Arrêt Schrems III : l'impossible transfert des données vers les États tiers ?

Ludovic Pailler

Mots-clés : Règlement général sur la protection des données - Transfert des données vers État tiers - Principe général - Décision d'adéquation (invalidation) - Clauses types de protection des données (validation) - Dérogations particulières

Solution : Dans son arrêt *Schrems III*, la Cour de justice invalide la décision d'adéquation qui permettait le transfert des données vers les États-Unis. Les garanties substantielles et procédurales des programmes de surveillance américain ne permettent pas d'assurer aux personnes concernées un niveau de protection de leurs données substantiellement équivalent à celui fourni par le droit de l'Union. Si la décision relative aux clauses types de protection des données n'est pas invalidée, elle ne peut fonder le transfert sans que le responsable de traitement ou son sous-traitant n'adopte des mesures complémentaires de protection. En l'état des choses, la Cour de justice ne laisse ouvert que le recours aux dérogations particulières de l'article 49 du règlement général sur la protection des données pour justifier un transfert vers les États-Unis.

Impact : La Cour de justice remet au premier plan le principe d'interdiction du transfert des données lequel ne doit pas compromettre le niveau élevé de protection des données assuré par le droit de l'Union. En l'absence de nouvelle décision d'adéquation, subordonnée à la levée des obstacles mis en lumière, les contraintes pesant sur les responsables de traitement ou leur sous-traitant paraissent excessives, à tout le moins particulièrement difficiles voire impossibles à satisfaire. Ne reste que les dérogations particulières mais elles ne peuvent justifier des transferts massifs, continus et systématique. L'arrêt sonne-t-il le glas des transfert de données ?

Arrêt Schrems III : l'impossible transfert des données vers les États tiers ?

Ludovic Pailler
Agrégé des facultés de droit
Professeur de droit privé et sciences criminelles
Centre de rechercher sur le droit international privé (EDIEC EA 4185)

Une pierre de plus. L'arrêt *Schrems III* (CJUE, gde ch., 16 juill. 2020, C-311/18) était doublement attendu. Par son enjeu d'abord, le transfert massif de données du territoire de l'Union vers les États-Unis et la mise en cause d'un GAFAM, Facebook. Par sa solution ensuite, qui ne surprend guère dès lors que le transfert de données est le moyen de compromission de la protection des données le plus prégnant.

L'arrêt commenté constitue tout au plus un nouveau rebondissement au sein d'un bloc de jurisprudence fourni d'arrêts de grande chambre qui donnent une vigueur toute particulière aux droits fondamentaux garantis par les articles 7 (respect de la vie privée et familiale) et 8 (protection des données à caractère personnel) de la Charte (CJUE, Gde ch., 30 mai 2006, C-317/04 et C-318/04, Parlement c. Conseil ; CJUE, Gde ch., 8 avril 2014, C-293/12 et C-594/12, Digital Rights Ireland ; CJUE, Gde ch., 6 oct. 2015, C-362/14, Schrems I ; CJUE, Gde ch., 21 déc. 2016, C-203/15 et C-698/15, Tele2 Sverige ; CJUE, Gde ch., 26 juillet 2017, avis 1/15 ; CJUE, Gde ch., 2 oct. 2018, C-207/16, Ministerio fiscal ; CJUE, Gde ch., 6 oct. 2020, C-511/18, C-512/18 et C-520/18, La Quadrature du Net e.a. ; CJUE, Gde ch., 6 oct. 2020, C-623/17, Privacy International). La Cour de justice martèle une fois encore que les pratiques des grands acteurs du numérique ne doivent pas prendre le pas sur le droit, et plus particulièrement sur la protection des données assurée par le droit de l'Union. Elle entend maintenir cette garantie pour les données au départ de l'Union européenne.

Pour en revenir au cas d'espèce, il constitue le second acte européen de la bataille menée par M. Schrems contre les transferts massifs de données vers les États-Unis (l'arrêt *Schrems II*

portait plus particulièrement sur la notion de consommateur au sens du règlement n°1215/2012 et sur la mise en œuvre d'un recours collectif, CJUE, 25 janv. 2018, C-498/16).

Acte I. Le célèbre militant de la protection des données, M. Schrems, a saisi l'autorité de contrôle irlandaise, le *Data Protection Commissioner*, afin qu'elle interdise à la société Facebook Ireland de transférer ses données à caractère personnel vers les États-Unis. Sa plainte fut rejetée considérant que, par une décision 2000/520 (Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique**)**, la Commission avait constaté que les États-Unis assuraient un niveau de protection adéquat. Il saisit la High Court d'un recours contre le rejet de sa plainte, laquelle soumit une question préjudicielle à la Cour de justice. Cette dernière aboutit à l'invalidation de la décision « sphère de sécurité » (CJUE, Schrems I, *préc*.). Le rejet de la plainte de M. Schrems fut en conséquence annulé. Mais le transfert des données ne prit pas fin. L'arrêt *Schrems I*ne fit que déplacer le problème.

Acte II. Dans sa plainte reformulée, M. Schrems demandait l'interdiction ou la suspension du transfert de données vers les États-Unis désormais fondé par Facebook sur les clauses types de protection des données adoptées par la Commission (décision de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil ; décision d'exécution (UE) 2016/2297 de la Commission du 16 décembre 2016 modifiant les décisions 2001/497/CE et 2010/87/UE relatives aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers et vers des sous-traitants établis dans ces pays, en vertu de la directive 95/46/CE du Parlement européen et du Conseil, « décision CPT », ci-après). La raison en était que les données transférées pouvaient être mises à disposition des autorités américaines à des fins de surveillance. L'autorité de contrôle irlandaise saisit en conséquence la *High Court* afin qu'elle interroge la Cour de justice sur la validité de la décision CPT.

