération dans les procédures pénales ou civiles régissant le type de transfert ont été respectées compte tenu du fait notamment qu'elles découlent des dispositions de la convention de la Haye du 18 mars 1970 (convention sur l'obtention des preuves)[31].

2.3.4. Consentement au transfert envisagé indubitablement donné par la personne concernée (article 26, paragraphe 1, point a))

Le consentement peut servir de base aux transferts de données, mais plusieurs éléments doivent être pris en considération. Le consentement devant être donné au transfert «envisagé», ce consentement doit être donné de manière préalable au transfert particulier (ou à la catégorie particulière de transferts). Lorsque le consentement est demandé en ligne, le groupe de travail «Article 29» recommande l'utilisation de cases à cocher (au lieu de cases préalablement cochées)[32]. Étant donné que le consentement doit être indubitable, tout doute sur la question de savoir s'il a réellement été donné rendrait la dérogation inapplicable. Ceci signifiera

---

30 Groupe de travail «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 (WP 114), 25 novembre 2005, p. 17. En matière d'emploi, par exemple, il ne peut être recouru à la dérogation pour transférer tous les fichiers des salariés vers la société mère du groupe établie dans un pays tiers au motif d'une éventuelle future procédure en justice.

31 Convention de La Haye du 18 mars 1970 sur l'obtention des preuves à l'étranger en matière civile ou commerciale, 23 U.S.T. 2555, 847 RTNU 241. Cette convention couvre, par exemple, l'enquête préalable ou les demandes faites par l'autorité judiciaire d'un État à l'autorité compétente d'un autre État afin d'obtenir des preuves à utiliser lors de procédures en justice dans l'État demandeur.

32 Groupe de travail «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 (WP 114), 25 novembre 2005, p. 12, faisant référence à l'avis 5/2004 portant sur les communications de prospection directe non sollicitées selon l'article 13 de la Directive 2002/58/CE (WP 90), du 27 février 2004, point 3.2.

probablement que de nombreuses situations dans lesquelles le consentement est, au mieux, implicite (par exemple parce qu'une personne a été informée de l'existence d'un transfert et ne s'y est pas opposée) ne seront pas admissibles. À l'inverse, la dérogation pourrait s'appliquer dans les cas où l'entité qui effectue le transfert est en contact direct avec la personne concernée, où les informations peuvent aisément être fournies et où un consentement indubitable est obtenu[33].

De plus, en vertu de l'article 2, point h), de la directive 95/46/CE, le consentement doit être libre, spécifique et informé. Selon le groupe de travail «Article 29», la première exigence signifie que l'exercice de toute «pression» risque d'invalider le consentement. Ceci est particulièrement vrai dans le contexte de l'emploi, lorsque la relation de subordination et de dépendance inhérente des salariés remettra normalement en question le recours au consentement[34]. De manière plus générale, le consentement donné par une personne concernée qui n'a pas eu la possibilité d'effectuer un véritable choix ou qui a été mise devant le fait accompli ne peut être considéré comme valable[35].

Il est particulièrement important que les personnes concernées soient dûment informées au préalable de l'éventualité d'un transfert des données en dehors de l'UE, du pays tiers destinataire et des conditions du transfert (finalité, identité et coordonnées du ou des bénéficiaires, etc.). L'information ainsi fournie doit faire apparaître aux personnes concernées le risque spécifique que leurs données sont susceptibles d'être transférées vers un pays tiers où il n'existe pas de protection adéquate[36]. En outre, comme l'a souligné le groupe de travail «Article 29», le retrait du consentement d'une personne concernée, tout en n'ayant pas d'effet rétroactif, doit en principe empêcher tout traitement ultérieur des données à caractère personnel[37]. À la lumière de ces restrictions, le groupe de travail «Article 29» estime qu'il est improbable que le consentement constitue un cadre adéquat à long terme pour les responsables du traitement des données dans des situations de transferts structurels[38].

---

33 Groupe de travail «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), 24 juillet 1998, p. 25.

34 Groupe de travail «Article 29», Avis 8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel (WP 48), 13 septembre 2001, p. 31, 32 et 36. Selon le groupe de travail, le recours au consentement doit être limité aux situations où le salarié est complètement libre de son choix et peut dès lors retirer son consentement sans préjudice. Voir aussi groupe de travail «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» (WP 114), 25 novembre 2005, p. 12-13.

35 Groupe de travail «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 (WP 114), 25 novembre 2005, p. 13. Voir également Avis 6/2002 sur la transmission par les compagnies aériennes d'informations relatives aux passagers et aux membres d'équipage et d'autres données aux États-Unis (WP 66), 24 octobre 2002.

