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

Les transferts de données à caractère personnel entre l'Union européenne et les Etats-Unis: une valse à mille temps[1]?

Maïka Bernaerts[2]

RÉSUMÉ

La réglementation relative aux transferts de données à caractère personnel depuis le territoire de l'Union européenne vers celui des Etats-Unis est en constante évolution et vient de faire l'objet d'une nouvelle décision de la Commission européenne suite à l'annulation de la décision préexistante par la Cour de justice de l'Union européenne. La présente contribution a pour objet de décrire et d'analyser le chemin parcouru et l'impact que le nouveau règlement relatif à la protection des données à caractère personnel pourrait avoir sur ce type de transferts.

SAMENVATTING

De regelgeving betreffende de doorgifte van persoonsgegevens vanaf het grondgebied van de Europese Unie naar dat van de Verenigde Staten evolueert voortdurend en maakt het voorwerp uit van een nieuw besluit van de Europese Commissie, uitgevaardigd na de nietigverklaring van het voorgaande besluit door het Hof van Justitie van de Europese Unie. Deze bijdrage beschrijft en analyseert de afgelegde weg en de invloed die de nieuwe verordening betreffende de bescherming van persoonsgegevens op dergelijke doorgiften kan hebben.

1. J. BREL, *La valse à mille temps*, 1959.
2. Avocate chez Liedekerke Wolters Waelbroeck Kirkpatrick et assistante chargée d'exercices à la Faculté de Droit et de Criminologie de l'Université libre de Bruxelles. L'auteur remercie Andrée Puttemans, Arnaud Nuyts et Thierry Tilquin pour leurs conseils précieux. Les opinions exprimées sont celles de l'auteur uniquement.

INTRODUCTION

« *Le partage et la communication internationale de données sont devenus la règle et non l'exception.* »[3].

1. Cette citation, vieille de 15 ans, est plus que jamais d'actualité[4]. Les transferts de données sont légion et des données personnelles transitent depuis le territoire de l'Union européenne vers celui des Etats-Unis de manière quotidienne. De tels transferts sont légalement encadrés mais cet encadrement a rarement été aussi branlant. De la directive (CE) n° 95/46[5], qui introduit le droit à la protection des données personnelles dans l'arsenal juridique européen, au règlement qui est voué à la remplacer[6], en passant par les décisions dites « *Safe Harbor* »[7] et « *Privacy Shield* »[8], les transferts européano-américains ont une existence pour le moins troublée.

2. La réglementation relative aux données à caractère personnel a en effet été amendée à diverses reprises, notamment suite à l'affaire *Schrems*[9] qui nous intéresse tout particulièrement. Pour les expliquer, nous partirons du passé, de la directive et de la décision « *Safe Harbor* », avant de détailler l'affaire *Schrems*, qui sonne le glas du *Safe Harbor*, le rôle majeur de la Cour de justice de l'Union européenne et le nouveau cadre législatif européen (que ce soit le règlement ou le nouvel accord européano-américain[10]) qui façonnera le futur en la matière, et ce dans le but d'examiner sa compatibilité avec les critiques de la Cour de justice. Comme nous le verrons, le nouvel accord ne fait pas l'unanimité[11].

3. Le présent article ne vise que le droit européen; les données personnelles telles que définies par la directive et par le règlement; et les relations commerciales entre l'Union européenne et les Etats-Unis dans ce cadre, c'est-à-dire les transferts de données à des fins commerciales et non à des fins judiciaires, pénales ou administratives. Nous ne pouvons cependant ignorer les intérêts des autorités publiques tant celles-ci sont liées au sujet qui nous occupe (les surveillances exercées par les autorités américaines sont notamment au cœur de l'affaire *Schrems*). Trois acteurs sont ainsi concernés: les individus, les entreprises et les autorités étatiques.

4. Seul le droit européen sera analysé et ce pour plusieurs raisons: d'une part, la marge d'appréciation octroyée aux Etats membres par la directive est assez restreinte[12] puisque celle-ci vise à une harmonisation en principe complète[13] et, d'autre part, l'Union européenne a adopté un nouveau règlement en la matière, qui, à terme, remplacera la directive et

3. B. HAVELANGE et A.-C. LACOSTE, « Les flux transfrontaliers de données à caractère personnel en droit européen », *J.D.E.,* 2001, p. 241.
4. En témoignent les chiffres sans cesse grandissants du marché des données: voir à ce sujet les recherches du BOSTON CONSULTING GROUP (« The value of our Digital Identity », novembre 2012) et de MCKINSEY (« Big data: The next frontier for innovation, competition, and productivity », 2011) citées par la Commission européenne en ces termes: « The estimated value of EU citizens' data was 315bn in 2011 and has the potential to grow to nearly 1tn annually by 2020. The market for the analysis of large sets of data is growing by 40% per year worldwide. »: COMMISSION EUROPEENNE, « Rebuilding Trust in EU-US Data Flows », *Communication COM(2013) 846 final*, 27 novembre 2013, p. 3.
5. Directive (CE) n° 95/46 du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, *J.O.C.E.*, L. 281, 23 novembre 1995, p. 31 et s. Ci-après la « directive ».
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, *J.O.U.E.*, L. 119, 4 mai 2016, p. 1 et s. Ci-après le « règlement ».
7. Décision (CE) n° 2000/520 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.C.E.*, L. 215, 25 août 2000, p. 7 et s. Ci-après référencée en tant que « décision (CE) n° 2000/520 de la Commission ». Nous utiliserons l'orthographe « *Safe Harbor* » plutôt que celle, parfois utilisée, de « *Safe Harbour* ». En effet, puisqu'il s'agit d'un accord impliquant les Etats-Unis, nous avons préféré garder l'orthographe américaine.
8. Décision d'exécution (UE) n° 2016/1250 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.U.E.*, L. 207, 1er août 2016, p. 1 et s.
9. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650.
10. Décision d'exécution (UE) n° 2016/1250 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.U.E.*, L. 207, 1er août 2016, p. 1 et s.
11. Voir notamment GROUPE DE L'ARTICLE 29, « Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision », *WP 238*, 13 avril 2016 (le Groupe de l'Article 29, appelé ci-après « G29 » ou « groupe 29 », étant un groupement européen de protection des données à caractère personnel et de la vie privée, à caractère consultatif et indépendant, créé par l'article 29 de la directive et composé notamment de représentants des autorités nationales de protection des données à caractère personnel: article 29 de la directive; devient le « comité européen de la protection des données », article 68 du règlement); A. JENNOTE, « Pourquoi le Privacy shield est un bouclier bien trop frêle pour la vie privée des Européens », *Le Soir*, 3 mars 2016; « 'Privacy Shield': ne sacrifions pas nos droits sur 'l'autel du pragmatisme'! », *Association européenne pour la défense des Droits de l'Homme*, www.aedh.eu/Privacy-Shield-ne-sacrifions-pas.html (consulté le 10 avril 2016).
12. Certains auteurs soulignent qu'en pratique cependant, les Etats membres ont transposé la directive avec de nombreuses différences entre eux, ce qui explique pourquoi l'Union a décidé de passer d'une directive à un règlement pour éviter cet écueil: N. PURTOVA, « Who decides on the future of data protection? Role of law firms in shaping European data protection regime », *International Review of Law, Computers & Technology*, 2014, p. 210.
13. C.J.C.E., 6 novembre 2003, C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596, point 96; C.J.C.E., 16 décembre 2008, C-524/06, *Heinz Huber / Bundesrepublik Deutschland*, ECLI:EU:C:2008:724, point 51.

fera donc place à une réglementation unique. Dans cette optique, il est peu pertinent d'analyser les quelques différences nationales pouvant exister à l'heure actuelle car celles-ci disparaîtront sous peu[14]. Notre propos se concentrera cependant sur la directive, celle-ci restant en vigueur jusqu'en 2018[15].

5. L'application de cette directive[16] est, dans le cadre de cette contribution, considérée comme acquise, c'est-à-dire que nous prendrons pour acquis d'être face à des données à caractère personnel qui entrent dans le champ d'application de la directive et qui sont traitées d'une manière visée par la directive[17] (et, dans le futur, par le règlement[18]).

6. Les données à caractère personnel y sont définies comme « toute information concernant une personne physique identifiée ou identifiable[19] (personne concernée) »[20]. *A contrario*, les données anonymes[21] et les données concernant les personnes morales[22] ne sont en principe[23] pas protégées et ne seront donc pas examinées. De même, nous n'entrerons pas dans le champ de ce que la directive appelle les « catégories particulières de traitements » pour lesquelles il existe des règles spécifiques[24].