La haute juridiction irlandaise relève, dans sa décision, un ensemble de moyens relatifs aux activités de renseignement américaines et à la protection juridictionnelle des personnes concernées qui ne sont pas citoyennes américaines, lesquels sont propres à mettre en cause l'existence, aux États-Unis, d'un niveau de protection substantiellement équivalent à celui assuré par le droit de l'Union. En conséquence, ses questions préjudicielles portent sur la validité de la décision CPT dans la mesure où celles-ci ne lient pas les autorités publiques étrangères.

Pour échapper aux critiques, Facebook Ireland s'est prévalu du constat d'adéquation du niveau de protection fourni par le droit des États-Unis dans la décision « Bouclier de protection » (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 ; « décision BDP », ci-après) venu combler le vide laissé après l'arrêt *Schrems I*. En conséquence, la prise en considération de la décision BDP dans l'appréciation du caractère suffisant des garanties du transfert des données ainsi que sa validité même sont interrogées.

Applicabilité matérielle et temporelle. Les questions d'applicabilité matérielle et temporelle du règlement général sur la protection des données (« RGPD », ci-après) n'appellent pas de plus amples commentaires. Ainsi celle relative à l'applicabilité du RGPD à un transfert de données vers un opérateur économique établi hors de l'Union lorsque, au cours ou à la suite de ce transfert, ces données peuvent être traitées par les autorités étrangères à des fins de sécurité publique, de défense ou de sûreté reçoit une réponse rapide. Cette dernière circonstance n'exclut pas le traitement en cause du champ d'application du RGPD dès lors que « l'opération

consistant à faire transférer des données à caractère personnel depuis un État membre vers un pays tiers constitue, en tant que telle, un traitement de données à caractère personnel […] effectué sur le territoire d'un État membre, traitement auquel ce règlement s'applique » (pt.84). Ensuite, posées à l'aune de la directive 95/46 qui était alors applicable, les questions sont traitées en application des dispositions du RGPD dès lorsqu'il constituera le fondement de la décision qui reste à adopter par l'autorité de contrôle irlandaise (pts.77 à 79). Si la continuité entre la directive et le RGPD sur la question du transfert des données rend cette solution acceptable, il demeure que la Cour procède à une application rétroactive du RGPD (v., sur ce point, N. MARTIAL-BRAZ, « Nouvelle donne en matière de transfert de données personnelles hors Union européenne », *JCP G* 2020, 1116).

Pour le reste et ***in globo***, la Cour de justice est interrogée sur les possibilités pour une autorité de contrôle d'interdire ou de suspendre un transfert de données vers un État soupçonné de ne pas assurer un niveau de protection des données substantiellement équivalent, et plus particulièrement sur la validité des décisions de la Commission qui le permettent.

La Cour y répond par une décision dont la densité, accrue par certaines redondances, est à la hauteur des enjeux prégnants pour les droits humains sans l'être pour l'économie des entreprises concernées, et plus particulièrement, pour les entreprises européennes dépendantes de services subordonnés au transfert de données.

Principe général en matière de transfert des données. Non sans lien avec une lecture stricte induite par l'interdiction de principe des transferts de données (art.44 RGPD), l'arrêt commenté resserre considérablement les possibilités théoriques de réaliser un transfert de données vers les États-Unis, et plus largement vers les États tiers, au point d'en interroger la possibilité même. Pour ce faire, la Cour met l'accent sur le « principe général applicable aux transferts » (art.44 RGPD) : la « continuité du niveau élevé de [la] protection » (pt.93) assuré par le règlement lu à la lumière des droits fondamentaux (pt.101). Dans l'État tiers, la personne concernée doit ainsi bénéficier « d'un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union » (CJUE, Gde ch. Schrems I, préc., pts.73 et 74 ; comp., sur l'exigence d'« un niveau de protection essentiellement équivalent à celui qui est garanti dans l'Union » pour les transferts fondés sur une décision d'adéquation, cons.104 RGPD). La Cour de justice étend cette exigence aux transferts fondés sur des clauses types de protection des données (pt.96). Elle vaut également pour l'ensemble des garanties appropriées de l'article 46 RGPD et devrait seulement être exclue pour les dérogations particulières envisagées par l'article 49 RGPD (voir *infra*).

Ce principe général traduit d'autant mieux l'« importance constitutionnelle du standard européen de protection des données » (B. BERTRAND et J SIRINELLI, « Schrems II : on prend les mêmes et on recommence », *Dalloz IP/IT* 2020, p.640). Sa réaffirmation dans l'arrêt commenté, au regard de la protection assurée par les droits étrangers et de sa mise en œuvre dans l'arrêt commenté, traduit une défiance certaine à l'égard des transferts de données qu'elle déstabilise une fois de plus (C. CASTETS-RENARD, « *Schrems II* et invalidation du *Privacy Shield*, un goût de « déjà vu »… », *D*. 2020, p.2432). Les conséquences prévisibles sont lourdes pour les grands importateurs de données pour lesquels l'Union est un marché précieux comme pour les entreprises d'une moindre échelle qui s'appuient, comme l'État français lui-même, sur les services offerts par des opérateurs dont la capacité et la performance de traitement reposent, en partie, sur le transfert des données. Aussi la question se pose-t-elle, à la suite de l'arrêt commenté, de la possibilité même de transférer des données vers un État tiers.

À la lecture de l'arrêt commenté, la réponse paraît essentiellement négative s'agissant des États-Unis, et pourrait plus largement valoir pour de nombreux États tiers. En effet, la Cour épuise quasiment les fondements juridiques possibles lorsqu'elle invalide la décision d'adéquation (I), caractérise l'insuffisance des garanties appropriées (II) et renvoie aux dérogations pour des situations particulières (III).