36 Groupe de travail «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), 24 juillet 1998, p. 25.

37 Groupe de travail «Article 29», Avis 15/2011 sur la définition du consentement (WP 187), 13 juillet 2011, p. 10.

38 Groupe de travail «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 (WP 114), 25 novembre 2005, p. 13.

2.4. En résumé: les autres bases possibles pour les transferts de données à caractère personnel

Il ressort de ce qui précède que les entreprises peuvent avoir recours à différents autres outils pour effectuer leurs transferts internationaux de données vers des pays tiers qui ne sont pas considérés comme offrant un niveau de protection adéquat au sens de l'article 25, paragraphe 2, de la directive 95/46/CE. À la suite de l'arrêt Schrems, le groupe de travail «Article 29» a notamment précisé, tout en poursuivant son évaluation et sans préjudice des pouvoirs d'examiner des situations particulières dont sont investis les PDA, que les CCT et les REC peuvent être utilisées pour transférer des données vers les États-Unis[39]. De leur côté, les professionnels du secteur ont réagi à l'arrêt de diverses manières, y compris en fondant leurs transferts de données sur ces autres outils[40].

Deux conditions importantes doivent toutefois être soulignées. Premièrement, il convient de rappeler que, quelle que soit la base juridique spécifique sur laquelle ils se fondent, les transferts vers un pays tiers ne peuvent avoir lieu en toute légalité que si les données ont été tout d'abord collectées, puis traitées par le contrôleur de données établi dans l'UE conformément aux législations nationales applicables transposant la directive 95/46/CE. La directive précise expressément que l'activité de traitement qui précède le transfert, au même titre que le transfert en soi, doit respecter pleinement les règles adoptées par les États membres en vertu des autres dispositions de la directive[41]. Deuxièmement, en l'absence d'une décision de la Commission constatant le caractère adéquat du niveau protection, il incombe aux contrôleurs de veiller à ce que leurs transferts offrent des garanties suffisantes conformément à l'article 26, paragraphe 2, de la directive. Cette évaluation doit être effectuée à la lumière de toutes les circonstances entourant le transfert en question. En particulier, tant les CCT que les REC prévoient que si l'importateur de données a des raisons de croire que la législation applicable dans le pays destinataire peut l'empêcher de remplir ses obligations, il est tenu d'en informer immédiatement l'exportateur des données dans l'UE. Dans une telle situation, il appartient à l'exportateur d'envisager la prise des mesures appropriées pour assurer la protection des données à caractère personnel[42]. Celles-ci peuvent aller des mesures techniques, organisationnelles, liées au modèle d'entreprise ou juridiques[43] à la possibilité de suspendre le transfert de données ou de mettre fin au contrat. Tenant compte de toutes les

---

[39] Voir la déclaration du groupe de travail «Article 29» du 16 octobre 2015 (cf. note de bas de page 8 *supra*).

[40] Plusieurs multinationales ont déclaré fonder leurs transferts de données vers les États-Unis sur les autres outils. Voir par exemple les déclarations de Microsoft (http://blogs.microsoft.com/on-the-issues/2015/10/06/a-message-to-our-customers-about-eu-us-safe-harbor/) ou de Salesforce (http://www.salesforce.com/company/privacy/data-processing-addendum-faq.jsp). D'autres entreprises américaines telles qu'Oracle ont déclaré offrir à leurs clients faisant appel à des services de cloud la possibilité de stocker leurs données en Europe, évitant ainsi qu'elles soient transférées ailleurs: http://www.irishtimes.com/business/technology/oracle-keeps-european-data-within-its-eu-based-data-centres-1.2408505?mode=print&ot=example.AjaxPageLayout.ot

[41] Voir le considérant 60 et l'article 25, paragraphe 1, de la directive 95/46/CE.

[42] Voir par exemple la clause 5 de l'annexe de la décision 2010/87/UE de la Commission et le groupe de travail «Article 29», Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes (WP 154), 24 juin 2008, p. 8.

[43] Voir par exemple les lignes directrices publiées par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA): https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf.

circonstances du transfert, il se peut donc que les exportateurs de données doivent mettre en place des garanties supplémentaires pour compléter celles offertes conformément à la base juridique applicable au transfert de façon à répondre aux exigences de l'article 26, paragraphe 2, de la directive.

Au dernier chef, ce sont les DPA qui doivent évaluer au cas par cas le respect de ces exigences dans le cadre de l'exercice de leurs fonctions de supervision et d'exécution, y compris dans le contexte de l'approbation d'accords contractuels et de REC ou sur la base de plaintes individuelles. Si certains DPA ont exprimé des doutes quant à la possibilité d'utiliser des instruments de transfert tels que des CCT et des REC pour les flux de données transatlantiques[44], le groupe de travail «Article 29» a annoncé, dans la déclaration qu'il a publiée suite à l'arrêt Schrems, qu'il poursuivra son analyse de l'impact de l'arrêt sur d'autres outils de transfert[45], Les pouvoirs des DPA en matière d'examen de cas particuliers et de protection des personnes individuelles n'en sont pas affectés.