7. La notion de « données à caractère personnel » vise des données aussi diverses qu'une adresse postale[25], un nom[26], un dossier médical, une photographie, une empreinte digitale, etc.[27]. Il peut s'agir de données objectives (le nom d'une personne) mais aussi de données subjectives comme des avis se rapportant à cette personne (« Julien mérite une promotion ») sans que ces données soient nécessairement vraies ou prouvées[28]. Tant les données de la sphère privée que celles qui concernent la sphère professionnelle ou publique sont visées[29].

8. Le spectre des données touchées par cette définition est volontairement large afin de couvrir toute donnée liée à une personne physique[30]. En effet, le but premier de la directive est de protéger la vie privée des individus[31] et elle doit donc être interprétée en ce sens[32], ce qui aura son importance, comme nous le verrons, dans la jurisprudence de la Cour de justice de l'Union qui se pose comme gardienne des droits fondamentaux que sont la protection de la vie privée et la

14. COMMISSION EUROPÉENNE, « Reform of EU data protection rules », www.ec.europa.eu/justice/data-protection/reform/index_en.htm, dernière mise à jour le 21 avril 2016 (consulté le 22 avril 2016).
15. *Ibid.* Les articles correspondants du règlement seront cependant mentionnés dès que nous ferons référence à des articles de la directive.
16. Cette directive complète notamment les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne, l'article 16 du traité sur le fonctionnement de l'Union européenne, l'article 36 du traité de l'Union européenne, l'article 8 de la convention européenne des droits de l'homme ainsi que la convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *STCE n° 108*, Strasbourg, 28 janvier 1981. Le champ d'application territorial de ce dernier instrument est néanmoins plus large que celui de la directive qui ne touche que les Etats membres de l'Espace économique européen alors que la convention n° 108 est ouverte aux membres du Conseil de l'Europe mais également aux Etats non membres. Ainsi, l'Uruguay y a par exemple adhéré. Voir liste sur le site du Conseil de l'Europe: www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=FtZTmVP8 (consulté le 26 janvier 2016); C.J.C.E., 20 mai 2003, C-465/00, C-138/01 et C-139/01, *Rechnungshof / Österreichischer Rundfunk e.a.*, *Christa Neukomm et Joseph Lauermann / Österreichischer Rundfunk*, ECLI:EU:C:2003:294, points 70 et s.; J.-M. VAN GYSEGHEM, C. DE TERWANGNE, J. HERVEG et C. GAYREL, « La protection des données à caractère personnel en droit européen », *J.E.D.H.*, 2014/1, p. 55 et s.; M. ELIANTONIO, F. GALLI et M. SCHAPER, « Guest Editors' Introduction – A Balanced Data Protection in the EU », *M.J.*, 2016/3, p. 393.
17. Art. 3 de la directive.
18. Art. 2 du règlement.
19. Il y a lieu d'entendre par « identifiable » « une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »: art. 2, a), de la directive (définition similaire prévue à l'art. 4, 1., du règlement).
20. Art. 2, a), de la directive (définition similaire prévue à l'art. 4, 1., du règlement).
21. Définies comme les données qui concernent une personne physique qui ne peut pas être identifiée: G29, « Avis 4/2007 sur le concept de données à caractère personnel », *WP 136*, 20 juin 2007, p. 21.
22. C.J.U.E., 9 novembre 2010, C-92/09 et C-93/09, *Volker und Markus Schecke GbR et Hartmut Eifert / Land Hessen*, ECLI:EU:C:2010:662, point 52; T. LÉONARD et Y. POULLET, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999-2000, n° 5928, § 9; A. DEBET, J. MASSOT et N. METALLINOS, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Issy-les-Moulineaux, Lextenso éditions, 2015, p. 37.
23. Certains Etats membres ont néanmoins décidé d'étendre, dans leur droit national, le champ d'application de la protection accordée par certains articles de la directive aux personnes morales: G29, « Avis 4/2007 sur le concept de données à caractère personnel », *WP 136*, 20 juin 2007, p. 24.
24. Art. 8 et 9 de la directive (art. 9, 10, 85 et 87 du règlement).
25. C.J.C.E., 7 mai 2009, C-553/07, *College van burgemeester en wethouders van Rotterdam / M. E. E. Rijkeboer*, ECLI:EU:C:2009:293, point 42.
26. *Ibid.*; C.J.U.E., 29 juin 2010, C-28/08 P, *Commission européenne / The Bavarian Lager Co. Ltd.*, ECLI:EU:C:2010:378, point 68.
27. G29, « Avis 4/2007 sur le concept de données à caractère personnel », *WP 136*, 20 juin 2007, p. 7, 8, 9 et 13; K. ROSIER, « Gestion et protection des données à caractère personnel dans la relation de travail », *Le droit du travail à l'ère du numérique*, Limal, Anthemis, 2011, p. 66 et s.
28. G29, « Avis 4/2007 sur le concept de données à caractère personnel », *WP 136*, 20 juin 2007, p. 6.
29. *Ibid.*, p. 6 et s.; K. ROSIER, « Gestion et protection des données à caractère personnel dans la relation de travail », *o.c.*, p. 62 et 67; T. LÉONARD et Y. POULLET, *o.c.*, § 8.
30. COMMISSION DES COMMUNAUTES EUROPEENNES, « Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data », *SYN 287, COM (90) 314 final* , 13 septembre 1990, p. 19.
31. Art. 1er de la directive (art. 1er du règlement).
32. G29, « Avis 4/2007 sur le concept de données à caractère personnel », *WP 136*, 20 juin 2007, p. 4.

protection des données à caractère personnel[33], trop souvent convoitées par les entreprises comme le nouvel Eldorado.

9. Néanmoins, pour que la directive s'applique, il ne faut pas seulement être en présence de ce type de données, il faut aussi que ces données soient traitées[34]. L'article 2, b), de la directive définit le traitement comme « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».

10. Nous pouvons très vite nous apercevoir que cette définition est aussi large que celle des données à caractère personnel et que toute opération est en principe visée dès qu'elle touche à ces données. La Cour suit cette interprétation extensive et estime généralement qu'il y a bien un traitement sans s'attarder sur cette qualification[35]. Nous n'examinerons donc pas davantage cette notion puisqu'il est clair que le transfert de données vers un pays tiers, au cœur de notre étude, est bien un traitement tel que défini par l'article 2, b), ce que la Cour a confirmé explicitement dans l'arrêt *Schrems*[36].

11. Les transferts de données à caractère personnel protégées par la directive depuis le territoire de l'Union vers un pays tiers sont non seulement visés par l'article 2, b), de la directive mais ils sont aussi abordés de manière spécifique par celle-ci: la directive les distingue des transferts de données à caractère personnel vers des destinataires établis dans un Etat membre de l'Union européenne (et de l'Espace économique européen plus généralement[37])[38]. Ce dernier type de traitement est libre tant qu'il est légal aux yeux de la loi nationale applicable transposant la directive puisque la protection des données est équivalente au sein de chaque Etat membre suite à cette transposition (« libre circulation des flux intracommunautaires »)[39].

12. Les transferts de données vers les pays tiers suivent un autre parcours et celui-ci est tout à fait particulier pour les Etats-Unis puisque la Commission européenne, suite à des négociations avec les Etats-Unis au sujet des données à caractère personnel, a pris, en 2000, une décision dénommée « *Safe Harbor* », pour permettre des transferts de données à des fins commerciales entre le territoire de l'Union européenne et certaines entreprises situées aux Etats-Unis[40].

13. Nous examinerons donc tout d'abord la réglementation prévue par la directive et cette décision *Safe Harbor* avant de passer à son invalidation par l'arrêt *Schrems* et ses conséquences, dont les négociations autour d'un nouvel accord et son adoption pour le moins rapide, et le tout récent règlement.

SECTION 1. LE PASSÉ EN GUISE DE PROLOGUE

« *Même si les Etats-Unis et l'Union européenne ont comme objectif commun de protéger davantage la vie privée de leurs citoyens, les Etats-Unis préconisent dans ce domaine une approche différente de celle de l'Union européenne.* »[41].