I. L'absence d'adéquation

Mise en cause de la décision « Bouclier de protection ». La question de la validité de la décision d'adéquation n'était qu'incidente, dès lors que le litige au principal portait sur la validité des clauses contractuelles types qui, à la suite de la décision d'invalidation de la première décision d'adéquation dite « Sphère de sécurité » (CJUE, Gde ch., Schrems I, *préc.*), fondaient le transfert. Toutefois, l'adoption entretemps de la décision « Bouclier de protection » imposait son examen eu égard aux arguments soulevés par M. Schrems et aux constatations de la juridiction de renvoi qui mettaient « en substance, en cause le constat de la Commission » (pt.160). En effet, à compter de son entrée en application cette décision a fondé le transfert de données sans qu'il soit nécessaire pour le responsable de traitement ou le sous-traitant de prévoir des garanties appropriées (art.46.1 RGPD).

Cependant, la Cour donne à la validité de la décision BDP la place de vedette américaine pour mieux justifier l'extension de sa saisine. Après avoir validé la décision CPT, elle répond à la question de savoir si l'autorité de contrôle est liée par la décision d'adéquation dès lors que les clauses contractuelles types peuvent ne pas suffire à garantir la continuité de la protection fournie par le droit de l'Union. En effet, la décision d'adéquation « est obligatoire dans tous ses éléments » (art.288, al.4, TFUE). Plus particulièrement, elle contraint l'autorité de contrôle à tenir pour substantiellement équivalent le niveau de protection assuré par l'État tiers (CJUE, Gde ch., Schrems I, *préc.*, pt.52). En revanche, elle ne contraint pas les personnes concernées. Elles peuvent saisir l'autorité de contrôle du niveau de protection existant dans un État tiers, laquelle pourra demander à une juridiction nationale qu'elle interroge la Cour de justice sur la validité de la décision d'adéquation (CJUE, Gde ch., Schrems I, *préc.*,pt.53 ; pour une transposition consécutive, art.39 de la loi « Informatique et Libertés »).

Motifs de l'invalidation. L'essentiel tient à l'examen de la conformité de la décision « Bouclier de protection » avec le RGPD, lu à la lumière de la Charte. Le point d'achoppement demeure (CJUE, Gde ch., Schrems I, *préc.*, pt.86) la primauté générale et sans limitation des exigences relatives à la sécurité nationale, à l'intérêt public et au respect de la législation sur les « Principes du cadre « Bouclier de protection des données [Union européenne]-États-Unis ». Restait à évaluer si les ingérences ainsi permises, notamment à des fins de surveillance, s'accompagnaient de limites et garanties substantiellement équivalentes à celles requises par le droit de l'Union, en d'autres termes si elles équivalent substantiellement aux exigences européennes de protection des libertés et droits fondamentaux de la personne. À cet égard, le considérant 140 de la décision BDP indique que ces restrictions « seront limitées à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il existe une protection juridictionnelle effective ».

L'adéquation est passée au crible d'un double tandem de critères d'analyse. L'un déduit de l'article 45.2.A RGPD, l'autre tiré de la charte.

Après avoir constaté l'existence incontestable d'une ingérence, la Cour rappelle, au titre de l'article 52.1 de la charte, les conditions de sa justification. Notamment, « la réglementation en cause doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales [et] en particulier indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prises » (pt.176). Et, de façon cinglante, sans pour autant identifier d'atteinte au contenu essentiel du droit fondamental au respect de la vie privée (comp., CJUE, Gde ch., Schrems I, pt.94), elle établit qu'aucun des deux textes de droit américain au fondement des programmes de surveillance n'y satisfait. L'article 702 du *Foreign Intelligence Surveillance Act* « ne fait ressortir d'aucune manière l'existence de limitations à l'habilitation », (pt.180) quand l'*Enforcement Order* 1233 ne confère aucun droit opposable aux autorités américaines (pt.182). Leur combinaison avec la directive stratégique présidentielle n°28, contraignante pour

les services de renseignement, ne modifie pas la conclusion. En effet, celle-ci « ne confère pas aux personnes concernées des droits opposables » (pt.181). Au contraire, elle organise une « collecte « en vrac » » (pt.183) sans en encadrer « de manière suffisamment claire et précise la portée » (pt.183).

Au défaut de protection adéquate au plan substantiel s'ajoute une défaillance au plan procédural. La Cour rappelle opportunément l'inhérence du contrôle juridictionnel à l'existence d'un État de droit et son importance aigue dans le contexte d'un transfert de donnés vers un pays tiers dans la mesure où la protection fournie par les autorités administratives et judiciaires d'un État membre peuvent n'être pas pleinement effectives. Dans sa décision BPD, la Commission constatait l'absence de toute voie de recours, ce que souligne la Cour en l'absence de droits opposables conférées aux personnes concernées par l'article 702 FISA et l'*Enforcement Order* 12333. Mais l'accord « Bouclier de protection » avait vocation à compenser ce défaut par la création d'un mécanisme de médiation dont la Commission faisait dument état (comp., sur l'absence rédhibitoire de constatations relatives aux voies de recours ouvertes, CJUE, Gde ch., Schrems I, *préc.*, pts.97 et 98). Toutefois, la Cour met en cause l'indépendance fonctionnelle de ce médiateur à l'égard du secrétaire d'État qui le nomme, à qui il rend compte, et qui fait partie du département d'État ainsi que son caractère juridictionnel même puisque rien n'indique qu'il puisse prendre des décisions contraignantes à l'égard des services de renseignement américains. Dès lors, le « contenu essentiel du droit fondamental à une protection juridictionnelle effective » est méconnu (pts.187 et 197 de l'arrêt commenté).

De ce double constat, la Cour déduit logiquement que l'entière décision BDP est invalide.

