« Uncle Sam is watching you »

Jacques, Florian

Published in:
Journal des Tribunaux

Publication date:
2021

Document Version
le PDF de l'éditeur

gime vise à réglementer des activités individuelles, alors que le second concerne des rassemblements. En procédant de la sorte, le Conseil d'État évite par ailleurs la délicate question, pourtant posée par les requérants, de la hiérarchie existant entre, d'une part, la liberté de culte, qui bénéficie d'une valeur constitutionnelle et internationale et, d'autre part, la liberté d'entreprendre qui n'a qu'une valeur législative[50].

24. Nous émettrons cependant quelques réserves sur l'analyse par l'assemblée générale du caractère non urgent de la demande introduite par les requérants. En effet, l'assemblée générale porte une appréciation particulièrement sévère sur la notion d'« inconvénients d'une gravité suffisante pour qu'on ne puisse les laisser se produire en attendant l'issue de la procédure au fond » ainsi que sur le caractère personnel de ces inconvénients. Cette appréciation stricte a pour effet de rendre exagérément difficile, voire quasiment impossible, la démonstration de l'existence de cette condition dans le chef tant d'une personne morale en charge d'un lieu de culte, d'un ministre du culte ou d'un croyant lorsque la dimension collective du culte est menacée. Ces enseignements feront cependant certainement jurisprudence étant donné qu'ils ont été rendus par l'assemblée générale du Conseil d'État et que, paradoxalement, l'analyse de la condition d'urgence par cette dernière n'était pas nécessaire pour conclure au rejet de la requête étant donné qu'aucun moyen n'a été jugé sérieux.

Stéphanie WATTIER
Professeure à la Faculté de droit de l'UNamur
Directrice adjointe du Centre Vulnérabilités et Sociétés
François XAVIER
Assistant et doctorant à la Faculté de droit de l'UNamur
Membre du Centre Vulnérabilités et Sociétés

(50) En droit belge voy. M. VANDERSTRAETEN, « La liberté d'entreprendre dans la jurisprudence de la Cour constitutionnelle et du Conseil d'État », *in* T. LÉONARD (dir.), *Actualités en droit économique : la liberté d'entreprendre ou le retour en force d'un fondamental du droit économique*, Bruxelles, Bruylant, 2015, pp. 7-41. Pour ce qui est de son inscription dans la Charte des droits fondamentaux de l'Union européenne, voy. T. LÉONARD et J. SALTEUR, « Article 16. Liberté d'entreprise », *in* F. PICOD, S. VAN DROOGHENBROECK et C. RIZCALLAH (dir.), *Charte des droits fondamentaux de l'Union européenne : commentaire article par article*, 2e éd., Bruxelles, Bruylant, 2019, pp. 395-415.

Le point sur…

« Uncle Sam is watching you »

Retour sur les enseignements de l'arrêt *Schrems II* de la Cour de justice de l'Union européenne

Introduction

Dans son arrêt rendu le 16 juillet 2020[1], la Cour de justice de l'Union européenne (ci-après, « la Cour ») a, pour la seconde fois en 5 ans, invalidé le mécanisme sur lequel reposait les transferts de données à caractère personnel entre l'Union européenne (UE) et les organisations auto-certifiées établies aux États-Unis[2]. Après avoir apporté des éclaircissements sur le champ d'application matériel du RGPD[2bis], la décision commentée ci-après se prononce sur la validité de deux mécanismes de transferts de données à caractère personnel vers des pays tiers à l'UE(ci-après, « pays tiers ») au sens du RGPD[3]. Ces instruments sont respectivement la décision de la Commission européenne 2016/1250[4], dite décision « privacy shield » et la décision de la Commission européenne 2010/87 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers[5] (ci-après la décision « CPT »)[6].

Cet arrêt fait suite à un renvoi préjudiciel de la *High Court* d'Irlande. À l'origine de cet arrêt, Max Schrems, militant pour la protection des données introduit une plainte auprès de l'autorité irlandaise compétente pour la protection des données, visant à interdire les transferts de données à caractère personnel de *Facebook Irland* à *Facebook Inc*. établie aux États-Unis. À la suite des révélations de l'affaire *Snowden*, M. Schrems considérait que le droit et la pratique des États-Unis ne protégeaient pas suffisamment les données traitées aux États-Unis contre les programmes de surveillance des autorités publiques. Sur la base des conclusions provisoires de son enquête, l'autorité irlandaise décida de saisir la *High Court*. Les résultats de cette enquête étaient de nature à remettre en question la validité de la décision *privacy shield* ainsi que des clauses contractuelles adoptées par la Commission sur lesquelles reposaient en partie les transferts de données effectués par *Facebook*.