33. Art. 7 et 8 de la charte des droits fondamentaux de l'Union européenne.
34. Art. 3 de la directive (art. 2 du règlement).
35. C.J.C.E., 6 novembre 2003, C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596, point 25 (la Cour y définit tout de même la notion de transfert mais en des termes très larges: « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel »); C.J.C.E., 16 décembre 2008, C-73/07, *Tietosuojavaltuutettu / Satakunnan Markkinapörssi Oy et Satamedia Oy*, ECLI:EU:C:2008:727, points 36 et 37; C.J.U.E., 13 mai 2014, C-131/12, *Google Spain SL et Google Inc. / Agencia Espanola de Proteccion de Datos (AEPD) et Mario Costeja Gonzalez*, ECLI:EU:C:2014:317, points 26 et 27; A. DEBET, J. MASSOT et N. METALLINOS, *o.c.*, p. 112; voir néanmoins J.-M. VAN GYSEGHEM, C. DE TERWANGNE, J. HERVEG et C. GAYREL, « La protection des données à caractère personnel en droit européen », *J.E.D.H.*, 2014/1, p. 82 et 83 pour des exemples de jurisprudence européenne sur la notion de traitement.
36. « L'opération consistant à faire transférer des données à caractère personnel depuis un Etat membre vers un pays tiers constitue, en tant que telle, un traitement de données à caractère personnel au sens de l'article 2, sous b), de la directive 95/46 »: C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 45; voir, dans le même sens, C.J.C.E., 30 mai 2006, C-317/04 et C-318/04, *Parlement européen / Conseil de l'Union européenne*, ECLI:EU:C:2006:346, point 56.
37. Le principe de libre circulation s'applique en effet aussi pour l'Islande, le Lichtenstein et la Norvège (Espace économique européen, ci-après « EEE ») qui ont transposé la directive dans leur ordre juridique interne en application des dispositions imposées par l'accord sur l'EEE: A. DEBET, J. MASSOT et N. METALLINOS, *o.c.*, p. 655.
38. Cette localisation dépend des critères repris à l'article 4 de la directive (art. 3 du règlement): J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010/2, p. 255.
39. C.J.C.E., 16 décembre 2008, C-524/06, *Heinz Huber / Bundesrepublik Deutschland*, ECLI:EU:C:2008:724, point 52; A. DEBET, J. MASSOT et N. METALLINOS, *o.c.*, p. 41, 653 et 654; K. ROSIER, « Gestion et protection des données à caractère personnel dans la relation de travail », *o.c.*, p. 97.
40. Décision (CE) n° 2000/520 de la Commission.
41. Annexe I, décision (CE) n° 2000/520 de la Commission, p. 10.

1.1. Le contexte des transferts européano-américains: les entreprises établies aux Etats-Unis, mieux loties que celles établies en Europe?

14. Le chapitre IV de la directive, visant le transfert de données à caractère personnel vers des pays tiers, se compose d'un principe tempéré par des exceptions. Le principe, énoncé à l'article 25, est simple: « le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si (…) le pays tiers en question assure un niveau de protection adéquat. »[42]. Les exceptions prévues subséquemment permettent, sous certaines conditions, des transferts vers un pays tiers n'assurant pas un niveau de protection adéquat.

15. Une remarque préliminaire s'impose avant d'examiner en détails les règles applicables: il est important de garder à l'esprit que ces règles existent pour éviter que la législation européenne ne soit réduite à néant par le simple transfert des données protégées en dehors du territoire de l'Union. Il fallait en effet imaginer une réglementation permettant d'assurer un niveau de protection équivalent à celui prévu par la directive même lorsque les données concernées sont transférées hors Union[43]; à défaut, il suffirait que toute entreprise traite ces données sur le territoire d'un pays tiers pour échapper à la législation européenne et violer les droits fondamentaux des citoyens européens[44]. Le but des articles 25 et 26 de la directive est ainsi de faciliter les transferts[45] tout en protégeant les données et les droits des citoyens européens, même en dehors de l'Union[46].

1.1.1. L'article 25, 1., de la directive: le niveau de protection adéquat

16. Le critère central est le « niveau de protection adéquat ». Cette notion n'est pas définie dans la directive[47] qui précise simplement que ce caractère adéquat s'apprécie « au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées »[48]. Ces critères sont exemplatifs, d'autres pourraient être pris en considération.

17. De manière générale, un pays tiers est considéré comme offrant un niveau de protection adéquat lorsque les principes majeurs prévus par la directive[49] sont effectivement mis en œuvre dans le droit interne de ce pays tiers[50], sans qu'il soit nécessaire que toutes les règles du pays tiers soient semblables à celles édictées par le législateur européen[51]. Le pays tiers doit assurer un « niveau satisfaisant de respect » de ces principes, apporter soutien et assistance aux personnes concernées dans l'exercice de leurs droits et leur fournir des voies de recours appropriées[52].

18. Pour le G29, auquel se rallie le Parlement européen[53], deux critères fondamentaux doivent finalement être pris en compte: « le contenu des règles applicables et les moyens d'assurer leur application efficace »[54]. Ces éléments sont primordiaux dans l'analyse de la Cour de justice pour déterminer si le pays tiers dispose du niveau de protection adéquat. Si c'est le cas, le transfert peut en principe avoir lieu, pour autant qu'il respecte par ailleurs les autres règles encadrant le droit à la protection des données personnelles dans l'Etat membre de départ[55].

1.1.2. Les autres solutions: comment la Commission européenne a permis les transferts de données vers les Etats-Unis

19. Certains pays tiers, comme les Etats-Unis, ne dispo-

42. Art. 25, 1., de la directive (art. 45, 1., du règlement); J.-P. MOINY, *o.c.*, p. 265.
43. B. HAVELANGE et A.-C. LACOSTE, *o.c.*, p. 241; A. DEBET, J. MASSOT et N. METALLINOS, *o.c.*, p. 648.
44. K. ROSIER, « Gestion et protection des données à caractère personnel dans la relation de travail », *o.c.*, p. 97.
45. Il est en effet inimaginable d'interdire tout transfert ou de les limiter « sans s'isoler de manière intenable »: B. HAVELANGE et A.-C. LACOSTE, *o.c.*, p. 241.
46. A. DEBET, J. MASSOT et N. METALLINOS, *o.c.*, p. 648.
47. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 70.
48. Art. 25, 2., de la directive (art. 45, 2., du règlement).
49. Limitation des transferts à une finalité spécifique, qualité et proportionnalité des données collectées, transparence, sécurité, droit d'accès, de rectification et d'opposition, et restrictions aux transferts ultérieurs vers d'autres pays tiers: G29, « Premières orientations relatives aux transferts de données personnelles vers des pays tiers. Méthodes possibles d'évaluation du critère adéquat de la protection », *WP 4*, 26 juin 1997, p. 6 et 7.
50. AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE, *Manuel de droit européen en matière de protection des données*, 2014, p. 143.
51. PARLEMENT EUROPÉEN, « Résolution du Parlement européen sur le projet de décision de la Commission relative à la pertinence des niveaux de protection fournis par les principes de la sphère de sécurité et les questions souvent posées y afférentes, publiées par le ministère du Commerce des Etats-Unis », *C5-0280/2000 – 2000/2144(C.O.S.)*, 5 juillet 2000; A. DEBET, J. MASSOT et N. METALLINOS, *o.c.*, p. 664.
52. *Ibid.*, p. 7 et 8.
53. PARLEMENT EUROPÉEN, *o.c.*, *C5-0280/2000 – 2000/2144 (C.O.S.)*, 5 juillet 2000.
54. G29, « Premières orientations relatives aux transferts de données personnelles vers des pays tiers. Méthodes possibles d'évaluation du critère adéquat de la protection », *WP 4*, 26 juin 1997, p. 6; G29, « Document de travail. Transfert de données personnelles vers des pays tiers: application des articles 25 et 26 de la directive relative à la protection des données », *WP 12*, 24 juillet 1998, p. 5.
55. Art. 25, 1., de la directive (art. 45, 1., du règlement).

sent pas du niveau de protection des données requis[56]. Ainsi, notamment suite à la déclaration du G29 constatant que, en l'état, les Etats-Unis ne disposaient pas du niveau de protection adéquat requis par la directive[57], c'est en vertu des paragraphes 5 et 6 de l'article 25 que la décision *Safe Harbor* a été adoptée par la Commission européenne[58].

20. En effet, le rôle joué *a posteriori* par la Cour complète et corrige celui joué *a priori* par la Commission puisque celle-ci a la possibilité d'engager des négociations avec un pays tiers en vue de permettre à celui-ci d'être reconnu au sein de l'Union comme assurant un niveau de protection adéquat[59].

21. La Commission et les Etats-Unis ont dès lors négocié pendant 2 ans un cadre légal permettant les transferts, à des fins commerciales, de données protégées par la directive[60]. Au vu des relations commerciales entre ces deux « géants »[61], il semblait en effet peu raisonnable et peu praticable de faire appel, pour chaque transfert, aux dérogations prévues à l'article 26 de la directive.

22. Cet article 26 prévoit, pour les responsables de traitement[62] établis dans des pays tiers ne disposant pas du niveau de protection adéquat, qu'un transfert de données pourra être autorisé sous le couvert d'une des conditions prévues en son point 1.[63] ou « lorsque le responsable de traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants », c'est-à-dire lorsque des clauses contractuelles ou des règles contraignantes d'entreprises prévoyant de telles garanties sont mises en place[64].