Portée de l'invalidation. À la lecture de l'arrêt, et quoi que les termes en soient un peu moins sévères que ceux de l'arrêt *Schrems I*, la décision d'invalidité était inévitable tant les manquements étaient manifestes. Sans doute la décision BDP était-elle le fruit d'une négociation précipitée. S'agissant des mesures de surveillance, elle ne répondait d'ailleurs pas aux craintes exprimées par le groupe de l'article 29 dans son avis sur cette décision (Opinion 01/2016 on the EU - U.S. Privacy Shield draft adequacy decision, spéc. p.33 et s.) qui ne se sont pas éteintes après son adoption (v., notamment, Report from the Commission to the European Parliament and the Council on the third annual review of the functioning of the EU-U.S. Privacy Shield, COM(2019) 495 final, 23 octobre 2019 ; EU-U.S. Privacy Shield – Third Annual Joint Review, Comité européen de la protection des données, 12 novembre 2019). Elles ont encore justifiées - par un effet boule de neige - que le Préposé fédéral à la protection des données et à la transparence estime que le bouclier de protection des données Suisses-États-Unis n'offre pas un niveau de protection des données adéquat (Prise de position sur la transmission de données personnelles vers les États-Unis et d'autres États n'offrant pas un niveau adéquat de protection des données au sens de l'art6, al.1 LPD). L'invalidation et ses motifs interrogent non seulement la possibilité d'un nouvel accord avec les États-Unis, dont les négociations auraient débutés (« U.S., European Commission begin discussions enhanced privacy shield framework : statement », Reuters, 10 août 2020) ou d'un accord post-*Brexit* avec le Royaume-Uni mais encore la validité des autres décisions d'adéquation adoptées (Andorre, Argentine, Canada, Îles Féroé, Guernesey, Israël, Île de Man, Japon, Jersey, Nouvelle-Zélande, Suisse et Uruguay).

Désormais, les législations des États-tiers relatives aux activités de renseignement, et plus largement relatives à leur accès aux données transférées, sont identifiées comme le principal obstacle à la caractérisation d'un niveau de protection substantiellement équivalent (Recommandations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, Comité européen de protection des données, 10 nov. 2020, pt.36 ; et le document dédié, Recommandations 02/2020 on the European Essential Guarantees for surveillance measures, Comité européen de protection des données, 10 nov. 2020, spéc. pt.8). La Cour de justice dans l'arrêt commenté (pts.175 à 177 et 187 à

189), et plus encore dans les arrêts relatifs à l'accès par les autorités publiques et à la conservation des données traitées par les services de communication en ligne, exige un niveau élevé de protection des droits substantiels et procéduraux des personnes concernées. Les derniers arrêts en date (CJUE, Gde ch., Quadrature du net, *préc.* ; CJUE, Gde ch., Privacy International, *préc.*) ont décliné le niveau de protection requis par les articles 7 et 8 de la charte en fonction de l'objectif poursuivi dès lors que « la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus […] doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité » (CJUE, Gde ch., Quadrature du net, *préc.*, pt.131). Elle a ainsi admis que la sécurité nationale puisse « justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier » les objectifs de lutte contre la criminalité en général (CJUE, Gde ch., Quadrature du net, *préc.*, pt.136 ; CJUE, Gde ch., Privacy International, *préc.*, pt.75). La législation applicable n'en doit pas moins prévoir de façon claire, précise et accessible les conditions matérielles et procédurales de l'accès des autorités publiques aux données. Les ingérences doivent ainsi être strictement nécessaires et proportionnées au regard de l'objectif poursuivi. Leur contrôle doit être réalisé par un organe indépendant, comme un juge ou une autorité administrative, dont les décisions sont contraignantes et des voies de recours doivent être ouvertes aux personnes concernées. Dans leur mise en œuvre, les exigences tirées du droit de l'Union, synthétisées par le Comité européen de la protection des données (Recommandations 02/2020, *préc.*), apparaissent plus strictes que celles tirées de la Convention européenne des droits de l'Homme, notamment par l'absence de marge d'appréciation laissée aux États (v., en dernier lieu, Cour EDH, 13 sept. 2018, n^{os}58170/13, 62322/14 et 24960/15, Big Brother Watch e.a. c. Royaume-Uni, spéc.§307 et 308) et font douter de l'intérêt pour un État tiers d'être partie à la Convention 108 modernisée qui envisage spécifiquement l'activité de traitement à des fins de sécurité nationale et de défense (art.11 de la Convention 108 modernisée pour la protection des personnes égard du traitement automatisé de données à caractère personnel). Alors que la législation des États membres, notamment justifiée par la nécessité de débusquer les acteurs du terrorisme, peine à se conformer au niveau de protection requis par la jurisprudence de la Cour de justice, il est d'autant plus douteux qu'un État tiers puisse y satisfaire et bénéficier ou continuer à bénéficier d'une décision d'adéquation (sur ce dernier point, Th. CHRISTAKIS, « « Schrems III » ? Firts Thoughts on the EDPB post-Schrems II Recommandations on International Data Transfers (Part 1), 13 nov. 2020, *European Law Blog*; comp. sur les potentialités d'une decision d'adéquation partielle, C. CASTETS-RENARD, *loc. cit.*). Il est encore plus improbable que les État tiers souhaitant garantir à leurs opérateurs économiques un accès facilité au marché européen des données en paient le prix par un affaiblissement de leur législation sécuritaire. Aussi ces opérateurs devraient-ils, à défaut de décision d'adéquation, prévoir des garanties appropriées ?