Dans le contexte de l'affaire présentée à la Cour, étaient notamment visés l'article 702 du *Foreign Intelligence Surveillance Act* (ou FISA) ainsi que l'*Executive Order* 12333 (ou E.O. 12333). En pratique, ces normes servaient de fondement à la mise en place de programmes de surveillance susceptibles de porter atteinte aux droits fondamentaux des citoyens de l'UE garantis par le RGPD et la Charte des droits fondamen-

(1) C.J., gr. ch., 16 juillet 2020, arrêt *Facebook Ireland et Schrems*, aff. C-311/18, EU:C:2020:559.
(2) Dans un arrêt de 2015, la Cour avait déjà invalidé la décision 2000/520/CE. Voy. C.J., gr. ch., 6 octobre 2015, arrêt *Schrems*, C-362/14, EU:C:2015:650.
(2*bis*) À ce sujet, la Cour précise que le RGPD, s'applique à un transfert de données à caractère personnel effectué à des fins commerciales par un opérateur économique établi dans un État membre vers un autre opérateur économique établi dans un pays tiers, même si, au cours ou à la suite de ce transfert, ces données sont susceptibles d'être traitées à des fins de sécurité publique, de défense et de sûreté de l'État par les autorités du pays tiers concerné. Voy. C.J., gr. ch., arrêt *Facebook Ireland et Schrems*, précité, points 86 et 89.
(3) Règlement (EU) 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, *J.O.* L 119 du 4 mai 2016. Ci-après « RGPD ».
(4) Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, *J.O.* L 207 du 1er août 2016. Ci-après la « décision *privacy shield* ».
(5) Décision 2010/87/CE 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.* L 39 du 12 février 2010. Ci-après « décision CPT ».
(6) Sur les notions de responsable du traitement et de sous-traitant, voy. les définitions inscrites aux articles 4, 7), et 4, 8), du RGPD. Voy. également les lignes directrices de l'European Data Protection Board (ci-après « EDPB ») y relatives : European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*, 2 septembre 2020.

taux de l'UE (ci-après « la Charte »)[6bis]. Ces textes habilitaient donc les autorités et les agences de renseignement américaines, telles que la NSA, à procéder à la collecte et à l'analyse d'une quantité vertigineuse de données à caractère personnel des citoyens de l'UE[7].

Dans la présente contribution, nous rappelons tout d'abord, brièvement, les règles applicables aux transferts de données vers un pays tiers. Nous analysons ensuite le raisonnement de la Cour ayant amené à l'invalidation de la décision *privacy shield*. Nous verrons également la position adoptée au sujet de l'utilisation de clauses contractuelles types. Enfin, en guise de conclusion, nous aborderons les conséquences de cette décision pour les acteurs désireux de procéder au transfert de données vers les États-Unis, et plus largement vers un pays tiers.

1 Principes applicables aux transferts de données vers des pays tiers

Lorsqu'une entreprise ou une autorité publique[8] située sur le territoire de l'UE décide de transférer des données à caractère personnel à un responsable du traitement ou à un sous-traitant situé sur le territoire d'un pays tiers, celle-ci sera tenue de respecter les dispositions du chapitre V du RGPD. Dans les lignes qui suivent nous emploierons respectivement les termes « exportateur de données » et « importateur de données » pour désigner l'acteur établi sur le territoire de l'UE et l'acteur établi dans un pays tiers. À la lecture du chapitre V du règlement, trois hypothèses dans lesquelles des données à caractère personnel peuvent être transférées à partir de l'UE doivent être distinguées[9].

Tout d'abord, le transfert peut reposer sur une décision d'adéquation par laquelle la Commission européenne décide, après examen, qu'un pays tiers, ou un secteur particulier au sein d'un État, assure un niveau de protection adéquat aux données à caractère personnel[10]. Aucune formalité additionnelle n'est alors requise. En l'absence de décision d'adéquation, le transfert peut être effectué moyennant des garanties appropriées[11]. À ce titre, divers instruments tels que les clauses types de protection des données adoptées par la Commission[12] ou les règles d'entreprise contraignantes peuvent être utilisés sans que le transfert ne doive être autorisé par une autorité de contrôle[13]. La dernière hypothèse concerne, quant à elle, la possibilité de transférer des données dans un pays tiers lorsqu'il n'existe pas de décision d'adéquation et en l'absence de garanties appropriés au sens de l'article 46[14]. Nous détaillons ci-après la manière dont ces deux premières hypothèses ont été analysées par la Cour.

