

**DROITS INTELLECTUELS, DROIT ET TECHNOLOGIE / INTELLECTUELE EIGENDOM, RECHT EN
TECHNOLOGIE**

Transfert de données à caractère personnel de l'Europe vers un pays tiers: état des lieux à la suite de la décision « Schrems 2 »

Ophélie SNOY¹

Introduction	582
1. Obligation de respecter le Chapitre V du RGPD afin de procéder à un transfert licite de données à caractère personnel de l'EEE vers un pays tiers ou à une organisation internationale (art. 44 et s.)	584
1.1. Définitions (large) de « transfert » par l'Autorité de contrôle du UK (ICO) et de « pays tiers » par le Comité	584
1.2. Obligation du responsable du traitement ou du sous-traitant de respecter le principe général du Chapitre V du RGPD afin de procéder à un transfert licite (art. 44 RGPD)	584
1.3. Obligation du responsable du traitement ou du sous-traitant de respecter un des trois instruments de transfert du Chapitre V du RGPD afin de procéder à un transfert licite: décision d'adéquation, garanties appropriées ou dérogations particulières (art. 45-47 et 49 GPD)	585
1.3.1. Transferts fondés sur une décision d'adéquation (art. 45 RGPD)	585
1.3.2. Transferts moyennant des garanties appropriées (art. 46 et 47 RGPD)	585
1.3.3. Dérogations pour des situations particulières (art. 49 RGPD)	585
2. Rappel de la procédure et de la décision « Schrems 1 » (arrêt CJUE, 6 octobre 2015, C-362/14)	585
2.1. Introduction d'une plainte auprès du commissaire	585
2.2. Rejet de la plainte par le commissaire car il considère être tenu par la décision Safe Harbour	586
2.3. Introduction d'un recours devant la Haute Cour d'Irlande, demande de renvoi préjudiciel et réponses de la Cour	586
3. Affaire « Schrems 2 » à la suite de la décision « Schrems 1 »	587
3.1. Annulation du rejet de la plainte et renvoi de la procédure au commissaire (en application de la décision Schrems 1)	587
3.2. Clauses contractuelles types	587
3.3. Reformulation de la plainte	587
3.4. Devoir d'enquête du commissaire (en application de la décision Schrems 1)	587
3.5. Introduction d'un recours devant la Haute Cour d'Irlande et demande de renvoi préjudiciel devant la Cour (en application de la décision Schrems 1)	587
3.6. Application du RGPD et adoption du « Privacy Shield » en cours de procédure	587
4. Analyse de la décision « Schrems 2 » (arrêt CJUE, 16 juillet 2020, C-311/18)	588
4.1. Position de la Haute Cour d'Irlande, juridiction de renvoi	588
4.2. Questions préjudicielles et réponses de la Cour	589
4.2.1. Application du RGPD nonobstant le fait que les données soient ultérieurement traitées à des fins de sécurité nationale (question 1)	589
4.2.2. Obligation pour le destinataire d'offrir un niveau de protection « substantiellement équivalent » à celui garanti par l'Union (questions 2, 3 et 6)	590
4.2.3. Obligation des Autorités de contrôle de suspendre ou d'interdire un transfert fondé sur les clauses contractuelles types lorsque le destinataire est dans l'incapacité de respecter ces clauses et que le niveau de protection substantiellement équivalent à celui garanti par l'Union ne peut pas être assuré par d'autres moyens (question 8)	590
4.2.4. La décision CPT est valide étant donné qu'elle prévoit des mécanismes effectifs permettant, en pratique, d'assurer que des transferts reposant sur le fondement des clauses contractuelles types	

¹ Avocate au barreau de Bruxelles.

<i>soient suspendus ou interdits lorsque le destinataire du transfert ne respecte pas ces clauses ou se trouve dans l'incapacité de les honorer et que le niveau de protection « substantiellement équivalent » ne peut pas être assuré par d'autres moyens (questions 7 et 11)</i>	591
<i>4.2.5. La décision BPD est invalide car les ingérences des agences de renseignement américaines dans le cadre de leurs programmes de surveillance ne se limitent pas à ce qui est strictement nécessaire (non-respect du principe de proportionnalité du RGPD) et que les personnes concernées n'ont pas de voies de recours juridictionnel effectives contre ces autorités américaines (questions 4, 5, 9 et 10)</i>	592
5. Réactions des Autorités de contrôle, du Comité et du marché international à la suite de la décision « Schrems 2 »	594
5.1. Premières réactions des Autorités de contrôle: prudentes vs. strictes	594
5.2. Déclaration du Comité selon laquelle il déclare être en train d'analyser la décision Schrems 2 afin de proposer des exemples concrets de « mesures de protection complémentaires » aux clauses contractuelles types (si nécessaire) afin d'offrir un « niveau de protection adéquat » tel que requis par l'Union & adoption d'un document clé « foire aux questions » (« FAQ ») dans lequel il clarifie certains points ayant fait l'objet de discussions à la suite de la décision Schrems 2	594
5.3. Premières réactions des organisations: « en route vers le changement » vs. « paralysie »	595
5.4. Projet de recommandations 01/2020 du Comité proposant des « mesures de protection complémentaires » aux clauses contractuelles types, projet de nouvelles clauses types et recommandations 02/2020 sur les garanties européennes essentielles aux mesures de surveillance	595
5.5. Déclaration des Etats-Unis en réponse à la décision Schrems 2	596
Conclusion.	596

RÉSUMÉ

Le présent article traite du transfert de données à caractère personnel de l'Espace économique européen vers un pays tiers ou à une organisation internationale au sens du RGPD et de l'invalidation de la décision n° 2016/1250 de la Commission européenne relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis (arrêt de la CJEU du 16 juillet 2020 dans l'affaire C-311/18). La présente contribution vise à faire le point sur le cadre législatif et jurisprudentiel européen actuellement applicable à de tels transferts.²

SAMENVATTING

Dit artikel behandelt de doorgifte van persoonsgegevens vanuit de Europese Economische Ruimte naar een derde land of naar een internationale organisatie in de zin van de AVG en de ongeldigverklaring van het besluit nr. 2016/1250 van de Europese Commissie betreffende de gepastheid van de door het EU-VS-privacyschild geboden bescherming (arrest van het HvJ van 16 juli 2020 in zaak C-311/18). Deze bijdrage omschrijft het Europese wetgevings- en jurisprudentiekader dat momenteel van toepassing is op dergelijke doorgiften.

INTRODUCTION³

L'un des objectifs principaux de l'Union européenne (ci-après, l'« Union ») est d'assurer un niveau élevé de protection des données à caractère personnel (ci-après, les

« données ») même lorsque celles-ci quittent le territoire européen.⁴ A cet égard, elle adopte une première *directive*⁵ en 1995, que le « RGPD »⁶ remplace en 2016. Bien que la

² Cette présente contribution tient compte uniquement du RGPD, du droit belge relatif à la protection des données à caractère personnel au sens du RGPD et aux 2 décisions de la Cour de justice de l'Union européenne « Schrems 1 et 2 ». Cette contribution n'a pas vocation à tenir compte d'autres législations complémentaires qui pourraient éventuellement s'appliquer à de tels transferts de données e.g. en matière de données de santé, de localisation de données, etc.

³ Cet article a été écrit le 2 décembre 2020 et peut ne pas être complètement à jour avec les derniers développements.

⁴ Considérant (101) RGPD.

⁵ Directive n° 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (J.O.L. 281, p. 31). Vous constaterez que ces dispositions ont été reprises dans le RGPD.

⁶ Règlement (UE) n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive n° 95/46/CE (règlement général sur la protection des données) (« RGPD »).

législation européenne en matière de protection des données existe, il est légitime de questionner encore à l'heure actuelle la manière dont cet objectif peut être atteint surtout à la suite de certaines révélations.

En 2013, M. Edward Snowden révèle que les services de renseignements aux Etats-Unis traitent des données en masse, y compris de personnes situées en dehors des Etats-Unis, dans le cadre de programmes de surveillance. En 2018, s'ensuit l'affaire « *Cambridge Analytica* » qui donne suite à différentes plaintes et enquêtes menées par les autorités de protection des données compétentes.

En référence aux révélations de E. Snowden, Maximilian Schrems⁷, un autrichien militant pour la protection de la vie privée et des données, s'inquiète du sort de ses données transférées de « Facebook Ireland » vers « Facebook Inc. » située aux Etats-Unis. Il introduit, le 25 juin 2013, une plainte auprès du commissaire de l'autorité irlandaise de protection des données (« Data Protection Commissioner »)⁸ (ci-après, le « *commissaire* »). La plainte est d'abord rejetée par le commissaire, considérant que ces transferts sont autorisés par la décision d'adéquation n° 2000/520⁹ émise par la Commission européenne et qu'il est tenu par cette décision (ci-après, la « *Commission* » et la « *décision Safe Harbor* »). Ceci fera l'objet d'une procédure devant la Haute Cour d'Irlande et d'un renvoi préjudiciel devant la Cour de justice de l'Union européenne (ci-après, la « *Cour* »). La Cour donne finalement raison à M. Schrems, dans son arrêt du 6 octobre 2015 (ci-après, la « *décision Schrems 1* »)¹⁰, en considérant que, en substance, les Etats-Unis n'offrent pas un niveau de protection adéquat des données tel que requis par l'Union et invalide la décision *Safe Harbor*. Elle considère, en outre, que les autorités nationales de protection des données de l'Union (ci-après, les « *Autorités de contrôle* ») ont l'obligation d'examiner l'ensemble des faits portés devant elles même lorsque ces faits concernent une remise en cause de la validité d'une décision d'adéquation.

A la suite de la décision *Schrems 1*, la Haute Cour d'Irlande annule le rejet de la plainte de M. Schrems et renvoie celle-ci au commissaire afin de la réévaluer. La décision *Safe Harbor* étant invalide, Facebook justifie désormais transférer une grande partie des données de l'EEE vers les Etats-Unis sur la base des « clauses contractuelles types », reprises dans la décision n° 2010/87¹¹ de la Commission (ci-après, la « *décision CPT* »). Néanmoins, M. Schrems maintient ses arguments selon lesquels les Etats-Unis n'offrent toujours pas de niveau de protection adéquat des données. Il fait, à nouveau, référence à l'accès et à l'utilisation des données en provenance de l'EEE par les services de renseignement américains d'une manière incompatible avec le droit de l'Union. Il réitère ainsi sa demande de suspendre ou d'interdire de tels transferts vers les Etats-Unis.