3. LES CONSEQUENCES DE L'ARRET SCHREMS SUR LES DECISIONS CONCERNANT LE CARACTERE ADEQUAT DU NIVEAU DE PROTECTION

Dans son arrêt, la Cour de justice ne remet pas en question les pouvoirs conférés à la Commission en vertu de l'article 25, paragraphe 6, de la directive 95/46/CE de constater qu'un pays tiers offre un niveau adéquat de protection, dès lors que les exigences énoncées par la Cour sont respectées. Selon celles-ci, la proposition de règlement général sur la protection des données[46] de 2012 visant à remplacer la directive 95/46/CE clarifie et détaille les conditions dans lesquelles les décisions concernant le caractère adéquat du niveau de protection peuvent être adoptées. Dans l'arrêt Schrems, la Cour a également précisé que

---

[44] Voir par exemple le document de position publié le 26 octobre 2015 par la conférence des autorités allemandes chargées de la protection des données au niveau fédéral et national sur la protection des données: https://www.datenschutz.hessen.de/ft-europa.htm#entry4521. Soulignant que l'arrêt Schrems contient des «exigences substantives strictes» qui doivent être respectées tant par la Commission que par les DPA, le document de position indique que les DPA allemands évalueront la légalité des transferts de données basés sur les autres outils (CCT et REC) et ne délivreront plus de nouvelles autorisations pour l'utilisation de ces outils. Parallèlement, certains DPA allemands ont clairement annoncé que les outils de transfert alternatifs font l'objet d'un examen juridique. Voir par exemple les documents de position publiés par les DPA du Land de Schleswig-Holstein:https://www.datenschutzzentrum.de/artikel/981-ULD-Position-Paper-on-the-Judgment-of-the-Court-of-Justice-of-the-European-Union-of-6-October-2015,— C-36214.html et du Land de Rhénanie-Palatinat: https://www.datenschutz.rlp.de/de/aktuell/2015/images/20151026_Folgerungen_des_LfDI_RLP_zum_EuGH-Urteil_Safe_Harbor.pdf.

[45] Voir la déclaration du groupe de travail «Article 29» du 16 octobre 2015 (cf. note de bas de page 8 *supra*).

[46] Commission européenne, proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données). Voir également Parlement européen, Résolution législative du 12 mars 2014 sur la proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), COM(2012)0011 – C7-0025/2012 – 2012/0011(COD); Conseil, proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données), préparation d'une approche générale, 9565/15. Cette proposition en est au stade final du processus législatif.

lorsque la Commission adopte une décision concernant le caractère adéquat du niveau de protection, celle-ci lie tous les États membres et leurs organes, y compris des DPA, jusqu'au moment où elle est retirée, annulée ou rendue invalide par la Cour de justice qui est seule compétente à cet égard. Les DPA restent compétents pour examiner les demandes, au sens de l'article 28, paragraphe 4, de la directive 95/46/CE, de vérification de la licéité d'un transfert de données au regard des exigences énoncées par la directive (telles qu'elles sont interprétées par la Cour de justice), sans pouvoir faire de constatation définitive. Les États membres doivent de ce fait prévoir la possibilité de porter l'affaire devant un tribunal national qui peut, de son côté, saisir la Cour de justice en introduisant une demande de décision préjudicielle conformément à l'article 267 du traité sur le fonctionnement de l'Union européenne (TFUE).

La Cour de justice a en outre expressément confirmé que le recours d'un pays tiers à un système d'autocertification (comme le prévoient les principes de la sphère de sécurité) n'exclut pas une décision constatant le caractère adéquat du niveau de protection arrêtée en vertu de l'article 25, paragraphe 6, de la directive 95/46/CE tant que des mécanismes effectifs de détection et de contrôle permettent d'identifier et de sanctionner, en pratique, toute violation des règles en matière de protection des données.

La décision sur la sphère de sécurité ne contenant pas suffisamment de constatations à cet égard, la Cour de justice a déclaré la décision invalide. Il est donc clair que les transferts transatlantiques de données ne peuvent plus avoir lieu sur cette base, c'est-à-dire en invoquant exclusivement le respect des principes de la sphère de sécurité relatifs à la protection de la vie privée. Puisque les transferts de données vers un pays tiers qui n'offrent pas un niveau de protection adéquat (ou du moins lorsque ceci n'a pas été établi dans une décision de la Commission arrêtée en vertu de l'article 25, paragraphe 6, de la directive 95/46/CE) sont en principe interdits[47], ils ne seront légaux que si l'exportateur de données peut se fonder sur l'un des autres outils décrits ci-dessus sous le point 2. En l'absence de décision concernant le caractère adéquat du niveau de protection, l'exportateur des données a la responsabilité de veiller, sous le contrôle des DPA, à ce que les conditions requises pour se fonder sur (l'un de) ces outils soient remplies en ce qui concerne le transfert de données en question.