2 L'invalidation de la décision *privacy shield*

Conformément à la jurisprudence de la Cour, le « niveau de protection adéquat », devant être accordé aux données transférées sur la base d'une décision d'adéquation, ne doit pas être identique à celui garanti par le droit de l'UE mais « substantiellement équivalent »[15]. Néanmoins, la décision *privacy shield* permettait d'écarter les principes de protection des données qu'elle contenait notamment pour des motifs liés à la sécurité nationale et au respect de la législation américaine[16]. Ce faisant, elle rendait possible les ingérences dans les droits fondamentaux des personnes dont les données faisaient l'objet d'un transfert aux États-Unis en permettant aux autorités publiques d'accéder et d'utiliser lesdites données dans le cadre de programmes de surveillance. Selon la Commission, ces ingérences étaient limitées au strict nécessaire pour l'accomplissement de l'objectif poursuivi et une protection juridictionnelle effective contre ces ingérences était assurée[16bis].

Dès lors, le droit et les pratiques des États-Unis devaient être examinés, au regard de l'article 52, § 1er, de la Charte[17] afin de vérifier si la décision *privacy shield* permettait effectivement d'assurer, aux données transférées, un niveau de protection substantiellement équivalent à celui garanti par le RGPD lu à la lumière de la Charte. En d'autres termes, le fait que les autorités d'un État tiers accèdent à des données à caractère personnel n'est pas automatiquement une violation des droits fondamentaux, mais, encore faut-il que cette mesure puisse être considérée comme, proportionnées, nécessaires et répondant effectivement à des objectifs d'intérêt général. L'analyse de la Cour met en lumière les conditions auxquelles doivent répondre d'éventuelles ingérences d'un état tiers dans les droits fondamentaux des personnes dont les données ont été transférées. Tout d'abord, ces ingérences doivent être prévues par la loi. Ensuite, afin de répondre à l'exigence de proportionnalité, la loi doit (i) prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et (ii) imposer des exigences minimales afin d'assurer que la personne concernée dispose de garanties pour protéger ses données contre les d'abus. La loi doit également garantir que l'ingérence soit limitée au strict nécessaire. Enfin, il est requis que la personne dispose de droits effectifs et opposables[18] [19].

Au regard de ces exigences, les programmes de surveillance américains étaient cependant loin de « passer le test ». L'article 702 du FISA ne fait ressortir ni l'existence de limitations à l'habilitation qu'il comporte pour la mise en œuvre de programmes de surveillance, ni l'existence de garanties dans le chef de citoyens non-américains. Quant à l'EO.12333, il n'encadre pas de manière suffisamment claire et précise la collecte de données « en vrac » qu'il permet. En ce sens, ces normes ne répondaient pas aux exigences attachées au principe de proportionnalité consacré en droit de l'UE. De telles mesures de surveillance ne