Dans le courant de la procédure, la Commission, après avoir longuement (re)négocié avec les Etats-Unis à la suite de la décision *Schrems 1*, adopte un nouveau cadre juridique permettant de transférer des données de l'EEE vers les Etats-Unis. Il s'agit de la « deuxième » décision d'adéquation n° 2016/1250¹² « *Privacy Shield* » ou « *Bouclier de protection* » (ci-après, la « *décision BPD* ») qui succède à la décision *Safe Harbor*. Ce cadre fonctionne globalement de la même manière que le « *Safe Harbor* » sauf que, suite à la décision *Schrems 1*, le « *Privacy Shield* » est censé ne plus permettre la surveillance en masse effectuée par les agences de renseignement américaines et renforcer le contrôle sur les entreprises américaines adhérant à ces principes (largement inspirés par le RGPD).

A la suite d'une longue procédure judiciaire, la Cour est à nouveau saisie d'un renvoi préjudiciel qui aboutit à une nouvelle décision du 16 juillet 2020 dans laquelle elle donne une nouvelle fois raison à M. Schrems (ci-après, la « *décision Schrems 2* »)¹³. Elle considère que, en substance, les Etats-Unis n'offrent toujours pas de niveau de protection des données substantiellement équivalent à celui garanti par l'Union. Elle invalide dès lors la « deuxième » décision *BPD*.

7. Forbes, Maximilian Schrems, www.forbes.com/profile/maximilian-schrems/, consulté le 20 novembre 2020; NOYB, www.noyb.eu/en/our-detailed-concept/, consulté le 20 novembre 2020.

8. Data Protection Commission est l'autorité de contrôle irlandaise (Supervisory Authority), www.dataprotection.ie/, consulté le 16 novembre 2020.

9. Décision de la Commission du 26 juillet 2000 conformément à la directive n° 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 Etats-Unis d'Amérique (*J.O.*, 2000, L. 215, p. 7). Pour rappel, la Commission et le département américain du commerce avaient négocié un premier cadre juridique de transfert, le « EU-US Safe Harbor » ou « Sphère de sécurité », permettant, dans certaines conditions, l'échange de données à caractère personnel de l'EEE vers les Etats-Unis. Concrètement, ce cadre est repris dans la décision d'adéquation n° 2000/520 de la Commission permettant à des entreprises américaines par un mécanisme d'autocertification, d'adhérer aux principes dits du « *Safe Harbor* », largement inspirés de la directive, et d'être ainsi reconnues comme offrant un « niveau adéquat de protection » des données. Un grand nombre de sociétés américaines avaient par la suite adhéré à ce cadre. J. HICK et R. INVIJAJEV, « Transferts de données à caractère personnel vers l'étranger », in *RGPD: quel impact sur la gestion du personnel?*, p. 101, Wolters Kluwer, mars 2018.

10. Arrêt de la Cour (gde ch.) du 6 octobre 2015 dans l'affaire C-362/14, www.eur-lex.europa.eu/leg.al-content/FR/TXT/PDF/?uri=CELEX:62014CJ0362&from=FR, consulté le 10 novembre 2020.

11. 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 n° 95/46/CE du Parlement européen et du Conseil (*J.O.*, 2010, L. 39, p. 5), telle que modifiée par la décision d'exécution (UE) n° 2016/2297 de la Commission du 16 décembre 2016 (*J.O.*, 2016, L. 344, p. 100).

12. Décision d'exécution de la Commission du 12 juillet 2016 conformément à la directive n° 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-Etats-Unis (*J.O.*, 2016, L. 207, p. 1).

13. Arrêt de la Cour (gde ch.), 16 juillet 2020, dans l'affaire C311/18, www.curia.europa.eu/juris/document/document.jsf?docid=228677&doclang=FR, consulté le 10 novembre 2020.

qui succède à la décision *Safe Harbor*. En outre, elle considère que la décision *CPT* est valide. Cependant, elle juge que le responsable du traitement ou le sous-traitant a l'obligation de vérifier si le pays tiers concerné par de tels transferts offre un niveau de protection des données substantiellement équivalent à celui garanti par l'Union. A défaut, il doit mettre en œuvre, outre les clauses contractuelles types, des mesures complémentaires de protection afin de combler cette insuffisance de protection. S'il n'est pas possible d'honorer ces clauses et d'obtenir un niveau de protection substantiellement équivalent à celui de l'Union par d'autres moyens, le transfert doit être suspendu ou terminé par les parties, et à défaut par les Autorités de contrôle.

Dans ce contexte, l'objectif de la présente contribution est de faire le point sur le cadre législatif et jurisprudentiel européen actuellement applicable aux transferts de données en provenance de l'Espace économique européen (ci-après « *EEE* »), vers un pays tiers (Chapitre V du RGPD). A cette occasion, nous rappelons les concepts clés et les conditions formulées par le Chapitre V du RGPD permettant un transfert licite de données de l'EEE vers un pays tiers. Nous revenons brièvement sur la procédure et la décision *Schrems 1* de 2015 qui nous mène à l'analyse de la procédure et la décision *Schrems 2* de 2020. Avant de conclure, nous abordons la manière dont la décision *Schrems 2* est perçue par les Autorités de contrôle, le Comité européen de la protection des données¹⁴ (ci-après, le « *Comité* ») et le marché international.

1. OBLIGATION DE RESPECTER LE CHAPITRE V DU RGPD AFIN DE PROCÉDER À UN TRANSFERT LICITE DE DONNÉES À CARACTÈRE PERSONNEL DE L'EEE VERS UN PAYS TIERS OU À UNE ORGANISATION INTERNATIONALE (ART. 44 ET S.)

Qu'est-ce qu'un transfert de données vers un pays tiers selon le RGPD? Quels en sont les principes applicables? Quels sont les trois instruments de transfert permettant un transfert licite?

1.1. Définitions (large) de « transfert » par l'Autorité de contrôle du UK (ICO) et de « pays tiers » par le Comité

Le RGPD ne définissant pas précisément les termes « transfert de données » et « pays tiers », nous empruntons la définition de l'Autorité de contrôle du UK (ICO) ainsi que celle du Comité. L'ICO définit un « transfert de données » comme étant: « *The processing of personal data, whereby you are sending personal data, or making it accessible, to a recipient to which the GDPR does not apply (usually because they are outside of the EEA) and the receiver is a separate organization or individual.* »¹⁵

Le Comité définit un « pays tiers » comme étant tout pays qui n'est pas membre de l'EEE.¹⁶ Pour rappel, l'EEE se compose des Etats membres de l'Union ainsi que de la Norvège, de l'Islande et du Liechtenstein.¹⁷

Sur la base de ces définitions, nous comprenons que dès qu'une entreprise située en dehors de l'EEE reçoit ou traite

autrement des données soumises au respect du RGPD ou a même simplement accès à ces données (e.g. stockage de données sur des serveurs étrangers, support administratif étranger qui a accès aux données stockées dans l'EEE, etc.), il s'agira d'un transfert de données vers un pays tiers au sens du RGPD engendrant pour l'exportateur le respect de son Chapitre V (ci-après, « *Transfert(s)* »).

1.2. Obligation du responsable du traitement ou du sous-traitant de respecter le principe général du Chapitre V du RGPD afin de procéder à un transfert licite (art. 44 RGPD)

Afin de procéder à des transferts licites, le responsable du traitement ou le sous-traitant doit respecter les dispositions du Chapitre V du RGPD lequel prévoit un principe général applicable à tous les transferts et trois instruments de transferts à respecter. Selon l'article 44 du RGPD, le *principe général* prévoit que de ces transferts ne peuvent avoir lieu que si (1) toutes les dispositions générales du RGPD sont respectées (i.e. principe de licéité, de transparence, de minimisation, etc.) et que si (2) le « niveau de protection » des personnes physiques garanti par le RGPD « n'est pas compromis à la suite de tels transferts ».¹⁸

¹⁴. European Data Protection Board (EDBP).

¹⁵. ICO, « *International Transfers* », www.ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers/, consulté le 20 novembre 2020.

¹⁶. EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, www.edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf, p. 20, consulté le 16 novembre 2020.

¹⁷. PARLEMENT EUROPEEN, « L'Espace économique européen (EEE), la Suisse et le Nord », www.europarl.europa.eu/factsheets/fr/sheet/169/l-espace-economique-europeen-eee-la-suisse-et-le-nord, consulté le 2 décembre 2020.

¹⁸. Art. 44 RGPD et considérant (101) RGPD.

1.3. Obligation du responsable du traitement ou du sous-traitant de respecter un des trois instruments de transfert du Chapitre V du RGPD afin de procéder à un transfert licite: décision d'adéquation, garanties appropriées ou dérogations particulières (art. 45-47 et 49 GPD)

1.3.1. Transferts fondés sur une décision d'adéquation (art. 45 RGPD)

Premièrement, selon l'article 45 du RGPD et son considérant (103), un responsable du traitement ou un sous-traitant est autorisé à procéder à un transfert lorsque la destination ou le destinataire (i.e. un pays tiers, un territoire ou un ou plusieurs secteurs d'activité déterminés) a obtenu une *décision d'adéquation* émise par la Commission. Dans ce cas, la Commission a estimé que cette destination ou ce destinataire offre un *niveau adéquat de protection* des données.¹⁹

La Commission doit *évaluer le caractère adéquat de protection des données en tenant compte de plusieurs éléments tels que*: l'état de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente y compris en ce qui concerne la sécurité nationale, ainsi que l'accès des autorités publiques aux données, l'existence et le fonctionnement effectif d'Autorités de contrôle indépendantes dans le pays tiers, etc.²⁰

La Commission doit *réévaluer* sa décision, au moins tous les 4 ans, en prenant en compte toutes les évolutions pertinentes. Si la Commission constate qu'il n'y a plus ce niveau adéquat de protection, elle doit *abroger, modifier ou suspendre sa*

décision.²¹ La Commission publie la liste de ses décisions d'adéquation sur son site internet.²²

1.3.2. Transferts moyennant des garanties appropriées (art. 46 et 47 RGPD)

Deuxièmement, selon l'article 46 du RGPD et son considérant (108), à défaut de décision d'adéquation, un responsable du traitement ou un sous-traitant est autorisé à procéder à un transfert lorsqu'il a mis en place des *garanties appropriées* afin de *compenser l'insuffisance de la protection*. Ces garanties peuvent consister à la mise en place des règles d'entreprises contraignantes, des clauses contractuelles types adoptées par la Commission, d'un code de conduite approuvé, etc.²³

En outre, les personnes concernées doivent disposer de *droits opposables et de voies de droit effectives* ce qui comprend « *le droit d'engager un recours administratif ou juridictionnel effectif et d'introduire une action en réparation, dans l'Union ou dans un pays tiers* ».²⁴

1.3.3. Dérogations pour des situations particulières (art. 49 RGPD)

Troisièmement, selon l'article 49 du RGPD, en l'absence de décision d'adéquation et de garanties appropriées, il est autorisé de procéder à un transfert uniquement lorsqu'il s'agit d'une situation particulière telle que définie par le RGPD.²⁵ Nous avons décidé de ne pas nous attarder sur cet instrument de transfert car celui-ci n'est pas pertinent dans le cadre de cette présente contribution.