II. L'absence de garantie appropriées

Mise en œuvre du principe général. Au cas d'espèce et au moment de la saisine de l'autorité de contrôle irlandaise, le transfert de données se fondait sur des clauses contractuelles types de protection des données issues de la décision CPT modifiée à la suite de l'arrêt *Schrems I*. En effet, l'article 46.1 RGPD (ancien art.26.4 de la directive 95/46) permet un transfert de données vers un pays tiers lorsque le responsable du traitement ou le sous-traitant « a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voie de recours effective ». Saisie de l'interprétation de ce texte par la juridiction de renvoi, la Cour de justice a précisé que l'évaluation d'un niveau de protection substantiellement équivalent suppose de « prendre en considération tant les stipulations contractuelles convenues entre le responsable du traitement ou son sous-traitant établis dans l'Union et le destinataire du

transfert établi dans le pays tiers concerné que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données à caractère personnel transférées, les éléments pertinents du système juridique de celui-ci » (pt.104 de l'arrêt commenté). Malgré la référence aux seules stipulations contractuelles et parce qu'il s'agit d'interpréter l'article 46.1 RGPD, la solution vaut pour l'ensemble des garanties appropriées listées par l'article 46.2 RGPD.

Pouvoirs de l'autorité de contrôle. La première décision CPT, depuis modifiée sur ce point, restreignait le pouvoir des autorités de contrôle de suspendre ou d'interdire le transfert à certaines hypothèses exceptionnelles (cons.11 et art.4 de la décision 2010/87). Aussi la juridiction de renvoi interrogeait la Cour de justice sur la portée des pouvoirs d'interdiction et de suspension d'un transfert conféré par l'article 58.2, f et j, RGPD. En réponse, la Cour de justice souligne l'« importance particulière » de la mission de ces autorités dans le contexte d'un transfert eu égard aux difficultés auxquelles sont exposées les personnes concernées dans l'exercice de leurs droits (pt.108 de l'arrêt commenté), leur devoir de traiter les réclamations qui lui sont soumises et les pouvoirs dont elles disposent à cette fin. Elle les élargit d'ailleurs (v., sur ce point, B. BERTRAND et J. SIRINELLI, *loc. cit.*) par une obligation pour l'autorité de contrôle de suspendre ou d'interdire le transfert « lorsqu'elle considère, à la lumière de l'ensemble des circonstances propres à ce transfert, que les clauses types de protection des données ne sont pas ou ne peuvent pas être respectées dans ce pays tiers et que la protection des données transférées requise par le droit de l'Union ne peut pas être assurée par d'autres moyens » (pt.113 de l'arrêt commenté). Elle ajoute encore que la Commission, dans l'exercice de son pouvoir d'exécution, ne peut restreindre les compétences des autorités de contrôle.

Pour autant, il demeure que la décision d'exécution adoptée sur le fondement de l'article 46.2.c est contraignante pour les autorités de contrôle (art.288, al.4, TFUE). C'est dire qu'elles ne peuvent d'elles-mêmes suspendre ou interdire un transfert au motif que les clauses contractuelles types adoptées par une décision de la Commission ne seraient pas valides. La Cour le confirme en n'abordant la suspension ou l'interdiction du transfert que lorsque « les clauses types de protection des données ne sont pas ou ne peuvent pas être respectées dans ce pays tiers » (pt.113 de l'arrêt commenté). En présence d'une décision adoptant des clauses contractuelles types de protection des données, l'autorité de contrôle qui considère devoir suspendre ou interdire le transfert a alors deux possibilités, qui ne s'excluent pas l'une l'autre. Soit la discontinuité trouve sa cause dans les clauses contractuelles types qui lient l'autorité de contrôle. Elle devra alors saisir son juge de la décision les approuvant pour qu'il l'examine et interroge, le cas échéant, la Cour de justice sur leur validité. Soit la discontinuité du niveau de protection des données a une source étrangère aux clauses contractuelles types. L'autorité pourra adopter sa décision sauf à être liée par une décision d'adéquation dont le juge national qui en est saisi, s'il partage les vues de l'autorité, interrogera la Cour de justice sur la validité de la décision (v. *supra* et pts. 116 et s. de l'arrêt commenté). Chacune de ces voies a été pavée par l'arrêt commenté.

Les contraintes pesant sur l'autorité de contrôle et les moyens les questionner devraient être les mêmes lorsque la Commission adopte des dispositions relatives aux règles contraignantes d'entreprise (art. 47.3 RGPD), lorsqu'elle approuve par une décision des clauses type de protection des données adoptées par une autorité de contrôle (art. 46.2.d) ou lorsqu'elle rend d'application générale un code de conduite (art. 40.9 et 46.2.e RGPD).

Validité de la décision CPT. Pour mettre en cause la validité de la décision CPT au regard des article 7, 8 et 47 de la charte alors que son article 1er affirme satisfaire aux exigences de l'article 46.1 RGPD, la *High Court* en souligne l'angle mort (B. BERTRAND et J. SIRINELLI, *loc. cit.*) : les clauses contractuelles types ne lient pas les autorités des États tiers, ce qui met en doute leur aptitude à garantir un niveau adéquat de protection des données. La Cour de justice, qui se prononce pour la première fois sur la validité d'une telle décision, commence par distinguer la décision d'approbation de clauses contractuelles types d'une décision

d'adéquation. Cette dernière requiert de la Commission, le constat d'un niveau adéquat de protection des données par un État tiers quand les clauses contractuelles types « s'appliquent de manière uniforme dans tous les pays tiers et, dès lors, indépendamment du niveau de protection garanti dans chacun d'entre eux » (pt.133 de l'arrêt commenté). Ainsi ne peuvent-elles être appréciées qu'*in abstracto* (C. CASTETS-RENARD, *loc. cit.*). En outre, par leur nature contractuelle, elles peuvent n'être pas suffisantes pour garantir à elles seules la continuité de la protection des données (cf. *infra*). La Cour en déduit que l'absence de caractère contraignant à l'égard des autorités des États tiers « ne saurait affecter la validité de [la] décision [CPT] » (pt.136 de l'arrêt commenté).