23. Ces solutions visent néanmoins des transferts plutôt ponctuels ou entre sociétés liées et non des flux continus de données, ce qui a amené les Etats-Unis à négocier un accord plus global avec l'Union.

24. L'accord intervenu s'est formalisé par l'adoption de la décision *Safe Harbor* en 2000[65]. Celle-ci disposait que, en raison des engagements internationaux pris par les Etats-Unis suite à ces négociations, les « organisations » établies sur le territoire des Etats-Unis qui le désiraient seraient considérées comme disposant du niveau adéquat de protection si elles respectaient les principes relatifs à la protection de la vie privée prévus à l'annexe I de cette décision (ci-après « les principes ») et qu'elles les appliquaient conformément aux orientations fournies par les « questions souvent posées » (*frequently asked questions*, ci-après « les FAQ »), prévues à l'annexe II de la décision[66].

25. Ce système est donc tout à fait particulier puisque la décision *Safe Harbor* ne s'applique pas à tout transfert de données vers les Etats-Unis de manière générale mais s'applique aux « organisations » basées aux Etats-Unis qui, de manière volontaire, s'engagent à en respecter les principes et les FAQ (première condition)[67]. La décision ne concerne donc pas le niveau de protection prévu par la législation américaine de manière générale comme c'est le cas pour d'autres Etats repris sur une liste de pays considérés comme assurant le niveau de protection requis[68].

---

56. La notion de vie privée aux Etats-Unis diffère grandement de celles existant en Europe. C'est une notion très fragmentée, le droit américain ne disposant d'aucun texte général qui garantirait un droit à la protection de la vie privée ou des données à caractère personnel: pour plus de détails, voir notamment F. GIRARD, « La notion de vie privée aux Etats-Unis », *Droit à l'oubli numérique*, Bruxelles, Larcier, 2015, p. 200 et s.
57. G29, « Avis 1/99 concernant le niveau de protection des données à caractère personnel aux Etats-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain », *WP 15*, 26 janvier 1999, p. 2; J.P. MELTZER, « Examining the EU safe harbor decision and impacts for transatlantic data flows », *Brookings Institution*, 3 novembre 2015.
58. Décision (CE) n° 2000/520 de la Commission.
59. Art. 25, 3. à 6., de la directive (art. 45, 3. à 6., du règlement); A. DEBET, J. MASSOT et N. METALLINOS, *o.c.*, p. 667.
60. B. HAVELANGE et A.-C. LACOSTE, *o.c.*, p. 245.
61. En témoignent notamment les chiffres cités par J. MELTZER concernant les échanges commerciaux entre les Etats-Unis et l'Union européenne et les échanges de données qui les accompagnent: J.P. MELTZER, *o.c.*
62. Le responsable du traitement est défini à l'article 2, d), de la directive comme « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel » (art. 4, 7., du règlement).
63. Sous réserve de dispositions contraires qui seraient prévues dans la législation de l'Etat membre compétent dans un cas déterminé puisque la directive permet aux Etats membres de prévoir des dispositions contraires aux cas prévus par l'article 26, 1., de la directive dans certains cas particuliers: art. 26, 2., de la directive (le sort de telles autorisations est visé par l'art. 46, 5., du règlement).
64. A. DEBET, J. MASSOT et N. METALLINOS, *o.c.*, p. 693. Pour plus de détails sur l'article 26 de la directive (art. 46 du règlement), voir *infra*, Section 2, point 2.2.
65. Décision (CE) n° 2000/520 de la Commission.
66. Considérant (5), article 1er, annexe I et annexe II, décision (CE) n° 2000/520 de la Commission, p. 7, 10 et s.
67. Art. 1er, 2. et 3. et annexe I, décision (CE) n° 2000/520 de la Commission, p. 8 et 10; Y. POULLET, « Internet et vie privée: entre risques et espoirs », *J.T.*, 2001, p. 161.
68. A. DEBET, J. MASSOT et N. METALLINOS, *o.c.*, p. 672. Une fois qu'un pays figure sur cette liste, les Etats membres se doivent, en principe, de permettre une libre circulation des données à caractère personnel vers ce pays si le transfert respecte par ailleurs les autres règles encadrant le droit à la protection des données personnelles dans l'Etat membre de départ: art. 25, 6., alinéa 2, de la directive; AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE, *Manuel de droit européen en matière de protection des données*, 2014, p. 144; A. DEBET, J. MASSOT et N. METALLINOS, *o.c.*, p. 670; A. GROSJEAN, « II – Les transferts de données à des responsables de traitement ou à des sous-traitants établis en dehors de l'Union européenne », *Enjeux européens et mondiaux de la protection des données personnelles*, Bruxelles, Larcier, 2015, p. 199.

26. La seconde condition prévue pour qu'un transfert soit licite est que l'organisation doit être soumise aux pouvoirs légaux de l'un des organes administratifs américains énumérés à l'annexe VII de la décision, cet organe devant être habilité à instruire des plaintes et à obtenir des mesures de redressement contre les pratiques déloyales ou frauduleuses ainsi que la réparation des préjudices subis par les personnes concernées en cas de non-respect des principes précités[69]. Les deux organes énumérés sont la Commission fédérale du commerce (Federal Trade Commission) et le ministère du Transport. Les banques, les sociétés de télécommunications et les entreprises financières d'épargne et de prêt notamment ne relèvent pas de leur compétence et sont donc exclues de l'accord *Safe Harbor* [70].

27. Les principes du *Safe Harbor* sont présumés respectés dès que l'organisation concernée déclare y adhérer[71] et ce sans aucune vérification préalable[72] ni obligation de prouver qu'elle les respecte[73]. Il s'agit d'un système d'autocertification[74], découlant d'un consensus entre l'approche européenne, prévoyant un contrôle par les autorités administratives, et l'approche américaine, privilégiant l'autorégulation par les entreprises elles-mêmes[75]. Ce système, non interdit par la directive[76], permet également aux Etats-Unis de ne pas devoir modifier leur réglementation sur les traitements de données à caractère personnel[77] dont la protection n'est pas un droit fondamental[78].

28. Le *Safe Harbor* a fait l'objet de nombreuses critiques depuis ses débuts, que ce soit du Parlement européen lui-même[79] ou de la part d'auteurs[80], notamment en ce qui concerne son manque d'effectivité et de transparence concernant les règles de protection des données dans les entreprises autocertifiées[81]. De même, le G29 a donné son avis à divers stades des négociations entre les Etats-Unis et la Commission, énonçant de nombreuses critiques, avec un dernier avis en mai 2000[82] qui continue à pointer certains problèmes, notamment les nombreuses exceptions possibles aux principes[83] et l'absence de voies de recours appropriées pour la personne concernée en cas de non-respect des principes[84]. Ce protocole ne semble avoir été bien accueilli ni en Europe, ni aux Etats-Unis[85].