2. RAPPEL DE LA PROCÉDURE ET DE LA DÉCISION « SCHREMS I » (ARRÊT CJUE, 6 OCTOBRE 2015, C-362/14)

2.1. Introduction d'une plainte auprès du commissaire

M. Schrems, utilisateur de Facebook depuis 2008, s'inquiète du sort de ses données transférées de l'EEE vers les Etats-Unis.²⁶

Le 25 juin 2013, il introduit une plainte auprès du commissaire. A cet égard, il fait notamment référence aux révélations de E. Snowden concernant les traitements en masse des données, y compris de personnes situées en dehors des Etats-Unis, par les services de renseignement des Etats-Unis dont la « National Security Agency »²⁷ (ci-après, la « *plainte* »).²⁸

¹⁹. Art. 45, 1. RGPD et considérant (103) RGPD.

²⁰. Art. 45, 2., a), RGPD.

²¹. Art. 45 RGPD et considérant (103) RGPD.

²². COMMISSION EUROPEENNE, « Adequacy decisions, How the EU determines if a non-EU country has an adequate level of data protection », www.ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en, consulté le 16 novembre 2020.

²³. Art. 46 RGPD et considérant (108) RGPD.

²⁴. Art. 46 RGPD et considérant (108) RGPD.

²⁵. Art. 49 RGPD.

²⁶. § 26-28 de la décision *Schrems I*.

²⁷. National Security Agency (ci-après, la « NSA »), www.nsa.gov/, consulté le 20 novembre 2020.

²⁸. § 28 de la décision *Schrems I*.

M. Schrems argumente que le droit et les pratiques aux **Etats-Unis n'offrent pas de protection suffisante de ses données** contre l'accès et l'utilisation par les autorités du gouvernement américain. Il demande dès lors au commissaire *à faire interdire ces transferts*.²⁹

« On the 25th of June, 2013, Mr. Schrems filed a complaint with the DPC [le Commissaire] in relation to the processing of his personal data by Facebook. He contended that in the light of Mr. Snowden's disclosures, the transfer of his personal data by Facebook to its US parent, Facebook Inc. for processing was unlawful both under national and EU law. »³⁰

2.2. Rejet de la plainte par le commissaire car il considère être tenu par la décision *Safe Harbour*

Cette plainte est rejetée par le commissaire car ce dernier estime que celle-ci est dépourvue de fondement. Il considère, en résumé, qu'il n'existe pas de preuve que la NSA ait accédé aux données de M. Schrems, que ces transferts sont autorisés en application de la décision *Safe Harbour* et qu'il est tenu par cette décision d'adéquation.³¹

« The DPC [le Commissaire] took the view that as the Commission had adopted the *Safe Harbour Decision* establishing and/or endorsing the *Safe Harbour arrangements*, the DPC was bound to accept the *Safe Harbour Decision* as binding upon him in light of Article 25 (6) of the Directive and s. 11 (2) of the Acts. On that basis, the DPC declined to investigate Mr. Schrems' complaint, deeming it unsustainable in law. »³²

2.3. Introduction d'un recours devant la Haute Cour d'Irlande, demande de renvoi préjudiciel et réponses de la Cour

Le 21 octobre 2013, M. Schrems introduit une procédure

devant la Haute Cour d'Irlande afin de lui demander d'annuler le rejet de sa plainte et d'ordonner au commissaire de mener une enquête et de statuer au fond.³³

« Mr. Schrems instituted judicial review proceedings on the 21st of October, 2013, seeking orders to quash the DPC's refusal to investigate his complaint and directing the DPC to investigate and decide his complaint on its merits. »³⁴

La Haute Cour d'Irlande décide finalement de saisir la Cour d'un renvoi préjudiciel. Il s'agit, en substance, d'interroger la Cour sur le fait de savoir si l'Autorité de contrôle est « absolument liée » par une décision d'adéquation. Dans le cas contraire, doit-elle mener sa propre enquête et analyser l'ensemble des faits faisant l'objet d'une réclamation d'une personne concernée afin de prendre position?³⁵

En résumé, la Cour considère, dans sa décision *Schrems I* du 6 octobre 2015, tout d'abord, que *les Autorités de contrôle doivent pouvoir examiner en toute indépendance si* de tels transferts respectent les exigences de la directive et ce, à la lumière des articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne³⁶ (ci-après, la « charte ») *même lorsqu'il existe une décision d'adéquation*. En revanche, la Cour précise qu'elle est la seule à pouvoir, si nécessaire, décider si une telle décision est valide ou non. C'est la raison pour laquelle, selon elle, les Autorités de contrôle doivent pouvoir saisir les juridictions nationales afin d'examiner le « niveau de protection adéquat » et introduire un renvoi préjudiciel en cas de doutes sérieux quant à la validité d'une telle décision. A cet égard, la Cour considère, à la suite de son analyse, que les *Etats-Unis n'assurent pas un niveau de protection adéquat* en vertu de la directive lue à la lumière de la charte et dès lors *invalide la décision Safe Harbour*.³⁷

Partant, les transferts de données basés sur l'adhésion d'une entreprise américaine aux principes du « Safe Harbor », en se fondant sur la décision *Safe Harbor*, deviennent illégaux.³⁸

²⁹. § 28 de la décision *Schrems I*.

³⁰. § 21 de l'arrêt du 3 octobre 2017 de la Haute Cour d'Irlande (« The High Court Commercial »), 2016, n° 4809 P., www.iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf, consulté le 24 novembre 2020. Procédure par laquelle le Commissaire demande à la Haute Cour d'Irlande d'introduire un renvoi préjudiciel à la Cour concernant la validité de 3 décisions de la Commission relatives aux transferts de données personnelles de l'EEE vers les Etats-Unis.

³¹. § 29 de la décision *Schrems I*.

³². § 22 de l'arrêt du 3 octobre 2017 de la Haute Cour d'Irlande (« The High Court Commercial »), 2016, n° 4809 P., www.iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf, consulté le 24 novembre 2020.

³³. § 23 de l'arrêt du 3 octobre 2017 de la Haute Cour d'Irlande (« The High Court Commercial »), 2016, n° 4809 P., www.iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf, consulté le 24 novembre 2020.

³⁴. § 23 de l'arrêt du 3 octobre 2017 de la Haute Cour d'Irlande (« The High Court Commercial »), 2016, n° 4809 P., www.iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf, consulté le 24 novembre 2020.

³⁵. § 28-36 de la décision *Schrems I*.

³⁶. Art. 7, 8 et 47 de la charte, www.eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:FR:PDF, consulté le 24 novembre 2020.

³⁷. § 67-106 de la décision *Schrems I* et § 53 de la décision *Schrems 2* se référant à la décision *Schrems I*.

³⁸. § 25, dernière ligne, de l'arrêt du 3 octobre 2017 de la Haute Cour d'Irlande (« The High Court Commercial »), 2016, n° 4809 P., www.iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf, consulté le 24 novembre 2020. J. HICK et R. INVIAJEV, « Partie 6. Transferts de données à caractère personnel vers l'étranger », *RGPD: quel impact sur la gestion du personnel*, Wolters Kluwer, p. 101, mars 2018, www.jura.kluwer.be/secure/showfile.aspx?id=dx2230554.pdf&source=HICK,%20J.,%20INVIAJEV,%20R.,%20Transferts%20de%20donn%C3%A9es%20%C3%A0%20caract%C3%A8re%20personnel%20vers%20l'E2%80%99%C3%A9tranger&sourceid=df300205306&originating-page=resultlist, consulté le 27 novembre 2020. § 25, dernière ligne, de l'arrêt du 3 octobre 2017 de la Haute Cour d'Irlande (« The High Court Commercial »), 2016, n° 4809 P., www.iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf, consulté le 24 novembre 2020.

3. AFFAIRE « SCHREMS 2 » À LA SUITE DE LA DÉCISION « SCHREMS 1 »

3.1. Annulation du rejet de la plainte et renvoi de la procédure au commissaire (en application de la décision *Schrems 1*)

A la suite de la décision *Schrems 1*, la Haute Cour d'Irlande annule le rejet de la plainte de M. Schrems et renvoie celle-ci au commissaire afin de la réévaluer.³⁹

3.2. Clauses contractuelles types

Facebook Ireland justifie qu'il réalise désormais une grande partie de ces transferts de données vers les Etats-Unis en se fondant sur les clauses contractuelles types figurant à l'annexe de la décision *CPT* (autre instrument de transfert). La Cour précise, en effet, que : « Dans le cadre de l'enquête ouverte par ce dernier [le Commissaire], Facebook Ireland a expliqué qu'une grande partie des données à caractère personnel était transférée à Facebook Inc. sur le fondement des clauses types de protection des données figurant à l'annexe de la décision *CPT*. Compte tenu de ces éléments, le commissaire a invité M. Schrems à reformuler sa plainte. »⁴⁰

3.3. Reformulation de la plainte

Dans sa plainte reformulée, M. Schrems maintient ses arguments selon lesquels les Etats-Unis n'offrent toujours pas de protection suffisante de ses données et réitère sa demande auprès du commissaire visant essentiellement à interdire ou à suspendre ces transferts. M. Schrems fait valoir, notamment, que le droit américain impose à la société américaine Facebook Inc. de mettre leurs données à la disposition des autorités américaines, telles que la NSA et le Federal Bureau of Investigation⁴¹ (ci-après, « FBI »). Il soutient que, « ces données étant utilisées dans le cadre de différents programmes de surveillance d'une manière incompatible avec les articles 7, 8 et 47 de la charte, la décision *CPT* ne peut justifier le transfert desdites données vers les Etats-Unis. »⁴²