Le champ d'application de l'arrêt se limite à la décision sur la sphère de sécurité de la Commission. Cependant, chacune des autres décisions concernant le caractère adéquat du niveau de protection[48] contient une limitation des pouvoirs des DPA qui est identique à l'article 3 de la décision sur la sphère de sécurité que la Cour de justice a annulée[49]. La Commission tirera les conséquences de l'arrêt en élaborant rapidement une décision, à adopter en suivant la procédure de comité applicable, qui remplacera cette disposition dans toutes les décisions existantes concernant le caractère adéquat du niveau de protection. La Commission s'engagera également dans une évaluation régulière des décisions existantes et futures

[47] Voir le considérant 57 de la directive 95/46/CE.

[48] Actuellement, des décisions concernant le caractère adéquat du niveau de protection ont été adoptées à l'égard des pays suivants: Andorre, Argentine, Canada, Îles Féroé, Guernesey, Île de Man, Israël, Jersey, Nouvelle-Zélande, Suisse et Uruguay. Voir: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

[49] Voir points 99 à 104 de l'arrêt Schrems.

concernant le caractère adéquat du niveau de protection, notamment par l'examen périodique de leur fonctionnement conjointement avec les autorités compétentes du pays tiers en question.

4. CONCLUSION

Comme l'a confirmé le groupe de travail «Article 29», les autres outils autorisant les flux de données peuvent continuer à être utilisés par les entreprises pour les transferts légaux de données vers des pays tiers tels que les États-Unis. Cependant, la Commission estime que l'établissement d'un nouveau cadre solide pour le transfert de données vers les États-Unis demeure une priorité. Un tel cadre est la solution la plus complète pour garantir la continuité effective de la protection des données à caractère personnel des citoyens européens lors de leur transfert vers les États-Unis. Il représente également la meilleure solution pour les échanges transatlantiques, étant donné qu'il constitue un mécanisme de transfert plus simple, moins contraignant et dès lors moins coûteux, en particulier pour les PME.

Dès 2013, la Commission avait entamé des négociations avec le gouvernement américain en vue de l'adoption d'un nouvel accord pour les transferts transatlantiques de données fondé sur ses treize recommandations[50]. De nets progrès ont été faits dans le rapprochement des points de vue respectifs, débouchant par exemple sur un contrôle renforcé et une application plus stricte des principes de la sphère de sécurité relatifs à la protection de la vie privée par, respectivement, le Department of Commerce et la Federal Trade Commission des États-Unis, une plus grande transparence à l'égard des consommateurs en ce qui concerne leurs droits en matière de protection des données, des voies de recours plus simples et moins onéreuses en cas de plaintes et des règles plus claires concernant les futurs transferts par les entreprises adhérant aux principes de la sphère de sécurité vers des entreprises n'y adhérant pas (par exemple à des fins de traitement ou de sous-traitement). La décision relative à la sphère de sécurité ayant été déclarée invalide, la Commission a intensifié ses négociations avec le gouvernement américain afin de garantir le respect des exigences légales formulées par la Cour. La Commission s'est fixé pour objectif de conclure ces décisions dans les trois mois.

Jusqu'à la mise en place du nouveau cadre transatlantique, les entreprises doivent se fonder sur les autres outils de transfert disponibles. Cette option entraîne toutefois des responsabilités pour les exportateurs de données, sous le contrôle des DPA.

Par opposition à une situation dans laquelle la Commission a conclu qu'un pays tiers garantit un niveau adéquat de protection des données sur lequel les exportateurs de données peuvent se fonder à des fins de transferts de données depuis l'UE, il incombe à ceux-ci de vérifier que les données à caractère personnel sont effectivement protégées lors de l'utilisation des autres outils, notamment en prenant des mesures appropriées, le cas échéant.

Les DPA ont un rôle central à jouer sur ce point. En tant que principaux responsables chargés de veiller au respect des droits fondamentaux des personnes concernées, les DPA sont à la

[50] Voir note de bas de page 4.

fois responsables et compétents, en toute indépendance, pour surveiller les transferts de données de l'UE vers les pays tiers. La Commission invite les responsables du traitement des données à coopérer avec les DPA et à les aider ainsi à s'acquitter efficacement de leur mission de surveillance. La Commission continuera de travailler en étroite coopération avec le groupe de travail «Article 29» afin de garantir une application uniforme de la législation de l'UE en matière de protection des données.