Dès lors la validité de la décision dépend uniquement de l'effectivité des mécanismes de garantie de la continuité de la protection des données dans le champ contractuel. En somme, il s'agit de s'assurer que le responsable du traitement ou son sous-traitant est informé des règles applicables à la protection des données dans l'État tiers de façon actualisée et qu'il dispose, en conséquence, de la faculté de poursuivre ou de mettre un terme au traitement. Deux mécanismes méritent à ce titre d'être relevés. Tout d'abord, des clause 4, sous a et b, et 5 sous a et b, la Cour déduit une obligation pour le responsable du traitement ou son sous-traitant ainsi que pour le destinataire de vérifier, au préalable, que le droit de l'État tiers de destination des données permet au destinataire de se conformer aux clauses contractuelles types. Ensuite, le responsable du traitement doit être informé par le destinataire de toute modification négative du droit applicable aux données dans l'État tiers, et en notifier l'autorité de contrôle lorsqu'il décide de poursuivre ou de lever la suspension du transfert (clause 4.g, 5.b, et 8.2). L'autorité de contrôle, qui n'est pas empêchée de suspendre ou d'interdire un transfert de données, est ainsi mise en mesure de l'exercer plus facilement. La Cour conclut à la validité de la décision CPT dès lors qu'elle comporte des mécanismes effectifs qui permettent la suspension ou l'interdiction du transfert lorsque les clauses contractuelles types ne sont pas ou ne peuvent pas être respectées par le destinataire, ce qui vise l'hypothèse d'un accès des autorités publiques aux données transférées dans des conditions qui ne sont pas substantiellement équivalentes à celle du droit de l'Union.

Responsabilisation du responsable de traitement ou de son sous-traitant. La lettre de l'article 46 RGPD laissait entendre que le transfert pouvait être pleinement justifié par les garanties appropriées qu'il vise. Les faits de l'espèce et le caractère générique des clauses contractuelles types démontrent qu'une telle interprétation ne pouvait être retenue sans méconnaître le principe général de l'article 44 RGPD. Aussi, la Cour admet-elle que les clauses contractuelles types peuvent nécessiter d'être complétées. Plus particulièrement, elle affirme que l'article 46.2.c RGPD « repose sur la responsabilisation du responsable de traitement ou de son sous-traitant établis dans l'Union » (pt.134 de l'arrêt commenté), en écho au principe de responsabilité (art.5.2 et 24 RGPD) auquel se réfère le principe général de l'article 44 RGPD. Elle en déduit, à partir du considérant 109 RGPD, qu'il leur revient de « prendre des mesures supplémentaires suffisantes pour garantir [la continuité de la protection des données de la personne concernée] » (pt.135 de l'arrêt commenté). La décision CPT ne peut constituer un écran de protection du responsable de traitement ou de son sous-traitant. La charge d'assurer l'existence d'un niveau de protection substantiellement équivalent est transférée au responsable du traitement et à son sous-traitant comme contrepartie du risque qu'ils prennent de transférer des données vers un État dont la Commission n'a pas constaté qu'il garantit un niveau adéquat de protection des données. C'est encore le prix de l'atteinte portée par le transfert des données à la protection des droits fondamentaux des personnes concernées.

Cette responsabilisation vaut-elle plus largement pour l'ensemble des garanties appropriées visées par l'article 46 RGPD ? La question se pose moins pour les clauses contractuelles types adoptées par une autorité de contrôle (art.46.2.d) auquel se réfère le considérant 109, que pour les règles d'entreprises contraignantes pour lesquels le considérant 110 n'évoque aucune

garantie supplémentaire. À considérer que la charge de la protection des données revient à celui qui prend le risque du transfert et à défaut pour ces garanties de lier les autorités des États tiers (à l'exception des garanties appropriées pour les transfert de données entre autorités publiques, art. 46.2.a et 46.3.b), la réponse est positive (dans le même sens, mais sans justification, Recommendations 1/2020, *préc*.).

Mais l'adoption de « mesures supplémentaires suffisantes » n'est pas systématique. Elle ne s'impose qu'à défaut pour les garanties appropriées de l'article 46.2 RGPD choisies par le responsable de traitement ou son sous-traitant d'assurer la continuité de la protection des données lors d'un transfert vers un État tiers donné. Toujours est-il que l'adoption ou l'absence de ces mesures devra être documentée (art.5.2 et 24.1 RGPD), avec l'aide du destinataire, en considération des lois et pratiques qui ont cours dans l'État tiers de destination et des particularités du transfert envisagé (Recommendations 1/2020, *préc.*, pt.30).

Reste à déterminer ce que recouvrent les termes « mesures supplémentaires suffisantes », que ni le RGPD ni la Cour de justice ne définissent. L'emploi de diverses expressions par la Cour n'est pas pour faciliter les choses (« garanties supplémentaires » au pt. 134 ; « mesures supplémentaires suffisantes » au pt.135 et « mécanismes effectifs » au pt.137). Quant au considérant 109 RGPD évoque uniquement des « engagement contractuels qui viendraient compléter les clauses types de protection ». De nouvelles stipulations contractuelles ne seraient-elles pas vaines à défaut de pouvoir lier les autorités des États tiers ? Sans doute est-ce la raison pour laquelle le Comité européen de la protection des données envisage également l'adoption de mesures organisationnelles et techniques, appelées à être combinées (Recommendations 01/2020, *préc*., pt.47). Toutefois, il ajoute que seules les mesures techniques peuvent « empêcher ou rendre ineffectif l'accès aux données personnelles par les autorités publiques dans des État tiers » (*ibid.*, pt.48). Et il recommande le recours au cryptage des données lorsqu'il s'agit uniquement de les stocker, leur pseudonymisation ou le fractionnement du traitement (*ibid.*, Annex 2, pts.72 et s.) lorsqu'elles doivent être traitées dans un État tiers. Il s'agit dans chaque cas, non pas d'empêcher l'accès aux données par les autorités publiques d'État tiers, mais de le rendre inutile en les privant du moyen d'identifier les personnes concernées, ce qui n'est pas un absolu, compte tenu de la ré-identification permise par l'agrégation des données.