3.4. Devoir d'enquête du commissaire (en application de la décision *Schrems 1*)

Le 24 mai 2016, le commissaire, ayant désormais une obligation confirmée par la Cour de mener sa propre enquête en application de la décision *Schrems 1*, publie un « projet de décision » dans lequel il considère qu'il existe en effet un

risque que ces données soient consultées et traitées par les autorités américaines d'une manière incompatible avec les articles 7 et 8 de la charte. Le commissaire ajoute que le droit et les pratiques des Etats-Unis n'offrent pas aux personnes concernées des voies de recours compatibles avec l'article 47 de la charte. Le commissaire estime par ailleurs que les clauses contractuelles types ne permettent pas de remédier à ce défaut de protection. Le commissaire précise en effet que, comme son nom l'indique, ces clauses confèrent aux personnes concernées uniquement des droits contractuels contre l'exportateur et l'importateur des données, sans toutefois lier les autorités américaines qui ne sont pas parties au contrat.⁴³

3.5. Introduction d'un recours devant la Haute Cour d'Irlande et demande de renvoi préjudiciel devant la Cour (en application de la décision *Schrems 1*)

Le 31 mai 2016, le commissaire décide lui-même, à nouveau en s'appuyant sur la décision *Schrems 1*, de faire intervenir la Haute Cour d'Irlande afin de lui demander de saisir (à nouveau) la Cour par une question préjudicielle. Il estime que le traitement de la plainte de M. Schrems dépend une nouvelle fois de la validité d'une décision de la Commission à savoir, la décision *CPT*. Par décision du 4 mai 2018, la Haute Cour d'Irlande saisit la Cour du renvoi préjudiciel.⁴⁴

3.6. Application du RGPD et adoption du « Privacy Shield » en cours de procédure

Le 25 mai 2018, dans le courant de cette procédure de renvoi préjudiciel, le RGPD entre en application et remplace la directive. Le RGPD sera dès lors le cadre législatif pris en compte par la Cour.

En outre, il est à noter qu'après l'ouverture de cette procédure de renvoi préjudiciel, la Commission, après avoir longuement (re)négocié avec les Etats-Unis à la suite de la décision *Schrems 1*, adopte un nouveau cadre juridique permettant de transférer des données de l'EEE vers les Etats-Unis. Il s'agit de la décision *BPD*. Ce cadre fonctionne globalement de la même manière que le « Safe Harbor » sauf que, suite à la décision *Schrems 1*, le « Privacy Shield » est censé ne plus permettre la surveillance en masse effectuée par les agences de renseignement américaines et renforcer le con-

^{39.} § 54 de la décision *Schrems 2*.

^{40.} § 54 de la décision *Schrems 2*.

^{41.} Federal Bureau of Investigation (FBI), www.fbi.gov/, consulté le 16 novembre 2020.

^{42.} § 55 de la décision *Schrems 2*.

^{43.} § 56 de la décision *Schrems 2*.

^{44.} § 57 de la décision *Schrems 2*.

trôle sur les entreprises américaines adhérant à ces principes (largement inspirés par le RGPD).⁴⁵ Tel que vous le constaterez ci-dessous, la validité de la décision *BPD* sera égale-

ment remise en cause par M. Schrems dans le cadre de la deuxième procédure de renvoi préjudiciel devant la Cour.

4. ANALYSE DE LA DÉCISION « *SCHREMS 2* » (ARRÊT CJUE, 16 JUILLET 2020, C-311/18)

4.1. Position de la Haute Cour d'Irlande, juridiction de renvoi

Dans le cadre de la procédure de renvoi préjudiciel devant la Cour, la Haute Cour d'Irlande se réfère à son arrêt du 3 octobre 2017⁴⁶, dans lequel elle manifeste, entre autres, son accord avec le point de vue de M. Schrems selon lequel le commissaire a des « préoccupations bien fondées » (« *well founded concerns* ») concernant le droit et les pratiques des Etats-Unis en matière de protection des données.⁴⁷

Dans cet arrêt, auquel la demande de décision préjudicielle se réfère à plusieurs reprises, elle constate que les activités de renseignement des autorités américaines se fondent, notamment, sur l'article 702 du FISA⁴⁸ et sur l'Executive Order 12333⁴⁹ (ci-après, l'« *E.O. 12333* »).⁵⁰

Concernant l'article 702 du FISA, « cet article permet [...] d'autoriser la surveillance de ressortissants non américains se trouvant en dehors du territoire des Etats-Unis et sert, notamment, de fondement aux programmes de surveillance PRISM et UPSTREAM ».⁵¹ Dans le cadre du programme PRISM, « les fournisseurs de services Internet sont tenus,

[...] de fournir toutes les communications envoyées et reçues par un 'sélecteur', [...] ».⁵² Concernant le programme UPSTREAM, [...], « les entreprises de télécommunications exploitant la 'dorsale' de l'internet – c'est-à-dire le réseau de câbles, commutateurs et routeurs – sont contraintes de permettre [...] de copier et de filtrer les flux de trafic Internet afin de recueillir des communications envoyées par ou reçues par ou concernant le ressortissant non américain visé par un 'sélecteur'. Dans le cadre dudit programme, la NSA a, [...], accès tant aux métadonnées qu'au contenu des communications concernées ».⁵³

En ce qui concerne l'E.O. 12333, « celui-ci permet [...] d'accéder à des données 'en transit' vers les Etats-Unis, en accédant aux câbles sous-marins posés sur le plancher de l'Atlantique, ainsi que de recueillir et de conserver ces données avant qu'elles arrivent aux Etats-Unis et y soient soumises aux dispositions du FISA. [...] les activités fondées sur l'E.O. 12333 ne sont pas régies par la loi ».⁵⁴ D'autre part, concernant les limites éventuelles apportées à ces activités de surveillance, la Haute Cour d'Irlande attire l'attention sur le fait que « les personnes non américaines relèvent uni-

45. J. HICK et R. INVIAJEV, « Partie 6. Transferts de données à caractère personnel vers l'étranger », *RGPD: quel impact sur la gestion du personnel*, Wolters Kluwer, p. 101, mars 2018, www.jura.kluwer.be/secure/showfile.aspx?id=dx2230554.pdf&source=HICK,%20J.%20INVIAJEV,%20R.%20Transferts%20de%20donn%C3%A9es%20%C3%A0%20caract%C3%A8re%20personnel%20vers%20l'E2%80%99%C3%A9tranger&source=df300205306&originatingpage=resultlist, consulté le 27 novembre 2020.

46. Arrêt du 3 octobre 2017 de la Haute Cour d'Irlande (« The High Court Commercial »), 2016, n° 4809 P., www.iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf, consulté le 24 novembre 2020. Procédure par laquelle le Commissaire demande à la Haute Cour d'Irlande d'introduire un renvoi préjudiciel à la Cour concernant la validité de 3 décisions de la Commission relatives aux transferts de données personnelles de l'EEE vers les Etats-Unis.

47. « To my mind the arguments of the DPC that the laws – and indeed the practices of the United States do not respect the essence of the right to an effective remedy before an independent tribunal as guaranteed by Art. 47 of the Charter, which applies to the data of all EU data subjects transferred to the United States, are well founded. Furthermore, even if the essence of that right is respected, there are, for the reasons advanced by the DPC, well founded concerns that the limitations on the exercise of that right faced by EU data subjects in the United States are not proportionate and are not strictly necessary within the meaning of Art. 52 (1) of the Charter. » Source: § 290 de l'arrêt du 3 octobre 2017 de la Haute Cour d'Irlande (« The High Court Commercial »), 2016, n° 4809 P., www.iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf, consulté le 24 novembre 2020. IAPP, « Irish High Court Decision in DPC v. Facebook Ireland Limited and Max Schrems », www.iapp.org/resources/article/irish-high-court-decision-in-dpc-v-facebook-ireland-limited-and-max-schrems/, consulté le 24 novembre 2020.

48. « Section 702 is a key provision of the FISA Amendments Act of 2008 that permits the government to conduct targeted surveillance of foreign persons located outside the United States, with the compelled assistance of electronic communication service providers, to acquire foreign intelligence information. » Source: US Government, « Section 702 Overview », www.dni.gov/files/icoir/Section702-Basics-Infographic.pdf, consulté le 15 novembre 2020.

49. « Executive Order 12333 is an important piece in the foreign intelligence puzzle in the U.S. Originally enacted in 1981, it has been amended by EOs 13284 (2003), 13355 (2004) and 13470 (2008). The EO does not create surveillance authority in the Executive Branch but rather reflects the president setting standards and regulating conduct, setting forth collection techniques, including restrictions on them, delegating authority to certain agencies, and setting forth goals for the IC. The EO mainly deals with foreign intelligence collection techniques of the U.S. government when acting abroad. Though the EO does address certain FISA activities involving certain members of the IC, EO is an independent basis for foreign intelligence activities, apart from FISA. » Source: IAPP, « An Overview of US Surveillance in Light of Schrems II », *White Paper*, août 2020, p. 12, www.iapp.org/resources/article/overview-us-surveillance-light-of-schremsii/, consulté le 15 novembre 2020.

50. § 58 et 60 de la décision *Schrems 2*.

51. § 61 de la décision *Schrems 2*.

52. § 61 de la décision *Schrems 2*.

53. § 62 de la décision *Schrems 2*.