(6bis) Étaient en particulier concernés les articles 7, 8 et 47 de la Charte.
(7) En pratique, l'article 702 du FISA permettait notamment la mise en place des programmes de surveillance PRISM et UPSTREAM. Le premier, permettait à la NSA de requérir, de la part des fournisseurs de services internet, l'ensemble des communications de certaines personnes. Le second permettait aux autorités d'accéder aux infrastructures matérielles de l'Internet (telles que les câbles ou les commutateurs) afin d'y collecter des données. l'E.O.12333 permettait, quant à lui, à la NSA d'accéder aux câbles sous-marins de l'Internet pour y procéder à une collecte « en vrac » de données à caractère personnel.
(8) En l'absence de décision d'adéquation, l'European Data protection Board, recommande aux autorités publiques de recourir aux instruments prévus aux articles 46, § 2, a), et 46, § 3, b), du RGPD. Toutefois, les autorités publiques restent libres de recourir à d'autres mécanismes de l'article 46. Voy. *Guidelines 2/2020 articles 46 (2) (a) and 46 (3) (b) Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies*, 15 décembre 2020, p. 5.
(9) Pour une analyse approfondie de ces différents mécanismes, voy. notamment. C. DE TERWANGNE et C. GAYREL *in* C. DE TERWANGNE et K. ROSIER (dir.), *Le Règlement général sur la protection des données (RGPD/GPDR). Analyse approfondie*, coll. du CRIDS, Bruxelles, Larcier, 2018, pp. 285-335.
(10) Article 45 du RGPD. À l'heure de la rédaction de ces quelques lignes, la Commission européenne a reconnu que 12 pays, parmi lesquels la Japon et l'Argentine offraient un niveau de protection adéquat. La liste de ces pays est tenue à jour sur le site internet de la Commission.
(11) Article 46 du RGPD.
(12) En ce qui concerne spécifiquement les clauses types de protection des données adoptées par la Commission, deux décisions sont à mentionner. La première, la décision CPT, a trait, aux transferts de données entre un responsable du traitement établi au sein de l'EEE et un sous-traitant établi dans un pays tiers. La seconde, concerne le transfert de données entre un responsable du traitement établi au sein de l'EEE et un autre responsable du traitement établi dans un pays tiers. Voy. 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, *J.O.* L 181 du 4 juillet 2001. Ci-après la « décision 2001/497 ». À la suite d'une modification de 2004, la décision 2001/497 contient deux ensembles de clauses différents.
(13) Voy. l'article 46, § 2, du RGPD pour une énumération de ces différents instruments.
(14) Sur ce sujet voy. european Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, 25 mai 2018.
(15) C.J., gr. ch., arrêt *Schrems*, précité, point 73.
(16) C.J., gr. ch., arrêt *Facebook Ireland et Schrems*, précité, point 164.
(16bis) Considérant 140 de la décision *privacy shield*.
(17) À ce sujet, voy. notamment. M. TZANOU, « *Schrems I* and *Schrems II* : Assessing the Case for the Extraterritoriality of EU Fundamental Rights », 2020. Disponible sur https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3710539.
(18) C.J., gr. ch., arrêt *Facebook Ireland et Schrems*, précité, points 174-177.
(19) De manière générale, l'EDPB considère qu'une mesure de surveillance d'un pays tiers, constituant une ingérence dans les droit fondamentaux garantis aux articles 7 et 8 de la Charte, doit répondre à 4 garanties essentielles : (i) le traitement de données constituant l'ingérence doit être prévu par des règles claires et accessibles, (ii) la proportionnalité et la nécessité au regard de l'objectif légitime poursuivi doivent être démontrées, (iii) un mécanisme de supervision indépendant doit exister et (iv) le droit à un recours effectif doit être assuré. Voy. European Data Protection Board, *Recommendations 02/2020 on the European Essential Guarantees for surveillance measures*, 10 novembre 2020.

pouvaient donc être considérées comme limitées au strict nécessaire[20].

En ce qui concerne l'existence d'un contrôle juridictionnel effectif, il est rappelé que l'impossibilité d'exercer un recours afin d'obtenir l'accès, la suppression ou la rectification de données à caractère personnel doit être considéré comme ne respectant pas les exigences de l'article 47 de la Charte. En pratique, les normes américaines ne conféraient pas de droits pouvant être invoqués à l'encontre des autorités publiques devant les cours et tribunaux. Afin de remédier à ce manquement, la décision *privacy shield* permettait de saisir un médiateur. Deux motifs empêchaient cependant l'assimilation de ce mécanisme au droit de faire entendre sa cause devant un tribunal indépendant et impartial. Tout d'abord, l'indépendance du médiateur vis-à-vis du pouvoir exécutif ne pouvait être suffisamment assurée. Ensuite, la décision *privacy shield* ne démontrait aucunement que ce médiateur était doté du pouvoir d'adopter des mesures contraignantes à l'encontre des autorités publiques.

3 *Quid* des transferts de données effectués sur la base de clauses contractuelles types ?

Les clauses contractuelles adoptées par la Commission, à l'instar de celles annexées à la décision CPT, constituent un autre mécanisme de transfert de données. Cependant, ces clauses ont vocation à être employées pour le transfert de données vers une multitude de pays tiers sans que la Commission n'ait préalablement examiné la législation de ces États. En l'absence de décision d'adéquation, l'exportateur de données sera tenu de prévoir des garanties appropriées pour assurer un niveau de protection substantiellement équivalent[21] [22].