À défaut pour le responsable de traitement de garantir un niveau de protection des données substantiellement équivalent à celui fourni par le droit de l'Union, au moyen de mesures supplémentaires le cas échéant, le transfert des données vers un État tiers fondé sur l'article 46 RGPD devra être suspendu ou interdit par l'autorité de contrôle compétente. Et la Cour de justice d'ajouter, que si cette dernière estime « que les transferts de données vers un pays tiers doivent, d'une manière générale, être interdits », il lui appartient de mettre en œuvre le mécanisme de cohérence de l'article 64.2 RGPD. Est ainsi confiée au Comité européen de la protection des données la charge de garantir la continuité du niveau de protection européen des données lors de transfert de données en dehors de l'Union européenne. En l'absence de décision d'adéquation, il peut rendre un avis défavorable à tout flux de données vers un État tiers donné et contraindre une autorité de contrôle récalcitrante à se conformer à sa décision (art.65.1.c RGPD).

Avenir des garanties appropriées. D'ores et déjà, ces solutions ne peuvent, de façon certaine, permettre de maintenir les flux transatlantiques de données en l'absence de décision d'adéquation, pas plus que l'adoption de nouvelles clauses contractuelles types, même si elles tirent les conséquences de l'arrêt commenté (v., le projet d'Annexe au projet de décision d'exécution sur les clauses contractuelles types pour le transfert de données vers un État tiers, Ares(2020)6654686), . Deux obstacles concrets persisteront, d'une inégale importance.

Le premier tient au coût de mise en œuvre d'un transfert fondé sur des garanties appropriées. Il ne suffit plus de recourir à l'un des outils listés par l'article 46.2 RGPD. Le niveau de protection des données existant dans l'État de destination devra nécessairement être documenté, pour

justifier s'il est substantiellement équivalent à celui existant dans le droit de l'Union. L'intérêt du destinataire des données à coopérer permettra-t-il de réunir facilement les nombreux éléments sur lesquels doit se baser l'appréciation du responsable de traitement ou de son sous-traitant (pt.104 de l'arrêt commenté) ? Cette potentielle facilité d'accès au droit étranger n'allège que partiellement la charge du responsable du traitement ou de son sous-traitant qui devra encore et *a minima* comparer le droit étranger avec les garanties offertes par le RGPD lues à la lumière de la charte et actualiser les données y relatives. Par ailleurs, en cas d'insuffisance du niveau de protection des données assuré dans le pays de destination, le responsable de traitement ou son sous-traitant devront adopter des mesures supplémentaires. Si des grandes entreprises comme *Facebook* ont certainement les moyens de développer des algorithmes de cryptage ou de pseudonymisation, les petites et moyennes entreprises, qu'elles soient expéditeurs ou destinataires pourraient rencontrer là une importante limite au transfert. Il y encore un risque qu'une entreprise ne s'expose, notamment, à des mesures de rétorsion économique de la part de l'État tiers à l'égard duquel elle constaterait un défaut de protection des données substantiellement équivalent à celui garanti par le droit de l'Union.

La somme des obstacles est étourdissante. L'étau dans lequel est pris le responsable du traitement ou son sous-traitant pourrait être inextricable. Toutefois, l'importance économique de l'accès aux données traitées sur le territoire de l'Union est tel que le marché devrait s'adapter. Les destinataires de données pourraient rapidement relocaliser leur activité (comp., sur l'absence d'interdiction faite aux sociétés américaines d'opérer des traitements sur le territoire de l'Union, CE, ord., 13 oct. 2020, Association Le Conseil national du logiciel libre e.a., n°444937, cons.18) ou bien proposer des solutions clés en main aux responsables de traitement ou à leur sous-traitant établis dans l'Union, dont la compatibilité avec le RGPD comme avec le droit des États tiers concernés ne manquera pas d'interroger. Mais il semble bien que les obligations juridiques contradictoires, émanant de l'Union et des États-Unis, soient difficiles à concilier en l'état. Ainsi le chiffrement des données de santé traitées par la Plateforme des données de santé dont la sous-traitance a été confiée à Microsoft a-t-il été jugé insuffisant par le Conseil d'État au regard des injonctions qui peuvent émaner des autorités américaines (CE, ord., 13 oct. 2020, *préc*.).

Par où se profile le second obstacle qui apparaît plus insurmontable et s'incarne dans le Comité européen de protection des données. Cela tient moins à l'avis qu'il peut donner sur le transfert de données vers un pays tiers identifié, qui suppose encore qu'il soit saisi par une autorité de contrôle qu'aux recommandations qu'il a publié à la suite de l'arrêt commenté. Les deux recommandations (Recommendations 01/2020, *préc*. ; Recommendations 02/2020) suivent strictement la ligne fixée par la Cour de justice pour évaluer le niveau de protection dans un État tiers. Là où la Commission, dans son rôle politique, acceptait des compromis pour permettre la circulation des données, le Comité européen de la protection des données paraît inflexible. À la lumière des « garanties européennes essentielles en matière de mesures de surveillance » (Recommendations 02/2020,*préc.*), bien peu d'États tiers devraient pouvoir bénéficier d'un avis favorable. L'arrêt commenté met ainsi en lumière un potentiel conflit entre le Comité sur la protection des données et la Commission, entre une autorité soucieuse avant tout de la protection des données et un organe politique. La Commission pourrait-elle briser un avis négatif du Comité par une décision d'adéquation ? Juridiquement oui, mais politiquement, ce serait prendre un risque d'être désavoué, une fois de plus, par la Cour de justice.

Il semble que Facebook ait d'ores et déjà renoncé à justifier ses transfert de données par le recours à des garanties appropriées pour se fonder sur les très subsidiaires dérogations pour des situations particulières (v. sur ce point, les échanges entre M. Schrems et Facebook *in* « Is the DPC actually stopping Facebook's EU-US data transfers?!..maybe half-way! », Noyb.eu, 9 sept. 2020). Mais le peuvent-elles ?