54. § 63 de la décision *Schrems 2*.

quement de la PPD-28⁵⁵ et que celle-ci se borne à indiquer que les activités de renseignement devraient être ‘**aussi ciblées que possible**’ (as tailored as feasible). [...] les Etats-Unis procèdent à un **traitement de données en masse, sans assurer une protection substantiellement équivalente à celle garantie par les articles 7 et 8 de la charte** ».⁵⁶

Par ailleurs, cette même juridiction expose que « **les citoyens de l'Union n'ont pas accès aux mêmes recours que ceux dont disposent les ressortissants américains contre les traitements [...], dès lors que le quatrième amendement de la Constitution of the United States (Constitution des Etats-Unis), qui constitue, en droit américain, la protection la plus importante contre la surveillance illégale, est inapplicable aux citoyens de l'Union. A cet égard, [...] les recours restant à la disposition de ces derniers se heurtent à des obstacles importants, en particulier à l'obligation – selon elle excessivement difficile à satisfaire – de justifier de leur qualité pour agir. Par ailleurs, [...], les activités [...] fondées sur l'E.O. 12333 ne font pas l'objet d'une surveillance judiciaire et ne sont pas susceptibles de recours juridictionnels. Enfin, [...], le médiateur du bouclier de protection de données ne constitue pas un tribunal, au sens de l'article 47 de la charte, le droit américain n'assure pas aux citoyens de l'Union un niveau de protection substantiellement équivalent à celui garanti par le droit fondamental consacré à cet article** ».⁵⁷

Pour davantage d'informations concernant les systèmes de surveillance aux Etats-Unis, nous renvoyons le lecteur vers deux articles de l'« International Association of Privacy Professionals » (IAPP) dont les références sont reprises en notes infrapaginales de cette présente contribution.⁵⁸

De surcroît, la Haute Cour d'Irlande s'interroge sur l'applicabilité du droit de l'Union à ces transferts lorsque les données sont susceptibles d'être traitées par les autorités du pays tiers à des fins de sécurité nationale.⁵⁹

Elle s'interroge également sur les éléments à prendre en considération aux fins de l'évaluation du « niveau de protection adéquat » assuré par le pays tiers concerné.⁶⁰

Enfin, la Haute Cour d'Irlande s'interroge sur la validité de la décision CPT dans la mesure où les clauses contractuelles types sont de nature « contractuelle », liant l'exportateur et l'importateur des données et sont dès lors « *dépourvues de caractère contraignant à l'égard des autorités étatiques du pays tiers concerné et, partant, ne sont pas de nature à remédier à une éventuelle absence de niveau de protection adéquat dans ce pays* ».⁶¹

Dans ces conditions, la Haute Cour d'Irlande décide de poser 11 questions préjudicielles à la Cour.⁶²

4.2. Questions préjudicielles et réponses de la Cour

La Cour rassemble les 11 questions préjudicielles posées, les résume en 5 questions principales et y répond de la manière suivante.

4.2.1. Application du RGPD nonobstant le fait que les données soient ultérieurement traitées à des fins de sécurité nationale (question 1)

La Haute Cour d'Irlande interroge la Cour, en substance, sur la manière dont il faut interpréter l'article 2, 1. et 2., sous a), b) et d), du RGPD, lus en combinaison avec l'article 4, 2., TUE concernant le champ d'application du RGPD. La question est de savoir si le RGPD s'applique à un transfert de données entre un opérateur économique de l'EEE (dans le cas d'espèce, Facebook Ireland) et d'un pays tiers (dans le cas d'espèce Facebook Inc.) lorsque, au cours ou à la suite de ce transfert, les données sont susceptibles d'être traitées par les autorités de ce pays tiers à des fins de sécurité publique, de défense et de sécurité de l'Etat?⁶³

La Cour répond que relève du champ d'application du RGPD « *un transfert de données à caractère personnel effectué à des fins commerciales par un opérateur économique établi dans un Etat membre vers un autre opérateur économique établi dans un pays tiers, nonobstant le fait que, au cours ou à la suite de ce transfert, ces données sont suscep-*

55. « Presidential Policy Directive 28 was issued to address certain issues regarding surveillance, including certain principles involving foreign nationals and collection of intelligence. Specifically, PPD-28 states, 'all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information'. Additionally, PPD-28 notes that, 'In determining why, whether, when, and how the United States conducts signals intelligence activities', we must weigh all of these considerations in a context in which information and communications technologies are constantly changing. » Source: IAPP, « An Overview of US Surveillance in Light of Schrems II », White Paper, août 2020, p. 17, www.iapp.org/resources/article/overview-us-surveillance-light-of-schremsii/, consulté le 15 novembre 2020.

56. § 64 de la décision Schrems 2.

57. § 65 de la décision Schrems 2.

58. IAPP, « An Overview of US Surveillance in Light of Schrems II », White Paper, août 2020, www.iapp.org/resources/article/overview-us-surveillance-light-of-schremsii/, consulté le 15 novembre 2020 et IAPP, « US surveillance law and the future of trans-Atlantic data flows », 6 août 2020, www.iapp.org/news/a/us-surveillance-law-and-the-future-of-trans-atlantic-data-flows/, consulté le 15 novembre 2020.

59. § 66 de la décision Schrems 2.

60. § 66 de la décision Schrems 2.

61. § 67 de la décision Schrems 2.

62. § 68 de la décision Schrems 2.

63. § 80 de la décision Schrems 2.

tibles d'être traitées par les autorités du pays tiers concerné à des fins de sécurité publique, de défense et de sûreté de l'Etat ». ⁶⁴ Dans le cadre de cette contribution, nous décidons de ne pas nous attarder davantage sur cette question.

4.2.2. Obligation pour le destinataire d'offrir un niveau de protection « substantiellement équivalent » à celui garanti par l'Union (questions 2, 3 et 6)

La Haute Cour d'Irlande interroge la Cour, en substance, sur la question de savoir quel est le niveau de protection des données exigé par l'article 46, 1. et 2., sous c), du RGPD en cas de transfert dont le fondement repose sur les clauses contractuelles types. En particulier, quels sont les éléments à prendre en considération pour déterminer si un tel niveau de protection est assuré ? ⁶⁵

La Cour répond que « [...] les garanties appropriées, les droits opposables et les voies de droit effectives [...] doivent assurer que les droits des personnes [...] bénéficient d'un **niveau de protection substantiellement équivalent** à celui garanti au sein de l'Union par ce règlement, lu à la lumière de la charte ». ⁶⁶

Nous observons que l'avocat général, M. Henrik SAUGMANDSGAARD ØE, a également relevé dans ses conclusions présentées le 19 décembre 2019 (ci-après, « l'avocat général ») que les dispositions du Chapitre V du RGPD visent à assurer la continuité du niveau élevé de la protection des données en cas de transfert, conformément à l'objectif de l'Union précisé au considérant (6) du RGPD. En particulier, l'avocat général soutient que le principe général de l'article 44 du RGPD vise « à éviter que les standards de protection découlant du droit de l'Union soient contournés en transférant des données à caractère personnel vers un pays tiers en vue de les y traiter ». ⁶⁷

Par ailleurs, la Cour précise également que le niveau de protection doit être « **substantiellement** » équivalent et non « **identique** » à celui de l'Union. Il s'agit d' **exiger que le pays tiers « assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et des droits fondamentaux 'substantiellement' équivalent à celui prévu par l'Union en vertu du RGPD, lu à la lumière de la charte »**. ⁶⁸

En outre, la Cour ajoute que le choix du fondement légal lié au transfert n'a pas d'impact sur cette obligation d'assurer un niveau de protection substantiellement équivalent à celui garanti au sein de l'Union. ⁶⁹ Nous constatons que ceci est également soutenu par l'avocat général, le commissaire et M. Schrems, qui énoncent que les garanties appropriées prévues à l'article 46 du RGPD doivent assurer une protection substantiellement équivalente à celle d'une décision d'adéquation. ⁷⁰

La Cour précise que « l'évaluation du niveau de protection assuré [...] doit, notamment, **prendre en considération tant les stipulations contractuelles convenues [...] que, en ce qui concerne un éventuel accès des autorités publiques de ce pays tiers aux données [...] transférées, les éléments pertinents du système juridique de celui-ci, notamment ceux énoncés à l'article 45, 2., dudit règlement** ». ⁷¹

4.2.3. Obligation des Autorités de contrôle de suspendre ou d'interdire un transfert fondé sur les clauses contractuelles types lorsque le destinataire est dans l'incapacité de respecter ces clauses et que le niveau de protection substantiellement équivalent à celui garanti par l'Union ne peut pas être assuré par d'autres moyens (question 8)

La Haute Cour d'Irlande interroge la Cour, en substance, sur la manière dont il faut interpréter et comprendre l'article 58, 2., sous f) et j), du RGPD relatif aux pouvoirs des Autorités de contrôle. La question est de savoir si une Autorité de contrôle compétente a l'obligation de suspendre ou d'interdire un transfert vers un pays tiers fondé sur les clauses contractuelles types lorsque celle-ci considère que ces clauses 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, en particulier par les articles 45 et 46 du RGPD ainsi que par la charte, ne peut pas être assurée, ou si elle ne peut le faire que dans des circonstances exceptionnelles. ⁷²

En premier lieu, la Cour rappelle que la « mission première » des Autorités de contrôle est de « contrôler l'application du RGPD et de veiller au respect de celui-ci », telle que formulée à l'article 57, 1., a), du RGPD. En particulier, la Cour met

⁶⁴. § 89 de la décision *Schrems 2*.

⁶⁵. § 90 de la décision *Schrems 2*.

⁶⁶. § 105 de la décision *Schrems 2*.

⁶⁷. § 117 des conclusions de l'avocat général du 19 décembre 2019 dans l'affaire *Schrems 2*, www.curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=30039, consulté le 20 novembre 2020.

⁶⁸. § 94 de la décision *Schrems 2*.

⁶⁹. § 96 de la décision *Schrems 2* et considérants (107)-(108) RGPD.

⁷⁰. § 115 des conclusions de l'avocat général du 19 décembre 2019 dans l'affaire *Schrems 2*, www.curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=30039, consulté le 20 novembre 2020.

⁷¹. § 105 de la décision *Schrems 2*.