69. Art. 1er, 2., décision (CE) n° 2000/520 de la Commission, p. 8.
70. Annexe VII, décision (CE) n° 2000/520 de la Commission, p. 47.
71. Art. 1er, 2. et 3., lu en combinaison avec la FAQ 6 (annexe II), décision (CE) n° 2000/520 de la Commission, p. 8.
72. G29, « Avis 4/2000 sur le niveau de protection assuré par les 'principes de la sphère de sécurité' », *WP 32*, 16 mai 2000, p. 3.
73. Certaines entreprises autocertifiées ne respectent d'ailleurs pas les principes *Safe Harbor*: COMMISSION DES COMMUNAUTÉS EUROPÉENNES, « Commission staff working document – The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce », *SEC (2004) 1323*, 20 octobre 2004, p. 6 et s.; R.T. NIMMER,« Internationally interactive law: perspectives on trans-border data control from the U.S. », *Défi du droit à la protection de la vie privée. Perspectives du droit européen et nord-américain*, Bruxelles, Bruylant (Cahiers du Centre de Recherches Informatique et Droit, vol. 31), 2008, p. 431; B. HAVELANGE et A.-C. LACOSTE, *o.c.*, p. 246.
74. COMMISSION EUROPÉENNE, « Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire », *Communication COM(2013) 847 final*, 27 novembre 2013, p. 5.
75. J. GONIÉ, « Le protocole 'safe harbour' ou les oppositions américaines et européennes de la protection de la vie privée », *Juriscom.net*, 28 mai 2003 (consulté le 7 mars 2016); pour de plus amples détails sur l'approche américaine de l'époque, voir notamment le volume 31 des Cahiers du Centre de Recherches Informatique et Droit, *Défi du droit à la protection de la vie privée. Perspectives du droit européen et nord-américain* (Bruxelles, Bruylant, 2008) et plus précisément les contributions de N.J. KING, « Fundamental human rights principle inspires U.S. data privacy law, but protections are less than fundamental », p. 72-97, C. MANNY, « Incomplete privacy: how federal law misses problems connected to the U.S. consumer database industry », p. 172-187 et R. GELLMAN, « The american approach to privacy supervision: less than the sum of its parts », p. 611-632; S. DHARAMVEER, « Chapter V – Data Protection », *The outsourcing of legal services*, Windhof, Promoculture-Larcier, 2015, p. 195 et s.; F. GIRARD, *o.c.*, p. 200-227.
76. Y. POULLET, « Transborder Data Flows and Extraterritoriality: The European Position », *Journal of International Commercial Law and Technology*, 2007, vol. 2 (issue 3), p. 146 et 147.
77. R.T. NIMMER, *o.c.*, p. 431.
78. F. MOUZAKITI, « Transborder Data Flows 2.0: Mending the Holes of the Data Protection Directive », *E.D.P.L.*, 2015/1, p. 42.
79. PARLEMENT EUROPÉEN, *o.c.*, *C5-0280/2000 – 2000/2144(C.O.S.)*, 5 juillet 2000.
80. B. HAVELANGE et A.-C. LACOSTE, *o.c.*, p. 245 et 246; A. GROSJEAN, *o.c.*, p. 201; S. DHARAMVEER, *o.c.*, p. 209.
81. F. MOUZAKITI, *o.c.*, p. 43.
82. G29, « Avis 1/99 concernant le niveau de protection des données à caractère personnel aux Etats-Unis et les discussions en cours entre la Commission européenne et le gouvernement américain », *WP 15*, 26 janvier 1999; G29, « Avis 2/99 concernant la pertinence des 'principes internationaux de la sphère de sécurité' publiés par le ministère du Commerce des Etats-Unis le 19 avril 1999 », *WP 19*, 3 mai 1999; G29, « Avis 4/9 concernant les questions souvent posées, devant être publiées par le ministère américain du Commerce dans le cadre des principes proposés pour la 'sphère de sécurité' », *WP 21*, 7 juin 1999; G29, « Document de travail sur l'état actuel des discussions en cours entre la Commission européenne et le gouvernement américain concernant les principes internationaux de la 'sphère de sécurité' relatifs à la protection de la vie privée », *WP 23*, 7 juillet 1999; G29, « Avis 7/99 sur le niveau de protection des données garanti par les principes de la 'sphère de sécurité' publiés avec les questions fréquemment posées (FAQ) et d'autres documents connexes les 15 et 16 novembre 1999 par le ministère du Commerce américain », *WP 27*, 3 décembre 1999; G29, « Avis 3/2000 concernant le dialogue entre l'Union européenne et les Etats-Unis sur l'accord relatif à la 'sphère de sécurité' », *WP 31*, 16 mars 2000; G29, « Avis 4/2000 sur le niveau de protection assuré par les 'principes de la sphère de sécurité' », *WP 32*, 16 mai 2000.
83. G29, « Avis 4/2000 sur le niveau de protection assuré par les 'principes de la sphère de sécurité' », *WP 32*, 16 mai 2000, p. 5.
84. *Ibid.*, p. 7.
85. En témoigne notamment aussi le peu d'entreprises qui se sont autocertifiées suite à l'adoption des principes *Safe Harbor* (400 entreprises fin 2003): COMMISSION DES COMMUNAUTÉS EUROPÉENNES, « Commission staff working document – The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce », *SEC (2004) 1323*, 20 octobre 2004, p. 5; B. HAVELANGE et A.-C. LACOSTE, *o.c.*, p. 246; R.T. NIMMER, *o.c.*, p. 431; S. DHARAMVEER, *o.c.*, p. 210; N.N. LOIDEAN, « The end of Safe Harbor implications for EU digital privacy and data protection law », *Journal of Internet Law*, 2016/19.8, p. 8.

29. L'une des critiques, reprise plus tard par la Commission européenne elle-même, est la distorsion de concurrence que le système mis en place peut générer[86]. En effet, puisqu'une entreprise établie aux Etats-Unis qui désire utiliser des données de citoyens européens peut elle-même déclarer qu'elle respecte les principes *Safe Harbor* sans que cette déclaration ne soit prouvée et sans mettre en place les mécanismes pour s'y tenir, cette entreprise peut éviter de nombreux coûts et ce à moindre risque puisque les recours semblent peu accessibles aux citoyens européens alors qu'une entreprise européenne exerçant les mêmes activités auprès des mêmes citoyens sera beaucoup plus contrôlée et devra même obtenir l'accord préalable de l'autorité nationale de contrôle compétente pour traiter ce type de données[87]. Le Parlement regrette à cet égard l'absence « de consultations des entreprises européennes sur les risques de discriminations par rapport aux entreprises US qui, en matière de protection des données, seraient soumises à des obligations moins contraignantes que celles que doivent respecter les entreprises européennes »[88].

30. Malgré les critiques, cet accord est resté en vigueur 15 ans avant d'être invalidé, le 20 octobre 2015, par la Cour de justice de l'Union européenne. Pourtant, la Commission avait déjà remis en question ce système...

1.2. La Commission européenne: l'autocritique avant l'annulation? Les révélations d'Edward Snowden ou l'impossibilité pour la Commission de continuer sa politique de l'autruche

31. Suite aux révélations de M. Snowden concernant la surveillance de masse des données par les autorités américaines, la Commission européenne a émis deux communications en date du 27 novembre 2013 dans lesquelles, tout en rappelant l'importance des transferts de données entre l'Union européenne et les Etats-Unis, elle réaffirme la nécessité d'assurer un niveau élevé de protection des données[89]. Ce niveau est, selon la Commission, assuré grâce à différentes réglementations existantes entre les deux entités dont seule la décision *Safe Harbor* nous intéresse en l'espèce.

32. Les révélations précitées ont bouleversé le monde entier[90]. Pour restaurer la confiance entre l'Union et les Etats-Unis, la Commission a dès lors proposé de procéder en plusieurs étapes[91], notamment en réformant la législation européenne en place, en renforçant les principes *Safe Harbor* et leur contrôle effectif par le ministère américain du Commerce[92] et en offrant les mêmes garanties procédurales aux citoyens européens qu'aux citoyens américains concernant le traitement de leurs données et ce via un système de recours accessible et économiquement abordable[93].

33. La Commission critique ainsi le système qu'elle a elle-même mis en place mais en propose les solutions via 13 recommandations[94]. Son objectif est clair: il existe effectivement des défauts, notamment concernant l'accès aux données de citoyens européens octroyé par certaines entreprises certifiées aux agences de renseignement américaines sous le couvert de la « sécurité nationale »[95] et le traitement de ces données d'une « manière incompatible, notamment, avec les finalités de leur transfert et au-delà de ce qui était strictement nécessaire et proportionné à la protection de la sécurité nationale »[96], mais la Commission ne met pas pour autant fin au système qu'elle a mis tant d'années à organiser.

34. Malgré ces communications émises en 2013, la nouvelle législation européenne concernant les données à caractère personnel n'a été adoptée qu'en 2016 et les principes *Safe Harbor* ne furent remis en question que suite à leur invalidation par la Cour de justice. Les entreprises américai-

86. COMMISSION EUROPÉENNE, « Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire », *Communication COM(2013) 847 final*, 27 novembre 2013, p. 15; COMMISSION EUROPÉENNE, « Rebuilding Trust in EU-US Data Flows », *Communication COM(2013) 846 final*, 27 novembre 2013, p. 4.

87. Art. 18 de la directive.

88. PARLEMENT EUROPÉEN, *o.c.*, *C5-0280/2000 – 2000/2144(C.O.S.)*, 5 juillet 2000.

89. COMMISSION EUROPÉENNE, « Rebuilding Trust in EU-US Data Flows », *Communication COM(2013) 846 final*, 27 novembre 2013, p. 2; COMMISSION EUROPÉENNE, « Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire », *Communication COM(2013) 847 final*, 27 novembre 2013; A. GROSJEAN, *o.c.*, p. 202.

90. G29, « Déclaration commune des autorités européennes de protection des données réunies au sein du groupe de l'article 29 », *WP 227*, 26 novembre 2014, p. 2; B. BEAUMONT, « Sept manières dont le monde a changé grâce à Edward Snowden », *Amnesty International*, www.amnesty.org/fr/latest/campaigns/2015/06/7-ways-the-world-has-changed-thanks-to-edward-snowden, 4 juin 2015 (consulté le 9 avril 2016).

91. COMMISSION EUROPÉENNE, « Rebuilding Trust in EU-US Data Flows », *Communication COM(2013) 846 final*, 27 novembre 2013, p. 5 et s.

92. COMMISSION EUROPÉENNE, « Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire », *Communication COM(2013) 847 final*, 27 novembre 2013, p. 10-11 et 20.

93. *Ibid.*, p. 11-12 et 16-17.