À cela s'ajoute le fait que ces clauses sont de nature contractuelle. Aussi, les autorités publiques d'un pays tiers ne sont pas liées par le contenu de ces clauses. Partant de ce constat, et en fonction du droit et des pratiques applicables dans un pays tiers, deux situations peuvent être distinguées. Soit une protection effective peut être assurée et le transfert peut se faire sur la base desdites clauses. Soit la législation applicable permet des ingérences disproportionnées dans les droits des personnes concernées et un transfert sur la base de ces seules clauses ne pourra effectivement assurer la protection des données transférées[23]. Dans ce second cas, la Cour n'exclut pas totalement la possibilité de procéder au transfert de données vers ce pays tiers. Cependant, l'exportateur de données devra adopter des mesures additionnelles. Dans ce contexte, l'arrêt insiste sur la responsabilité de l'exportateur de données de vérifier, au cas par cas, si le droit du pays tiers permet d'assurer un niveau de protection approprié[24] aux données transférées sur la base de clauses contractuelles types complétées, si nécessaire, par des garanties supplémentaires[25]. Suite à la décision de la Cour, l'EDPB a fourni, une liste non exhaustive de mesures techniques, organisationnelles et contractuelles susceptibles d'être implémentées à cet effet[26]. Lorsque ces garanties supplémentaires ne peuvent assurer un niveau de protection adéquat — en ce compris contre l'accès aux données par les autorités publiques — il sera requis de suspendre ou de mettre fin au transfert des données. À défaut, cette mission reviendra aux autorités de contrôle[27].

Au sujet de ces dernières, il est rappelé que la Charte et le RGPD leur confient la mission de contrôler le respect des règles du droit de l'UE applicables en matière de protection des données. À ce titre, elles disposent de la compétence de vérifier si un transfert de données réalisé au départ de leur territoire respecte les exigences du RGPD. Le législateur européen les a dotées d'importants pouvoirs d'enquête en vue de traiter les réclamations introduites par une personne concernée. À l'issue d'une enquête, et lorsque l'autorité constate qu'un niveau adéquat de protection ne peut être assuré, elle doit réagir en vue de remédier rapidement à cette insuffisance[28]. Faisant siennes les conclusions de l'avocat général, la Cour en conclut qu'en l'absence de décision d'adéquation, l'autorité de contrôle est en principe tenue de suspendre ou d'interdire un transfert de données lorsque, compte tenu de l'ensemble des circonstances, les garanties inscrites dans les clauses types ne peuvent être respectées et que le niveau de protection requis au titre du droit de l'UE ne peut être assuré par d'autre moyens[29].

Pour autant, le caractère contractuel de ces clauses n'est pas, à lui seul, de nature à remettre en cause la validité de la décision CPT. En effet, ces clauses imposent aux parties de procéder, conjointement, à l'évaluation de la législation du pays tiers. Sur cette base, l'exportateur doit garantir que le transfert et le traitement des données sera effectué dans le respect du RGPD. En outre, il doit être informé par l'importateur si cette obligation ne peut plus être remplie notamment en raison d'une modification de la législation du pays tiers. En tel cas, l'exportateur dispose de la faculté de suspendre le transfert et/ou de résilier le contrat. La Cour précise toutefois que la suspension ou la résiliation doivent être considérées comme obligatoires. À défaut, l'exportateur des données agirait en violation de son obligation contractuelle visant à assurer la réalisation du traitement dans le respect du RGPD. Enfin, dans l'hypothèse où l'exportateur de données déciderait de maintenir le transfert, il devra informer l'autorité de contrôle compétente, laquelle pourra procéder à des vérifications auprès de l'importateur des données[30] et, au besoin, suspendre ou l'interdire le transfert. Sur la base de ces éléments la Cour en conclut à la présence de mécanismes effectifs dans la décision CPT, et partant à sa validité[31].

Conclusion

À titre de conclusion il est ici permis de formuler plusieurs observations et d'adopter une vision nuancée de cet arrêt. Des éléments constructifs peuvent être mis en évidence mais cette décision est également source d'incertitudes et crée certaines craintes. En ce qui concerne les éléments constructifs, l'arrêt de la Cour doit bien évidemment être salué en ce qu'il vise à protéger, notamment, les citoyens de l'UE à l'égard des mesures de surveillance des États-Unis[32] et rappelle l'importance des droits fondamentaux. Par cet arrêt, la Cour ouvre la voie à la suspension ou à l'interdiction des transferts de données vers les États-Unis. Sur le plan de la supervision, l'arrêt de la Cour semble adresser, aux autorités de contrôle, un appel à l'application plus stricte du RGPD. Lorsqu'un transfert de données ne peut assurer un niveau de protection substantiellement équivalent, la suspension ou l'interdic-