⁷². § 106 de la décision *Schrems 2*.

l'accent sur l'importance de cette mission dans le cadre de transferts vers un pays tiers en faisant référence notamment au considérant (116) du RGPD qui énonce que « *lorsque des données [...] franchissent les frontières extérieures de l'Union, cela peut accroître le risque que les personnes physiques ne puissent exercer leurs droits liés à la protection des données, notamment pour se protéger de l'utilisation ou de la divulgation illicite de ces informations* ». Dans cette hypothèse, « *les autorités de contrôle peuvent être confrontées à l'impossibilité d'examiner des réclamations ou de mener des enquêtes sur les activités exercées en dehors de leurs frontières* ».⁷³

Pour ces raisons, la Cour répond « *[...], l'autorité [...] est tenue de suspendre ou d'interdire un transfert de données [...] fondé sur des clauses types de protection des données [...], lorsque cette autorité de contrôle considère, à la lumière de l'ensemble des circonstances propres à ce transfert, que ces clauses 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, en particulier par les articles 45 et 46 du RGPD et par la charte, ne peut pas être assurée par d'autres moyens, à défaut pour le responsable du traitement ou son sous-traitant établis dans l'Union d'avoir lui-même suspendu le transfert ou d'avoir mis fin à celui-ci* ».⁷⁴

Nous observons que la Cour a suivi l'argumentation de l'avocat général qui précise que les Autorités de contrôle sont tenues de réagir de manière *appropriée et efficace* afin de remédier aux éventuelles violations du RGPD. Il met l'accent sur le fait que le RGPD prévoit un large éventail de moyens qui peuvent être utilisés à cet effet (art. 58 RGPD).⁷⁵ Selon lui, bien que le choix du moyen le plus efficace relève de la discrétion de ces autorités, dans le cadre de sa mission de surveillance de l'application du RGPD, *ces autorités doivent suspendre ou interdire un transfert vers un pays tiers lorsqu'elles constatent que « les clauses contractuelles types ne sont pas respectées et qu'une protection appropriée des données transférées ne peut pas être assurée par d'autres moyens, à défaut pour l'exportateur d'avoir lui-même mis fin au transfert »*.⁷⁶

4.2.4. La décision CPT est valide étant donné qu'elle prévoit des mécanismes effectifs permettant, en pratique, d'assurer que des transferts reposant sur le fondement des clauses contractuelles types soient suspendus ou interdits lorsque le destinataire du transfert ne respecte pas ces clauses ou se trouve dans l'incapacité de les honorer et que le niveau de protection « substantiellement équivalent » ne peut pas être assuré par d'autres moyens (questions 7 et 11)

La Haute Cour d'Irlande interroge la Cour, en substance, sur la question de savoir si la décision CPT est valide au regard des articles 7, 8 et 47 de la charte. En particulier, la Haute Cour d'Irlande se demande si la décision CPT est à même d'assurer un niveau de protection adéquat des données transférées vers des pays tiers, dans la mesure où les clauses types de protection des données qu'elle prévoit ne lient pas les autorités publiques de ces pays tiers.⁷⁷

La Cour répond, en référence aux garanties appropriées prévues à l'article 46 du RGPD, que « *ces dispositions n'énoncent pas que l'ensemble desdites garanties doit nécessairement être prévu par une décision de la Commission telle que la décision CPT* ».⁷⁸

La Cour poursuit en mettant l'accent sur le fait que les clauses types de protection des données « *visent uniquement à fournir aux responsables du traitement ou à leurs sous-traitants établis dans l'Union des garanties contractuelles s'appliquant de manière uniforme dans tous les pays tiers et, dès lors, indépendamment du niveau de protection garanti dans chacun d'entre eux. Dans la mesure où ces clauses types de protection des données ne peuvent, eu égard à leur nature, fournir des garanties allant au-delà d'une obligation contractuelle de veiller à ce que le niveau de protection requis par le droit de l'Union soit respecté, elles peuvent nécessiter, en fonction de la situation prévalant dans tel ou tel pays tiers, l'adoption de mesures supplémentaires par le responsable du traitement afin d'assurer le respect de ce niveau de protection* ».⁷⁹

La Cour précise que dans le cas où le responsable de traitement ou le sous-traitant n'est pas en mesure de pouvoir prendre des mesures supplémentaires suffisantes pour garantir une telle protection, ces derniers doivent *suspendre ou mettre fin au transfert* de ces données. A défaut, la Cour considère que les Autorités de contrôle sont tenues de le faire. La

⁷³. § 108 de la décision *Schrems 2* et considérant (116) RGPD.

⁷⁴. § 121 de la décision *Schrems 2*.

⁷⁵. § 147 des conclusions de l'avocat général du 19 décembre 2019 dans l'affaire *Schrems 2*, www.curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=30039, consulté le 20 novembre 2020.

⁷⁶. § 148 des conclusions de l'avocat général du 19 décembre 2019 dans l'affaire *Schrems 2*, www.curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=30039, consulté le 20 novembre 2020.

⁷⁷. § 122-123 de la décision *Schrems 2*.

⁷⁸. Art. 46 RGPD et § 128 de la décision *Schrems 2*.

⁷⁹. § 133 de la décision *Schrems 2*.

Cour ajoute que « *tel est notamment le cas lorsque le droit de ce pays tiers impose au destinataire d'un transfert de données [...] des obligations qui sont contraignantes auxdites clauses et, partant, de nature à remettre en cause la garantie contractuelle d'un niveau de protection adéquat contre l'accès des autorités publiques dudit pays tiers à ces données* ».⁸⁰

Nous observons que l'avocat général considère que le mécanisme contractuel prévu à « l'article 46 [...] du RGPD repose sur la **responsabilisation** de l'exportateur ainsi que, à titre subsidiaire, des Autorités de contrôle. C'est **au cas par cas**, pour chaque transfert spécifique, que le responsable du traitement ou, à défaut, l'Autorité de contrôle, **examinera si** le droit du pays tiers de destination fait **obstacle** à l'exécution des clauses types et, partant, **à une protection appropriée** des données transférées, **si bien que les transferts doivent être interdits ou suspendus** ».⁸¹

Sur la base de ces arguments, la Cour considère que le seul fait que les clauses types de protection ne lient pas les autorités publiques de ces pays tiers n'étant pas des parties au contrat n'affecte pas la validité de la décision CPT.⁸² Selon la Cour, « *cette validité dépend en revanche, du point de savoir si, conformément à l'exigence résultant de l'article 46, 1. et de l'article 46, 2., sous c), du RGPD, interprétés à la lumière des articles 7, 8 et 47 de la charte, une telle décision comporte des **mécanismes effectifs** permettant, en pratique, d'**assurer que le niveau de protection requis par le droit de l'Union soit respecté et que les transferts de données [...], soient suspendus ou interdits en cas de violation de ces clauses ou d'impossibilité de les honorer*** ».⁸³

Nous constatons que la Cour a suivi l'argumentation de l'avocat général qui énonce que la conformité de la décision CPT aux articles 7, 8 et 47 de la charte dépend « *du point de savoir s'il existe des **mécanismes suffisamment solides permettant d'assurer que les transferts fondés sur les clauses contractuelles types soient suspendus ou interdits en cas de violation de ces clauses ou d'impossibilité de les honorer*** ».⁸⁴

La Cour ajoute que le responsable de traitement ou le sous-traitant a l'*obligation de suspendre et/ou de résilier le contrat* lorsque l'importateur de données situé dans le pays tiers concerné « *n'est pas, ou n'est plus, en mesure de respecter les clauses types de protection des données* », et ce en appli-

cation des exigences résultant de l'article 46, 1. et 2., sous c), du RGPD, lu à la lumière des articles 7 et 8 de la charte. « *A défaut, le responsable du traitement méconnaîtrait les exigences lui incombant au titre de la clause 4, sous a), de l'annexe de la décision CPT interprétée à la lumière des dispositions du RGPD et de la charte.* »⁸⁵

La Cour conclut que « *le responsable du traitement établi dans l'Union et le destinataire du transfert de données [...] sont tenus de vérifier, au préalable, le respect, dans le pays tiers concerné, du niveau de protection requis par le droit de l'Union. Le destinataire de ce transfert est, le cas échéant, [...] dans l'obligation d'informer le responsable du traitement de son éventuelle **incapacité de se conformer à ces clauses**, à charge alors pour ce dernier de **suspendre le transfert de données et/ou de résilier le contrat*** ».⁸⁶

Pour toutes ces raisons, la Cour considère que la *décision CPT prévoit des mécanismes effectifs* permettant, en pratique, d'assurer que des transferts reposant sur le fondement des clauses contractuelles types soient suspendus ou interdits lorsque le destinataire du transfert ne respecte pas ces clauses ou se trouve dans l'incapacité de les honorer et que le niveau de protection substantiellement équivalent ne peut pas être assuré par d'autres moyens.⁸⁷ La Cour considère dès lors que la *décision CPT est valide*.⁸⁸

4.2.5. La décision BPD est invalide car les ingérences des agences de renseignement américaines dans le cadre de leurs programmes de surveillance ne se limitent pas à ce qui est strictement nécessaire (non-respect du principe de proportionnalité du RGPD) et que les personnes concernées n'ont pas de voies de recours juridictionnel effectives contre ces autorités américaines (questions 4, 5, 9 et 10)

La Haute Cour d'Irlande s'interroge, en substance, sur le fait de savoir si et dans quelle mesure une Autorité de contrôle est liée par les constatations reprises dans la décision BPD selon lesquelles les Etats-Unis assurent un niveau de protection adéquat. Elle demande, en substance, si, compte tenu de ses propres constatations relatives au droit et pratiques des Etats-Unis, de tels transferts basés sur le fondement des clauses contractuelles types violent les droits garantis aux

^{80.} § 135 de la décision *Schrems 2*.

^{81.} § 126 des conclusions de l'avocat général du 19 décembre 2019 dans l'affaire *Schrems 2*, www.curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=30039, consulté le 20 novembre 2020.

^{82.} § 136 de la décision *Schrems 2*.

^{83.} § 137 de la décision *Schrems 2*.

^{84.} § 127 des conclusions de l'avocat général du 19 décembre 2019 dans l'affaire *Schrems 2*, www.curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=30039, consulté le 20 novembre 2020.

^{85.} § 140 de la décision *Schrems 2*.

^{86.} § 142 de la décision *Schrems 2*.

^{87.} § 148 de la décision *Schrems 2*.