94. COMMISSION EUROPÉENNE, « Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire », *Communication COM(2013) 847 final*, 27 novembre 2013.

95. *Ibid.*, p. 19.

96. *Ibid.*, p. 21 et s.; E. WÉRY et T. LÉONARD, « Le Safe Harbour est mort! C'est la justice qui l'a tué », *Droit & Technologies*, 6 octobre 2015 (consulté le 23 mars 2016). De tels traitements sont notamment autorisés par le USA Patriot Act du 24 octobre 2001, le Foreign Intelligence Surveillance Act de 1978 tel qu'amendé le 9 juillet 2008 (et plus spécifiquement les art. 702 et 1881a) et le Electronic Communications Privacy Act de 1986.

nes ont donc pu continuer à transférer des données jusque fin 2015 sous le couvert du *Safe Harbor* malgré les problèmes constatés. L'arrêt de la Cour, d'une clarté solaire, permet enfin d'avancer.

SECTION 2. LE « TRAIT D'UNION ENTRE CE QUI A ÉTÉ ET CE QUI SERA »[97]

« *Du fait de son histoire et de sa culture communes, l'Europe doit faire entendre sa voix sur les moyens d'assurer le respect des droits fondamentaux, parmi eux la protection de la vie privée et la protection des données à caractère personnel, sans faire obstacle ni à l'innovation, ni au besoin d'assurer la sécurité de nos sociétés.* »[98].

2.1. La Cour de justice de l'Union européenne tranche le nœud gordien

35. Il est dorénavant impossible d'étudier les transferts transfrontaliers de données à caractère personnel entre l'Union européenne et les Etats-Unis sans mentionner et analyser l'affaire *Schrems* qui a eu l'effet d'un tsunami, ou, en réalité, considérant les critiques préexistantes, de la goutte d'eau faisant déborder le vase.

36. Maximillian Schrems, citoyen autrichien, utilisateur du réseau Facebook[99], a lancé cette affaire en Irlande, pays d'établissement de Facebook Ireland, filiale de Facebook Inc., établie aux Etats-Unis. Suite aux révélations de Snowden concernant les activités des services de renseignement américains[100], Schrems a saisi l'autorité de contrôle irlandaise[101] pour lui demander d'empêcher Facebook Ireland de transférer ses données vers les Etats-Unis[102] (les serveurs de traitement des données de Facebook y sont situés[103]) car « le droit et les pratiques en vigueur dans ce pays ne garantissaient pas une protection suffisante des données à caractère personnel conservées sur le territoire de celui-ci contre les activités de surveillance qui y étaient pratiquées par les autorités publiques »[104].

37. L'autorité irlandaise a refusé de faire droit à sa plainte, estimant que la décision *Safe Harbor* constatait que les Etats-Unis assuraient un niveau de protection adéquat[105]. La Haute Cour de justice irlandaise (High Court of Ireland), saisie d'un recours contre cette décision, a décidé d'interroger la Cour de justice de l'Union européenne sur le caractère liant de la décision *Safe Harbor* pour l'autorité de contrôle, estimant celle-ci contraire aux articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne[106], protégeant la vie privée, les données à caractère personnel, le droit à un recours effectif et à accéder à un tribunal impartial. Autrement dit, l'autorité irlandaise pouvait-elle examiner la demande de M. Schrems concernant le transfert de ses données vers les Etats-Unis et, le cas échéant, décider que ce pays n'offre pas un niveau de protection adéquat au sens de l'article 25, 1., de la directive[107]?

38. Après avoir rappelé la présomption de légalité recouvrant les actes des institutions de l'Union[108], dont la décision *Safe Harbor* de la Commission, ainsi que l'aspect contraignant de cette décision pour les Etats membres[109], la Cour dit pour droit que ni cette présomption de légalité, ni l'aspect contraignant de la décision, ne pourraient empêcher les personnes concernées par un transfert de leurs données vers un pays tiers de saisir les autorités nationales de contrôle d'une demande concernant la protection de leurs droits et libertés à l'égard du traitement de ces données et ces autorités de se prononcer[110]. En effet, la Cour note que ni l'article 8, 3., de la charte[111], ni

97. H. Bergson, *L'énergie spirituelle*, Paris, Félix Alcan, 1919, p. 7.
98. G29, « Déclaration commune des autorités européennes de protection des données réunies au sein du groupe de l'article 29 », *WP 227*, 26 novembre 2014, p. 2.
99. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 26.
100. Snowden révèle en effet en 2013 que toutes les grandes entreprises américaines fournissent des données à caractère personnel de citoyens notamment européens à la NSA sans en informer ces citoyens et sans que ceux-ci puissent faire de recours: S. PEYROU, « La Cour de justice de l'Union européenne, à l'avant-garde de la défense des droits numériques », *J.D.E.*, 2015, p. 395; G. TOUSSAINT, « La protection des données, un enjeu démocratique majeur », *La Libre.be*, 19 octobre 2013 (mise à jour le 20 octobre 2013).
101. Etablie par l'art. 28 de la directive (art. 51 du règlement).
102. Pour des exemples de données traitées par Facebook et des traitements réalisés, voir J.-P. MOINY, *o.c.*, p. 241-243.
103. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 27.
104. *Ibid.*, point 28.
105. *Ibid.*, point 29.
106. HIGH COURT OF IRELAND, 16 juillet 2014, Case No. 2013/765JR, *Maximilian Schrems / Data Protection Commissioner*, www.europe-v-facebook.org/Order_ADJ.pdf (consulté le 1er avril 2016), p. 2; C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, points 34-36.
107. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 37.
108. *Ibid.*, point 52.
109. Art. 25, 6., alinéa 2, de la directive; art. 288, alinéa 4, TFUE; C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 51.
110. Ce point de vue n'était pas celui attendu par certains commentateurs qui pensaient que la Cour se bornerait à renvoyer à la décision *Safe Harbor* de la Commission: A. GROSJEAN, *o.c.*, p. 205. *A contrario*, d'autres en avaient déjà évoqué la possibilité: F. MOUZAKITI, *o.c.*, p. 49.
111. Qui permet aux personnes visées par un traitement de leurs données à caractère personnel de saisir les autorités nationales de contrôle d'une demande concernant la protection de leurs droits fondamentaux.

l'article 28 de la directive[112] n'excluent le contrôle des transferts de données personnelles vers des pays tiers du domaine de compétence des autorités nationales même lorsque ces transferts sont réglementés par une décision de la Commission adoptée en vertu de l'article 25, 6., de la directive[113].

39. Néanmoins, lorsqu'une personne fait valoir que le droit et les pratiques d'un pays vers lequel ses données ont été ou pourraient être transférées n'assurent pas un niveau de protection adéquat alors qu'une décision de la Commission constate le contraire, seule la Cour de justice est compétente pour se prononcer sur la validité de cette décision[114]. Une question préjudicielle s'impose donc afin d'obtenir son avis.

40. La Cour commence par rappeler que l'article 25, 6., de la directive vise à assurer un niveau de protection élevé en cas de transfert de données vers un pays tiers[115], ce niveau ne devant pas être identique à celui garanti dans l'ordre juridique de l'Union mais « substantiellement équivalent »[116]. Comme nous l'avons relevé[117], à défaut d'une telle exigence, il serait facile de contourner la directive en transférant simplement les données personnelles depuis l'Union vers des pays tiers pour les traiter là-bas[118].

41. L'article 25, 6., de la directive prévoit que la Commission doit prendre en compte, avant de décider qu'un pays tiers offre un niveau de protection adéquat, la législation interne, les engagements internationaux et la pratique de ce pays[119]. Ce niveau doit par ailleurs être vérifié de manière périodique, tant en fait qu'en droit, puisqu'il est susceptible d'évoluer[120] et la validité de la décision adoptée par la Commission peut être remise en cause suite à des circonstances intervenues après l'adoption de la décision[121].

42. En l'espèce, la Cour estime que le niveau de protection requis n'est pas atteint et ce notamment parce que (1) les autorités publiques américaines ne sont pas soumises au respect des principes *Safe Harbor* [122]; (2) la décision ne constate pas de manière suffisante qu'il existerait des mesures par lesquelles les Etats-Unis assureraient un niveau de protection adéquat[123]; (3) les limitations à l'application des principes *Safe Harbor* sont exorbitantes[124]; (4) la décision *Safe Harbor* ne mentionne aucune règle à caractère étatique qui pourrait limiter les éventuelles ingérences dans les droits fondamentaux des personnes dont les données sont visées[125] et; (5) la décision ne mentionne pas l'existence d'une protection juridique efficace contre ces éventuelles ingérences (seuls les litiges commerciaux portant sur le respect des principes *Safe Harbor* par les entreprises américaines sont visés et non les ingérences d'origine étatique)[126].