(20) C.J., gr. ch., arrêt *Facebook Ireland et Schrems*, précité, points 179-185.
(21) *Ibidem*, précité, point 96.
(22) Un niveau de protection substantiellement équivalent doit en effet être garanti indépendamment de la disposition du chapitre V du RGPD sur laquelle repose le transfert. Tel que souligné par la Cour, ce chapitre vise à assurer la continuité du niveau élevé de protection des données inscrit dans le RGPD. Voy. C.J., gr. ch., arrêt *Facebook Ireland et Schrems*, précité, points 92 et 93. La Cour semble consacrer la position de l'EDPB selon laquelle les dispositions de l'article 49 ne peuvent être interprétées comme autorisant la violation d'un droit fondamental lors d'un transfert à destination d'un pays tiers. European Data Protection Board, *Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679*, *op. cit.*, p. 3.
(23) Voy. C.J., gr. ch., arrêt *Facebook Ireland et Schrems*, précité, points 125-126.
(24) Les termes « niveau de protection approprié » doivent s'entendre comme des synonymes des termes « niveau de protection substantiellement équivalent ».
(25) *Ibidem*, points 131 et 134.
(26) European data protection board, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 10 novembre 2020. Voy. en particulier les différents scénarios mentionnés dans la seconde annexe de ce document, à savoir les pages 21 à 38.
(27) C.J., gr. ch., arrêt *Facebook Ireland et Schrems*, précité, point 135.
(28) *Ibidem*, points 107, 109 et 110.
(29) *Ibidem*, précité, points 113 et 121.
(30) Conformément au second paragraphe de la clause n° 8 de la décision CPT, l'autorité de contrôle de l'état de l'exportateur de données peut effectuer des vérifications chez l'importateur des données.
(31) C.J., gr. ch., arrêt *Facebook Ireland et Schrems*, précité, points 138-148. Bien que l'examen de la Cour concerne uniquement la décision CPT, ces enseignements nous semblent également transposables aux clauses contractuelles annexées à la décision 2001/497. Cette analyse repose sur une lecture combinée des clauses 5, a), 5, b), et 5, c), du premier ensemble de clauses annexé à la décision 2001/497 et des clauses II, c), II, h), II, e), et VI, b), ii), du second ensemble de clauses annexé à cette décision.
(32) Cet arrêt ne met cependant pas un coup d'arrêt définitif aux possibilités dont disposent les autorités américaines d'accéder aux données de citoyens de l'UE. À ce titre l'on songera notamment au *Cloud Act* qui permet aux autorités de solliciter des entreprises américaines l'accès à des données à caractère personnel de citoyens de l'UE. Sur le sujet voy. A. Cassart, « Premières réflexions sur le *Cloud Act* : contexte, mécanismes et articulations avec le RGPD », *R.D.T.I.*, 2018/4, pp. 41-53.

tion du transfert n'apparaissent pas comme une faculté mais bel et bien comme une obligation.

Sur le plan des incertitudes, il doit être constaté que cet arrêt crée une insécurité juridique certaine dans le chef des entreprises désireuses de transférer des données à caractère personnel vers les États-Unis. En invalidant, selon nous à juste titre, la décision *privacy shield*, la Cour prive *de facto* les entreprises installées au sein de l'UE d'un mécanisme de transfert de données vers ce territoire. Par ailleurs, bien que la validité de la décision CPT soit maintenue, les possibilités de transférer des données sur la base de clauses contractuelles s'en retrouvent sérieusement affaiblies. À la lecture de cet arrêt, il ressort clairement qu'aux yeux de la Cour, le droit et la pratique des États-Unis, en raison des programmes de surveillance qu'ils permettent, ne sont pas de nature à assurer un niveau de protection des droits fondamentaux substantiellement équivalent à celui requis en droit de l'UE. Or, en l'absence de décision d'adéquation, et notamment lorsqu'un transfert de données se fonde sur l'utilisation de clauses contractuelles, un même niveau de protection devrait être assuré. Aussi, l'exportateur de données devrait partir du constat, qu'en l'état, un transfert de donnée sur la seule base de ces clauses ne peut se faire[33]. Les transferts ne sont, certes, pas interdits en toutes hypothèses mais l'exportateur de données devra, le cas échéant en concertation avec l'importateur des données, mettre en place des mesures contractuelles, techniques et/ou organisationnelles additionnelles. Comme le souligne l'EDPB, en fonction des caractéristiques du traitement et des besoins de l'importateur de données, de telles mesures ne pourront toujours être mises en place[34].