^{88.} § 149 de la décision *Schrems 2*.

articles 7, 8 et 47 de la charte et interroge la Cour, en particulier, sur le point de savoir si la mise en place du médiateur mentionné dans l'annexe III de la décision BPD est compatible avec cet article 47 de la charte.⁸⁹

En premier lieu, la Cour considère que *les Autorités de contrôle sont en principe tenues par les constatations reprises par la Commission dans la décision BPD* lesquelles confirment que les Etats-Unis offrent un niveau de protection adéquat (« caractère contraignant »). Partant, elles ne peuvent suspendre ou interdire un transfert de données de l'EEE vers les Etats-Unis aussi longtemps que la Cour n'a pas déclaré ladite décision invalide.⁹⁰ Néanmoins, la Cour considère qu'elles doivent examiner, en toute indépendance la situation lorsqu'elles sont saisies d'une réclamation qui remet en cause la validité d'une telle décision et ce, en application de l'article 77 du RGPD. La Cour ajoute qu'elles doivent introduire « un recours devant les juridictions nationales » lorsqu'elles estiment le bien-fondé de la réclamation afin de permettre à cette juridiction d'introduire une procédure de renvoi préjudiciel pour permettre à la Cour de se positionner sur la question de la validité de cette décision.⁹¹ A cet égard, la Cour fait référence à la décision *Schrems I*.⁹² Nous observons que ceci est également soutenu par l'avocat général et que ceci a bien été respecté par le commissaire dans le cadre de cette deuxième procédure.⁹³

Concernant la *décision BPD*, la Cour rappelle que, « **la Commission a constaté, [...], que 'les Etats-Unis assurent un niveau adéquat de protection [...], et estimé, [...], que [...] toute ingérence des autorités publiques américaines dans l'exercice des droits fondamentaux [...] pour les besoins de la sécurité nationale, [...] et, partant, les restrictions imposées aux organisations autocertifiées en ce qui concerne leur respect des principes seront limitées à ce qui est strictement nécessaire pour atteindre l'objectif légitime visé et qu'il**

existe une protection juridictionnelle effective contre des ingérences de cette nature'. »⁹⁴ « [...] **L'ingérence doit prévoir des règles claires et précises** régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes [...] disposent de **garanties suffisantes** permettant de **protéger efficacement** leurs données [...] contre les risques d'abus. »⁹⁵

Or, la Cour constate que « **l'article 702 du FISA ne fait ressortir d'aucune manière l'existence de limitations à l'habilitation qu'il comporte pour la mise en œuvre des programmes de surveillance [...], pas plus que l'existence de garanties pour des personnes non américaines potentiellement visées par ces programmes** ».⁹⁶ « [...] le gouvernement américain a admis, [...] que **la PPD-28 ne confère pas aux personnes concernées des droits opposables aux autorités américaines devant les tribunaux.** »⁹⁷ La Cour constate que ceci est également applicable aux programmes de surveillance fondés sur l'E.O. 12333.⁹⁸ Enfin, la Cour constate que la PPD-28 permet de collecter des données « en vrac » dans le cadre de ces programmes de surveillance.⁹⁹ « [...] le **mécanisme de médiation [...] ne fournit pas de voie de recours devant un organe qui offre aux personnes [...] des garanties substantiellement équivalentes à celles requises à l'article 47 de la charte.** »¹⁰⁰

Partant, la Cour estime que la Commission en constatant le niveau de protection adéquat des Etats-Unis a méconnu les exigences résultant de l'article 45, 1., du RGPD, lu à la lumière des articles 7, 8 et 47 de la charte.¹⁰¹ Eu égard à l'ensemble des considérations qui précèdent, la Cour conclut que la **décision BPD** est incompatible avec ces articles, et qu'elle est de ce fait invalide.¹⁰² La Cour précise enfin que l'annulation de cette décision ne crée pas de vide juridique puisque l'article 46 du RGPD permet d'utiliser d'autres instruments de transferts.¹⁰³

^{89.} § 150 de la décision *Schrems 2*.

^{90.} § 156 de la décision *Schrems 2*.

^{91.} § 157-158 de la décision *Schrems 2*.

^{92.} « Voir par analogie, en ce qui concerne l'art. 25, paragraphe 6, et l'art. 28, paragraphe 4, de la directive 95/46, arrêt du 6 octobre 2015, *Schrems*, C362/14, EU:C:2015:650, point 59 », § 158 de la décision *Schrems 2*.

^{93.} § 175 des conclusions de l'avocat général du 19 décembre 2019 dans l'affaire *Schrems 2*, www.curia.europa.eu/juris/document/document.jsf?text=&docid=221826&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1&cid=30039, consulté le 20 novembre 2020.

^{94.} § 167 de la décision *Schrems 2*.

^{95.} § 176 de la décision *Schrems 2*.

^{96.} § 180 de la décision *Schrems 2*.

^{97.} § 181 de la décision *Schrems 2*.

^{98.} § 182 de la décision *Schrems 2*.

^{99.} § 183 de la décision *Schrems 2*.

^{100.} § 197 de la décision *Schrems 2*.

^{101.} § 198 de la décision *Schrems 2*.

^{102.} § 201 de la décision *Schrems 2*. Nous précisons, à des fins de clarification, que la Cour invalide la décision d'adéquation de la Commission et non le mécanisme « Privacy Shield » lui-même. Ce qui veut dire que d'autres pays en dehors de l'EU pourraient encore se fonder sur ce mécanisme afin de transférer des données personnelles vers les Etats-Unis.

^{103.} § 202 de la décision *Schrems 2*.

5. RÉACTIONS DES AUTORITÉS DE CONTRÔLE, DU COMITÉ ET DU MARCHÉ INTERNATIONAL À LA SUITE DE LA DÉCISION « *SCHREMS 2* »

5.1. Premières réactions des Autorités de contrôle: prudentes vs. strictes

A la suite de la décision *Schrems 2*, au lendemain du 16 juillet 2020, nous observons sur la base d'un article publié par l'IAPP¹⁰⁴, différentes réactions de la part des Autorités de contrôle. Certaines, plus prudentes, restent silencieuses et annoncent être en train d'analyser les conséquences de cette décision (e.g. Belgique¹⁰⁵, France, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg et Portugal) alors que d'autres adoptent une approche plus précise et/ou plus stricte.¹⁰⁶ Par exemple, l'Autorité de contrôle de Berlin déclare que les données ne peuvent plus être transférées vers les États-Unis pour le moment car ils n'offrent pas un niveau de protection des données adéquat.¹⁰⁷

Nous observons, par ailleurs, sur la base d'un autre article publié par l'IAPP¹⁰⁸ que l'Autorité de contrôle de Baden-Wurtemberg, située en Allemagne, adopte des lignes directrices obligatoires à la suite de la décision *Schrems 2*. A cet égard, elle considère que les clauses contractuelles types sont toujours valides et peuvent encore être utilisées comme mécanisme de transfert de données vers un pays tiers qui ne bénéficie pas de décision d'adéquation. En revanche, l'autorité précise qu'il a été clarifié par la Cour que le pays tiers doit offrir un niveau de protection des données équivalent à celui garanti par l'Union. Dans ses lignes directrices, elle fournit dès lors une liste de points d'action que les entreprises devraient suivre afin d'assurer leur conformité avec la décision *Schrems 2*. Concernant l'accès des données par les autorités publiques ne respectant pas le principe de proportionna-

lité, et en particulier l'accès par les services américains, l'Autorité de contrôle de Baden-Wurtemberg impose aux exportateurs de données vers les U.S. d'adopter deux mesures complémentaires de protection. D'une part, l'encryptage dont seul l'exportateur a la clé et dont le système ne peut être contourné par les services américains. D'autre part, l'anonymisation ou pseudonymisation dont seul l'exportateur de données peut re-identifier les données.¹⁰⁹

5.2. Déclaration du Comité selon laquelle il déclare être en train d'analyser la décision *Schrems 2* afin de proposer des exemples concrets de « mesures de protection complémentaires » aux clauses contractuelles types (si nécessaire) afin d'offrir un « niveau de protection adéquat » tel que requis par l'Union & adoption d'un document clé « foire aux questions » (« FAQ ») dans lequel il clarifie certains points ayant fait l'objet de discussions à la suite de la décision *Schrems 2*

Le 17 juillet 2020, le Comité déclare que les organisations concernées par ces transferts doivent évaluer la situation « au cas par cas » et doivent si nécessaire, adopter des « mesures de protection complémentaires » notamment aux clauses contractuelles types. Ces mesures n'ayant pas été définies ou spécifiées par la Cour ni par le RGPD, le Comité annonce proposer rapidement des exemples concrets de mesures.¹¹⁰

¹⁰⁴. IAPP, « Using SCCs post-*Schrems II*: Guidance from DPAs », 17 juillet 2020, www.iapp.org/news/a/using-sccs-post-schrems-ii-guidance-from-dpas/, consulté le 25 novembre 2020.

¹⁰⁵. AUTORITÉ DE PROTECTION DES DONNÉES (APD), « Invalidation de la décision relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-Etats-Unis », 31 août 2020, www.autoriteprotectiondonnees.be/professionnel/actualites/2020/08/31/invalidation-de-la-decision-relative-a-l-adequation-de-la-protection-assuree-par-le-bbbouclier-de-protection-des-donnees-ue-etats-uniseb, consulté le 25 novembre 2020.

¹⁰⁶. IAPP, « Using SCCs post-*Schrems II*: Guidance from DPAs », 17 juillet 2020, www.iapp.org/news/a/using-sccs-post-schrems-ii-guidance-from-dpas/, consulté le 25 novembre 2020.

¹⁰⁷. IAPP, « Using SCCs post-*Schrems II*: Guidance from DPAs », 17 juillet 2020, www.iapp.org/news/a/using-sccs-post-schrems-ii-guidance-from-dpas/, consulté le 25 novembre 2020.

¹⁰⁸. IAPP, « Post-*Schrems II*: Understanding Baden-Württemberg's updated guidance on international data transfers », 24 septembre 2020, www.iapp.org/news/a/post-schrems-ii-understanding-baden-wuerttembergs-updated-guidance-on-international-data-transfers/, consulté le 27 novembre 2020.

¹⁰⁹. « Where public authorities disproportionately intervene with the transferred personal data, additional safeguards need to be taken by the EU data exporter, in agreement with the data importer, for the level of protection in the third country to be considered adequate for the transfer. After the CJEU's assessment of the U.S. in *Schrems II*, the following two additional safeguards need to be mandatorily taken for transfers to the U.S.: encryption for which 'only the data exporter has the key' and 'cannot be broken by U.S. [intelligence] services'; and anonymization or pseudonymization where 'only the data exporter can re-identify the data'. » IAPP, « Post-*Schrems II*: Understanding Baden-Württemberg's updated guidance on international data transfers », 24 septembre 2020, www.iapp.org/news/a/post-schrems-ii-understanding-baden-wuerttembergs-updated-guidance-on-international-data-transfers/, consulté le 27 novembre 2020.