43. Il est dès lors évident que les droits fondamentaux des personnes dont les données personnelles sont transférées ou pourraient être transférées depuis l'Union vers les Etats-Unis sont bafoués[127]. Notons qu'à l'heure actuelle, au vu de la mondialisation et du nombre de sociétés basées aux Etats-Unis qui possèdent des filiales en Europe[128] susceptibles de leur transférer des données, cela touche potentiellement chaque citoyen européen.

44. La Cour pousse ensuite le vice jusqu'à citer l'appréciation de la Commission elle-même, à travers les deux communications exposées *supra*, pour démontrer que la décision

112. Qui institue une autorité de contrôle par Etat et explicite ses compétences (art. 51 du règlement).
113. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, points 54 et s.
114. C.J.C.E., 22 octobre 1987, C-314/85, *Foto-Frost / Hauptzollamt Lübeck-Ost*, ECLI:EU:C:1987:452, points 15-20; C.J.C.E., 10 janvier 2006, C-344/04, *International Air Transport Association et European Low Fares Airline Association / Department for Transport*, ECLI:EU:C:2006:10, point 27; C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, points 59 et 62.
115. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 72.
116. *Ibid.*, point 73.
117. Voir *supra*, section 1, point 1.1.
118. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 73.
119. *Ibid.*, point 75.
120. *Ibid.*, point 76.
121. *Ibid.*, point 77.
122. *Ibid.*, point 82.
123. *Ibid.*, points 83 et 97.
124. *Ibid.*, points 84-86.
125. *Ibid.*, point 88.
126. *Ibid.*, point 89; E. WÉRY et T. LÉONARD, « Le Safe Harbour est mort! C'est la justice qui l'a tué », *o.c.*; R. SCHOEFS, « Doorsturen van persoonsgegevens naar VS in het gedrang », *Juristenkrant*, 2015 (liv. 315), p. 3.
127. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 87; c.-à-d. les droits au respect de la vie privée et à la protection des données à caractère personnel (art. 7 et 8 de la charte des droits fondamentaux de l'Union européenne) ainsi que le droit à une protection juridictionnelle effective (art. 47 de la charte des droits fondamentaux de l'Union européenne): E. WÉRY et T. LÉONARD, « Le Safe Harbour est mort! C'est la justice qui l'a tué », *o.c.*
128. COMMISSION EUROPEENNE, « Rebuilding Trust in EU-US Data Flows », *Communication COM(2013) 846 final*, 27 novembre 2013, p. 3. Notons que ces entreprises bénéficiaient du régime *Safe Harbor*: O. TAMBOU, « Propos libres autour de l'invalidation par la CJUE de la décision Safe Harbor », *Dalloz Actualité*, 9 octobre 2015; « U.S.-EU Safe Harbor List », *Export.gov*, www.safeharbor.export.gov/list.aspx (consulté le 9 avril 2016).

prise par cette même institution 15 ans plus tôt doit être déclarée invalide[129].

45. Pour toutes ces raisons, la Cour estime que l'article 1er de la décision *Safe Harbor* méconnaît les exigences de l'article 25, 6., de la directive, lu à la lumière de la charte et qu'il est donc invalide[130]. Elle note ensuite que l'article 3, 1., alinéa 1er, de la même décision empêche les autorités nationales de contrôle de prendre des mesures pour assurer le respect de l'article 25 de la directive, ce qui est contraire à l'article 28 de la directive et constitue un excès de pouvoir de la part de la Commission qui ne pouvait pas restreindre ainsi les pouvoirs des autorités de contrôle en vertu de l'article 25, 6., de la directive, lu à la lumière de la charte. Cet article 3 est donc également invalidé[131]. Comme ces deux articles sont indissociables du reste, leur invalidité emporte l'invalidité de la décision dans son ensemble[132], et ce sans que la Cour ne doive se prononcer sur les principes *Safe Harbor* eux-mêmes.

46. Les deux points forts de la décision de la Cour, par lesquels elle suit les recommandations de son avocat général[133], concernent la marge de manœuvre des autorités nationales de contrôle lorsqu'une décision de la Commission existe[134] et l'invalidation du système *Safe Harbor*[135] prononcée par la Cour sans qu'elle ne soit interrogée sur ce point par le juge *a quo* [136]. Mentionnons également l'interprétation de la notion de « niveau de protection adéquat » par la Cour comme requérant un niveau de protection « substantiellement équivalent » à celui prévu au sein de l'Union européenne.

47. M. Schrems n'a pas été le premier à remettre en doute la décision *Safe Harbor* suite aux révélations concernant les programmes des agences de renseignement américaines mais c'est le seul particulier à avoir été aussi loin[137]. Le Parlement européen lui-même avait expressément demandé à la Commission de suspendre cette décision suite aux révélations concernant la NSA, tout comme le G29[138] et la Commission LIBE[139], mais la Commission n'en a eu cure[140], préférant continuer, contre vents et marées, à utiliser le *Safe Harbor*. La Cour s'en est dès lors chargée.

48. Cet arrêt n'est pas le premier dans lequel la Cour se pose en véritable gardienne de la vie privée et de la protection des données des citoyens européens. En effet, en avril 2014, elle avait, dans son arrêt *Digital Rights Ireland*, invalidé une directive concernant la rétention de données personnelles et ce sur base de critiques également formulées dans l'arrêt *Schrems* telles que le non-respect du principe de proportionnalité, l'absence de garanties suffisantes pour éviter un accès abusif, notamment par les autorités nationales, aux données ainsi que l'absence de garanties procédurales pour les citoyens[141]. L'arrêt *Google Spain*[142] démontre lui aussi que la Cour décide de se positionner en véritable Cour constitutionnelle garantissant le respect des droits fondamentaux inscrits dans la charte de l'Union[143]. Dans cet arrêt, elle a ainsi affirmé l'existence du désormais célèbre « droit à l'oubli »[144].

49. L'un des points communs des arrêts *Digital Rights Ireland* et *Schrems* est l'affirmation par la Cour du fait que les

129. COMMISSION EUROPÉENNE, « Rebuilding Trust in EU-US Data Flows », *Communication COM(2013) 846 final*, 27 novembre 2013; COMMISSION EUROPÉENNE, « Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire », *Communication COM(2013) 847 final*, 27 novembre 2013; C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 90.
130. *Ibid.*, point 98.
131. *Ibid.*, points 100-104.
132. *Ibid.*, points 105 et 106.
133. C.J.U.E., Concl. Av. gén. M. Y. BOT, 23 septembre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:627, point 237.
134. Les pouvoirs des autorités nationales ont aussi fait l'objet de l'arrêt *Weltimmo* rendu le même mois: C.J.U.E., 1er octobre 2015, C-230/14, *Weltimmo s.r.o. / Nemzeti Adatvedelmi es Informacioszabadsag Hatosag*, ECLI:EU:C:2015:639; S. PEYROU, *o.c.*, p. 396.
135. E. WÉRY et T. LÉONARD, « Le Safe Harbour est mort! C'est la justice qui l'a tué », *o.c.*
136. A. BAILLEUX et N. TULKENS, « Les droits fondamentaux dans l'ordre juridique de l'Union européenne », *J.D.E.*, 2015, p. 414.
137. COMMISSION EUROPÉENNE, « Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire », *Communication COM(2013) 847 final*, 27 novembre 2013, p. 6.
138. G29, Lettre de I. Falque-Pierrotin, présidente du G29, à V. Reding, vice-présidente de la Commission, *Ares(2014)1139376*, 10 avril 2014, p. 1.
139. COMMISSION DES LIBERTÉS CIVILES, DE LA JUSTICE ET DES AFFAIRES INTÉRIEURES, « Rapport sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)) », *A7-0139/2014*, 21 février 2014, p. 29 et 30. La Commission LIBE va même jusqu'à demander aux Etats membres de faire usage de leurs compétences pour suspendre les flux de données aux organisations ayant adhéré aux principes *Safe Harbor*.
140. PARLEMENT EUROPÉEN, « Résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)) », *P7_TA(2014)0230*, 12 mars 2014, p. 26; S. PEYROU, *o.c.*, p. 397.
141. C.J.U.E., 8 avril 2014, C-293/12 et C-594/12, *Digital Rights Ireland Ltd / Minister for Communications, Marine and Natural Resources e.a.*, ECLI:EU:C:2014:238, points 35, 37, 45, 54, 61, 62, 65 et 66; K. ROSIER, « La C.J.U.E. invalide la directive européenne sur la rétention des données », *B.S.&J.*, 2014/2, p. 14.
142. C.J.U.E., 13 mai 2014, C-131/12, *Google Spain SL et Google Inc. / Agencia Espanola de Proteccion de Datos (AEPD) et Mario Costeja Gonzalez*, ECLI:EU:C:2014:317.
143. O. TAMBOU, « Propos libres autour de l'invalidation par la CJUE de la décision *Safe Harbor* », *o.c.*
144. N.N. LOIDEAN, *o.c.*, p. 11.

critères de légalité, de nécessité et de proportionnalité doivent être rencontrés dans toute future (et actuelle) législation européenne concernant le droit à la protection des données à caractère personnel (et surtout les ingérences dans ce droit) et ce à la lumière des articles 7 et 8 de la charte de l'Union[145]. Ces articles sont également repris dans l'analyse juridique de l'arrêt *Google Spain*[146].