En ce qui concerne plus largement les transferts de données vers des pays tiers, cet arrêt rappelle qu'en l'absence de décision d'adéquation, c'est avant tout à l'exportateur de données qu'il revient d'évaluer, préalablement au transfert, le droit et la pratique de l'État tiers. À cet effet, il sera notamment tenu de vérifier dans quelle mesure la législation permettant aux autorités publiques d'accéder à des données à caractère personnel permet d'assurer aux données transférées un niveau de protection substantiellement équivalent à celui garanti en droit de l'UE. Bien que cette obligation nous paraisse conforme au principe d'*accountability*[35], certains observateurs y voient une potentielle charge financière importante notamment pour les PME européennes[36]. De manière additionnelle, en soulignant que les clauses contractuelles types, ne lient pas les autorités publiques d'un État tiers, la Cour remet *de facto* en question la possibilité d'effectuer un transfert de données sur la seule base d'autres instruments contractuels tels que les règles d'entreprise contraignantes[37].

Enfin, sur le plan des craintes, dans son arrêt, la Cour rappelle le caractère liant des décisions d'adéquation vis-à-vis des autorités de contrôle. Celles-ci paraissent dépourvues de marge de manœuvre lorsqu'elles sont confrontées à un transfert de données fondé sur une décision d'adéquation. La remise en cause de l'appréciation de la Commission semble, à la lecture de la jurisprudence de la Cour, nécessiter un important investissement des personnes concernées afin de porter l'affaire devant la Cour de justice[38]. Aussi, on peut s'interroger sur l'absence de mécanisme d'exception lorsqu'on sait que la Commission avait, déjà en 2018, été invitée par le Parlement européen à suspendre les transferts de données vers les États-Unis[39]. Dernièrement, suite à cet arrêt, certains observateurs craignent que les transferts de données reposent de plus en plus souvent sur l'article 49 du RGPD et que ce mécanisme, en principe dérogatoire, devienne la règle[40].

Florian JACQUES
Assistant à la Faculté de droit de l'UNamur et chercheur au Nadi/Crids

(33) À ce propos, il est intéressant de mentionner que la Cour a récemment décidé que des mesures de surveillance, instaurées par le droit du Royaume-Uni, excédaient les limites du strict nécessaire et ne pouvaient être considérées comme étant justifiées, dans une société démocratique. À défaut d'adoption d'une décision d'adéquation, le Royaume-Uni sera considéré comme un pays tiers, au sens du RGPD, à partir du 1er juillet 2021. Voy. C.J., gr. ch., arrêt *Privacy International*, 6 octobre 2020, aff. C-623/17, EU:C:2020:790, point 81.
(34) European data protection board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, *op. cit.*, pp. 26-27. L'EDPB y mentionne, notamment, l'hypothèse dans laquelle les données doivent être accessibles « en clair » dans le pays tiers.
(35) Article 5, § 2, du RGPD. Selon ce principe, le respect des règles et principes en matière de protection des données incombe au responsable de traitement en tant que personne prenant l'initiative de réaliser un traitement de données. À ce titre, il doit être en mesure de démontrer le respect de ces règles et principes.
(36) A. Chander, « Is Data Localization a Solution for *Schrems II* ? Is Data Localization a Solution for *Schrems II* ? Anupam », 2020, p. 4. disponible sur https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3662626.
(37) En ce sens, European data protection board, *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*, *op. cit.*, pp. 17-18.
(38) C.J., gr. ch., arrêt *Facebook Ireland et Schrems*, précité, points 118-120.
(39) L. Drechsler, « What is Equivalent ? A Probe into GDPR Adequacy based on EU Fundamental Rights », 2019, p. 1. Disponible sur https://papers.ssrn.com/sol3/papers.cfm ?abstract_id=3549252.
(40) S. Fantin, « *Schrems 2*, Privacy Shield and Transatlantic Data Flows. Part Two : The impact of *Schrems 2*, a list of homework (comment) », 23 juillet 2020. Disponible sur https://www.law.kuleuven.be/citip/blog/schrems-2-privacy-shield-and-transatlantic-data-flows-part-two/.