¹¹⁰. ONE TRUST DATA GUIDANCE, « Europe: Data protection authorities react to *Schrems II* judgment [updated 2 October 2020] », www.dataguidance.com/news/europe-data-protection-authorities-react-schrems-ii, 17 juillet 2020, consulté le 25 novembre 2020; IAPP, « Using SCCs post-*Schrems II*: Guidance from DPAs », 17 juillet 2020, www.iapp.org/news/a/using-sccs-post-schrems-ii-guidance-from-dpas/, consulté le 25 novembre 2020; EDPB, « Statement on the Court of Justice of the European Union Judgment in Case C-311/18 – Data Protection Commissioner v. Facebook Ireland and Maximilian Schrems », 17 juillet 2020, www.edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_fr, consulté le 20 novembre 2020. EDPB, « Foire aux questions sur l'arrêt rendu par la Cour de justice de l'Union européenne dans l'affaire C-311/18 – Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems », 24 juillet 2020, www.edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_fr, consulté le 20 novembre 2020.

Le 23 juillet 2020, le Comité adopte un document clé « foire aux questions » (« FAQ ») dans lequel il clarifie certains points ayant fait l'objet de discussions à la suite de la décision *Schrems 2*. Il précise, en résumé, que *le seuil du « niveau de protection adéquat » établi par la Cour s'applique à toutes les garanties appropriées reprises à l'article 46 du RGPD*, que le droit des Etats-Unis (e.g. section 702 FISA et E.O. 12333) s'applique à tous ces transferts de données effectués vers les Etats-Unis indépendamment de l'instrument de transfert appliqué, qu'il n'y a *pas de période de grâce concernant l'annulation de la décision BPT*, que si les organisations concernées arrivent à la conclusion que leurs garanties appropriées ne permettent *pas d'assurer un niveau de protection adéquat mais décide tout de même de continuer leurs transferts, elles doivent en informer l'Autorité de contrôle compétente*, que les transferts vers les Etats-Unis sur le fondement de la décision *BPT* sont « illégaux » et que même le fait de simplement autoriser un pays tiers à accéder aux données, par exemple, à des fins administratives ou à des fins de stockage ou de maintenance équivaut à un transfert.¹¹¹

5.3. Premières réactions des organisations: « en route vers le changement » vs. « paralysie »

Quant aux organisations concernées, nous observons sur la base de notre expérience que la plupart des grandes entreprises entament la mise en œuvre de nouvelles mesures (e.g. mise en place d'addendum aux clauses contractuelles types, relocalisation du stockage de leurs données, etc.) alors que les moyennes et petites entreprises se retrouvent « paralysées » par la décision *Schrems 2* ne sachant pas quels types de « mesures de protection complémentaires » mettre en place. Celles-ci préfèrent dès lors attendre la publication de lignes directrices et/ou recommandations dont celles annoncées par le Comité.

5.4. Projet de recommandations 01/2020 du Comité proposant des « mesures de protection complémentaires » aux clauses contractuelles types, projet de nouvelles clauses types et recommandations 02/2020 sur les garanties européennes essentielles aux mesures de surveillance

Le 10 novembre 2020, le Comité, comme annoncé, adopte un projet de recommandations 01/2020 concernant les « mesures de protection complémentaires » permettant d'assurer la conformité de tels transferts avec le « niveau de protection adéquat » requis par l'Union. Ce projet fait actuellement l'objet d'une consultation du public se terminant le 21 décembre 2020.¹¹² En outre, le Comité adopte, à la même date, les recommandations 02/2020 sur les garanties européennes essentielles aux mesures de surveillance.¹¹³

Le 12 novembre 2020, la Commission publie un projet de décision reprenant en annexe un nouvel ensemble de clauses contractuelles types afin de remplacer les précédentes reprises dans la décision *CPT*, de les moderniser et de les mettre à jour en ligne avec le RGPD et la décision *Schrems 2*. Ce projet fait également l'objet d'une consultation du public se terminant le 10 décembre 2020. Le projet précise qu'à partir de l'entrée en vigueur de ladite décision, *les organisations concernées par ces transferts seront encore autorisées à utiliser les clauses types de la décision CPT pendant une période d'1 an pour autant que les organisations, si nécessaire, et sur la base de leurs propres évaluations et conclusions, mettent en œuvre les « mesures de protection complémentaires » telles qu'imposées par la décision Schrems 2*.¹¹⁴

Nous sommes dès lors impatients de connaître les résultats des consultations du public et les décisions finales du Comité et de la Commission afin de bien comprendre l'impact opérationnel de la décision *Schrems 2* pour les entreprises. Il s'agira de savoir précisément quelles clauses contractuelles types et quelles mesures complémentaires de protection (si nécessaire) l'exportateur et l'importateur de données

¹¹¹ EDPB, « Foire aux questions sur l'arrêt rendu par la Cour de justice de l'Union européenne dans l'affaire C-311/18 – Data Protection Commissioner contre Facebook Ireland Ltd et Maximilian Schrems », 24 juillet 2020, www.edpb.europa.eu/our-work-tools/our-documents/ohrajn/frequently-asked-questions-judgment-court-justice-european-union_fr, consulté le 20 novembre 2020.

¹¹² EDPB, « Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data », 10 novembre 2020, www.edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en, consulté le 20 novembre 2020.

¹¹³ EDPB, « Recommendations 02/2020 on the European Essential Guarantees for surveillance measures », 10 novembre 2020, www.edpb.europa.eu/our-work-tools/our-documents/recommendations/edpb-recommendations-022020-european-essential_en, consulté le 25 novembre 2020. Par ailleurs, le Comité a également adopté des lignes directrices pour les institutions de l'Union, « Strate.g.y for Union institutions, offices, bodies and agencies to comply with the 'Schrems II' Ruling », 29 octobre 2020, www.edps.europa.eu/sites/edp/files/publication/2020-10-29_edps_strate.g.y_schremsii_en_0.pdf, consulté le 25 novembre 2020.

¹¹⁴ COMMISSION EUROPEENNE, « Protection des données – Clauses contractuelles types pour les transferts de données à caractère personnel à des pays tiers (acte d'exécution) », www.ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries?mkt_tok=eyJpIjoiTURVNU5XSTFaREZsTkdbClIsInQiOiJlYWIsTnpIRWxKS1VBUENtXNCS1ZoQzQrcjVQdE13TGNGcDNZV0xYS1d2dURaNRiRGEzYUZWGhZUWpcL2drVHFjRUVaZjJrdlwbllST3Y3YVZtOUZyMjRjRGVkbNHNnNkKzaDNHk3hjRvJwc1ZjZXFUT3paXC9IM0szS3IWSklpMiJ9, consulté le 25 novembre 2020.

devront mettre en œuvre afin de (continuer à) transférer légalement des données de l'EEE vers les Etats-Unis ou tout autre pays tiers ne bénéficiant pas d'une décision d'adéquation.

5.5. Déclaration des Etats-Unis en réponse à la décision *Schrems 2*

Enfin, concernant la réaction des Etats-Unis, les autorités étatiques publient en septembre 2020 une déclaration en réponse à la décision *Schrems 2* dans laquelle ils contredisent diverses considérations de la Cour concernant les garanties offertes par le droit et les pratiques des Etats-Unis en matière de protection des données.¹¹⁵

CONCLUSION

Eu égard à toutes les considérations qui précèdent, nous observons que le « niveau de protection adéquat » des données et la manière de le respecter a fait couler beaucoup d'encre. En particulier, lorsque des données quittent le territoire européen vers les Etats-Unis.

A la suite de l'intervention de M. Schrems, nous bénéficions à l'heure actuelle de 2 décisions majeures de la Cour, la décision *Schrems 1* de 2015 et la décision *Schrems 2* de 2020, nous permettant de mieux comprendre la manière dont il faut interpréter les articles 44, 45 et 46 du RGPD concernant le transfert de données de l'EEE vers un pays tiers, lus à la lumière des articles 7, 8 et 47 de la charte.

En pratique, il ressort de la décision *Schrems 2*, qu'un responsable du traitement ou un sous-traitant de données lorsqu'il souhaite transférer des données de l'EEE vers un pays tiers non reconnu par une décision d'adéquation, doit au préalable, vérifier, que le destinataire de ces données est capable d'offrir un « niveau de protection » des données « substantiellement équivalent » à celui garanti par l'Union.

Il s'agit d'examiner, au cas par cas, sur la base d'informations publiques, si la législation interne, les accords internationaux et les pratiques du droit du pays tiers concerné par ce transfert permettent « effectivement » au destinataire d'offrir aux personnes concernées un « niveau de protection adéquat » tel que requis par l'Union. En application des décisions *Schrems 1* et *Schrems 2*, il faut vérifier, entre autres, si le pays tiers offre des garanties suffisantes aux personnes concernées en cas d'ingérences dans leurs droits fondamentaux par les autorités publiques (e.g. respect du principe de

proportionnalité), des voies de recours effectives, un tribunal indépendant, des dispositions légales claires et précises concernant les limitations aux droits fondamentaux des personnes, etc.

Si un responsable du traitement ou un sous-traitant de données constate une insuffisance de protection dans le cadre de ce transfert, il doit ajouter des « mesures complémentaires de protection » appropriées permettant de combler cette insuffisance et ce, peu importe l'instrument de transfert ou les garanties appropriées utilisées.

S'il constate que, même après avoir mis en place ces « mesures complémentaires de protection », le destinataire est toujours dans l'incapacité d'honorer ce « niveau de protection » requis par l'Union ou n'est plus capable de le respecter, il doit suspendre ou mettre fin à ce transfert. A défaut, les Autorités de contrôle doivent le faire.

En ce qui concerne le type de « mesures complémentaires de protection » à mettre en place, le responsable du traitement ou le sous-traitant de données peut s'inspirer des exemples concrets proposés par le Comité dans son projet de recommandation 01/2020. Il peut également s'inspirer du nouvel ensemble de clauses contractuelles types repris dans le projet de décision de la Commission.

S'il décide tout de même de transférer des données vers le pays tiers n'offrant pas un « niveau de protection adéquat » malgré la mise en place de « mesures complémentaires de protection », il doit en informer l'Autorité de contrôle compétente.

¹¹⁵. US AUTHORITIES, « Information on U.S. Privacy Safe.g.uards Relevant to SCCs and Other EU Le.g.al Bases for EU-U.S. Data Transfers after Schrems II », *White Paper*, septembre 2020, www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF, consulté le 25 novembre 2020.