III. Le renvoi aux dérogations pour des situations particulières

Absence de vide juridique. À la crainte que l'invalidation de la décision d'adéquation ne rende strictement impossible tout transfert de données, la Cour de justice oppose les dérogations particulières de l'article 49 dont le paragraphe premier précise qu'il s'applique en l'absence de décision d'adéquation et de garanties appropriées. La réponse lapidaire appelle immédiatement deux remarques. Tout d'abord, sous la rigueur de sa réponse, la Cour de justice envoie un message clair. En l'état des choses, le maintien temporaire de la décision BDP dans l'attente d'une nouvelle décision n'est pas acceptable. Les atteintes sont telles qu'elles requièrent de profonds changements du droit américain ou la concession de garanties bien supérieures. Ensuite, la Cour enfonce le clou s'agissant des garanties appropriées qu'elle ne mentionne pas au titre des voies subsidiaires pour un transfert des données vers les États-Unis. Les mesures de surveillance existantes rendent illusoires les garanties supplémentaires, même techniques, qui pourraient être mises en œuvre (v., dans le même sens, CE, ord., 13 oct. 2020, *préc.*, cons.11). Quoi qu'il en soit, le recours à l'article 49 présente un intérêt évident pour le responsable de traitement ou pour son sous-traitant. Il n'a pas à documenter, ni même à vérifier, l'existence d'un niveau substantiellement équivalent de protection des données dans l'État tiers de destination.

Exception au principe général de l'article 44 RGPD. En effet, comme son intitulé et le caractère très subsidiaire du fondement qu'il offre au transfert des données l'indiquent, les dérogations de l'article 49 font exception au principe général selon lequel un transfert de donnés vers un pays tiers ne peut avoir lieu si ce dernier ne garantit pas, de façon générale, un niveau substantiellement équivalent de protection. S'agissant d'une exception au principe qui régit l'exception au principe d'interdiction du transfert des données, elle devrait être interprétée restrictivement. S'agissant de la matière civile et commerciale, sont pertinentes les dérogations fondées sur le consentement explicite de la personne concernée, sur la nécessité du traitement pour l'exécution du contrat ainsi que sur la nécessité du traitement pour la constatation, l'exercice ou la défense des droits en justice (art.49.1, a,b, c et e RGPD). *Facebook* justifierait désormais (« Is the DPC… », *loc. cit.*) le maintien du transfert de données vers les États-Unis au motif qu'il est « nécessaire à l'exécution du contrat entre la personne concernée et le responsable de traitement » (art.49.1.b).

Mais un transfert massif, continu et systématique de données peut-il être justifié par un tel fondement sans priver d'effet utile le principe général (art.44 RGPD) et ses traductions que sont la décision d'adéquation et l'exigence de garanties appropriées ? La réponse ne peut qu'être négative sauf à rendre illusoire la protection des données vigoureusement défendue par la Cour de justice et à faire de ces exceptions le principe. Qui plus est, les dérogations particulières n'écartent aucun des dangers soulignés pour la protection des données à caractère personnel. Le législateur, en conscience, réserve ces fondements à un transfert « occasionnel et nécessaire dans le cadre de l'exécution d'un contrat ou d'une action en justice » (cons.111 RGPD ; comp., sur l'exigence d'un transfert non répétitif qui ne touche qu'un nombre limité de personnes lorsqu'il est nécessaire aux des intérêts légitimes impérieux poursuivis par le responsable de traitement, art.49.1, al.2, RGPD) pour lesquels les risques généraux pèsent moins lourdement. Le Comité européen sur la protection des données en fait la même lecture (Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement (UE) 2016/679, 25 mai 2018, spéc. p.5).

En outre, rien n'exclut que le responsable de traitement ou son sous-traitant soit contraint de fournir des garanties supplémentaires au cas particulier. En effet, s'il est dérogé à l'exigence d'un niveau de protection substantiellement équivalent, l'article 44 dispose en revanche que « toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis ».

Acte III. La pièce mise en scène par M. Schrems n'en est pas à son dernier acte. L'arrêt commenté a mis juridiquement un terme au transfert massif de données mais, concrètement, il n'en a pas fermé les vannes. Les enjeux économiques et politiques sont trop prégnants. Un troisième acte est à venir qui pourrait porter, à court terme, sur l'interprétation de l'article 49 RGPD, à moyen terme, sur la contestation d'un avis du Comité européen de la protection des données sur le transfert des données vers un État tiers et à long terme, sur la validité d'une troisième décision d'adéquation.

Dans l'attente, l'insécurité juridique domine quant à la possibilité de garantir un niveau élevé de protection des droits et libertés fondamentaux lors d'un transfert de données vers un État tiers. Elle ne manquera pas d'avoir des « conséquences contentieuses en cascade » (B. BERTRAND et J. SIRINELLI, *loc. cit.*). La charge des autorités de contrôle pourrait singulièrement s'accroître, d'autant plus qu'elles affirment progressivement leur rôle face aux GAFAM (v., sur les récentes sanctions contre *Amazon* et *Google*, délib. de la formation restreinte n° SAN-2020-012 du 7 déc. 2020 concernant les sociétés GOOGLE LLC et GOOGLE IRELAND LIMITED et délib. de la formation restreinte n°SAN-2020-013 du 7 déc. 2020 concernant la société AMAZON EUROPE CORE), tout comme la saisine des juridictions pénales (sur la répression du transfert illicite, art. 226-22-1 du Code pénal) et civiles (par ex., sur le fondement de l'action de groupe de l'art.37, al.2, de la loi « informatique et libertés »). Ces complications convaincront-elles les acteurs concernés et les pouvoirs publics de re-localiser sur le territoire de l'Union les traitements concernés ?