50. Ces trois arrêts datent de la période « post Snowden » et ce n'est sans doute pas un hasard. La position de la Cour s'est durcie: en 2006, également à propos d'une décision d'adéquation entre l'Union et les Etats-Unis, elle avait laissé aux autorités un délai de plusieurs mois durant lesquels l'une des décisions en cause[147] conservait ses effets[148] tandis que dans l'arrêt *Schrems*, elle ne mentionne aucun délai, l'invalidation est immédiate, et ce même si cela crée un climat d'incertitude dans les échanges commerciaux américano-européens. Ce dernier arrêt, selon O. Tambou, « prend les allures d'une décision *Solange*[149] », car la Cour affirme implicitement qu'aucun transfert ne pourra avoir lieu vers les Etats-Unis aussi longtemps que le niveau de protection des données n'y sera pas « adéquat »[150], tout comme la Cour constitutionnelle allemande avait affirmé qu'elle exercera son contrôle sur le droit communautaire dérivé aussi longtemps que (« Solange ») le niveau de protection des droits fondamentaux prévus par le droit européen ne sera pas équivalent à celui prévu par la législation allemande[151].

51. La Cour s'est ainsi chargée de rappeler l'importance du droit à la protection des données à caractère personnel, droit qui ne peut pas être sacrifié sur l'autel de l'ère numérique et des désirs sécuritaires des Etats-Unis, aussi légitimes soient-ils. Tant que l'accès aux données ne sera pas limité à ce qui est proportionnel et nécessaire, la Cour risque de continuer à jouer le gendarme dans les négociations entre l'Union et les Etats-Unis, gendarme soutenu par les citoyens qui, à la fois dans l'arrêt *Google* et dans l'arrêt *Schrems*, ont permis à l'Europe de garder la tête haute. Cela ne veut cependant pas dire qu'il faille arrêter tout transfert de données européennes vers des entreprises américaines...

2.2. L'annulation du *Safe Harbor* condamne-t-elle les transferts de données vers les Etats-Unis?

52. Si c'est enfoncer des portes ouvertes que d'annoncer qu'après la décision de la Cour plus aucun transfert ne peut prendre la décision *Safe Harbor* pour fondement légal[152], et ce avec effet immédiat[153], les entreprises n'ont pas dû cesser tout transfert en attendant le nouvel accord: il existe en effet d'autres possibilités pour continuer à transférer des données vers les Etats-Unis, du moins en théorie, une fois les autres principes prévus par la directive respectés[154].

53. L'article 26 de la directive prévoit ainsi plusieurs cas de figure si le niveau adéquat de protection n'est pas atteint (*supra*, n^{os} 21-22): outre la possibilité d'obtenir le consentement de la personne concernée[155] et les cas dans lesquels le transfert lui est nécessaire[156], des solutions telles que les règles contraignantes d'entreprise ou les clauses contractuelles[157] existent. Ces solutions contractuelles seront examinées avant les autres dérogations prévues à l'article 26, 1., car ces dernières doivent être utilisées, selon le G29, en dernier ressort[158].

145. *Ibid.*

146. C.J.U.E., 13 mai 2014, C-131/12, *Google Spain SL et Google Inc. / Agencia Espanola de Proteccion de Datos (AEPD) et Mario Costeja Gonzalez*, ECLI:EU:C:2014:317, points 68-74.

147. Deux décisions étaient remises en cause en l'espèce par le Parlement européen: C.J.C.E., 30 mai 2006, C-317/04 et C-318/04, *Parlement européen / Conseil de l'Union européenne*, ECLI:EU:C:2006:346.

148. C.J.C.E., 30 mai 2006, C-317/04 et C-318/04, *Parlement européen / Conseil de l'Union européenne*, ECLI:EU:C:2006:346, point 74.

149. BUNDESVERFASSUNGSGERICHT (2^{e} ch.), 29 mai 1974, Internationale Handelsgesell-schaft, *R.T.D.E.*, 1975, p. 316-333, citée par J. CALLEWAERT, « Les droits fondamentaux entre cours nationales et européennes », *Rev. trim. D.H.*, 2001, p. 1188 et M. ROCCATI, « Section 2. L'abandon relatif de souveraineté des juridictions nationales », *Le rôle du juge national dans l'espace judiciaire européen*, Bruxelles, Bruylant, 2013, p. 389.

150. O. TAMBOU, « Propos libres autour de l'invalidation par la CJUE de la décision *Safe Harbor* », *o.c.*

151. J. CALLEWAERT, *o.c.*, p. 1188; M. ROCCATI, *o.c.*, p. 389.

152. G29, « Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14) », *Communiqué de presse*, 16 octobre 2015, p. 2; K. ROSIER, « L'arrêt *Schrems* de la CJUE: un coup d'arrêt au transfert de données à caractère personnel vers les Etats-Unis », *B.J.S.*, 2016/2, p. 6.

153. N.N. LOIDEAN, *o.c.*, p. 12.

154. G29, « Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 », *WP 114*, 25 novembre 2005, p. 9.

155. Article 26, 1., a), de la directive (art. 49, 1., a), du règlement).

156. Que ce soit pour la conclusion d'un contrat entre elle et le responsable du traitement ou que ce soit pour sauvegarder son intérêt vital notamment: art. 26, 1., b) et e), de la directive (art. 49, 1., b) et f), du règlement).

157. Art. 26, 2., de la directive (art. 46 du règlement); G29, « Document de travail: transferts de données personnelles vers des pays tiers: application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données », *WP 74*, 3 juin 2003; G29, « Statement of the Article 29 Working Party on the consequences of the Schrems judgment », *Communiqué de presse*, 3 février 2016, p. 2; R. ROBERT, « Archivage des e-mails et protection de la vie privée », *L'archivage électronique et le droit*, Bruxelles, Larcier, 2012, p. 91; la CNIL, autorité de contrôle française, a ainsi publié une foire à questions à destination des entreprises concernant les transferts de données vers les Etats-Unis: CNIL, « Le Safe Harbor », www.cnil.fr/le-safe-harbor, 8 janvier 2016 (consulté le 16 mars 2016).

158. G29, « Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 », *WP 114*, 25 novembre 2005, p. 10.

54. Les règles contraignantes d'entreprise, mieux connues sous le nom de « binding corporate rules » (ci-après les « BCR »), sont des règles internes adoptées par des groupes multinationaux de sociétés afin de définir leur politique globale concernant les transferts internationaux de données protégées par la réglementation européenne, entre sociétés du groupe, notamment celles situées dans des pays tiers n'offrant pas un niveau de protection adéquat[159]. Ces BCR ont été créées par le G29 en 2003 comme une alternative aux clauses contractuelles et au *Safe Harbor* pour les transferts internationaux complexes vers plusieurs pays tiers[160].

55. Les principes guidant ces BCR ne se trouvent donc pas dans la directive même mais dans des documents du G29[161], ce qui a rendu ces BCR particulièrement attractives puisque moins sujettes à interprétation que la directive qui donne des principes plutôt larges[162] là où le G29 formule de nombreux conseils et précisions dans les divers documents adoptés à cet égard.

56. Ces BCR doivent être approuvées par l'autorité nationale de contrôle dite « chef de file »[163] mais permettent ensuite de transférer librement des données au sein du groupe sans aller à l'encontre des principes prévus aux articles 25 et 26 de la directive[164]. Ainsi, UCB dispose de telles BCR (approbation des autorités belges), tout comme BMW (approbation des autorités allemandes), e-Bay (approbation des autorités luxembourgeoises) ou le cabinet d'avocats Linklaters (approbation des autorités anglaises)[165].

57. Les clauses contractuelles visent, quant à elles, à fournir des garanties similaires aux BCR mais dans le cadre d'un contrat spécifique prévoyant un transfert de données dans un Etat n'assurant pas un niveau de protection adéquat[166] et ce en dehors d'un groupe de sociétés. Il s'agit donc d'un équivalent, quoique moins pratique puisqu'il implique des clauses inscrites dans chaque contrat, pour les transferts entre des sociétés non liées. Les entreprises peuvent choisir entre les clauses contractuelles types, adoptées par la Commission en vertu de l'article 26, 4., de la directive[167], et leurs propres clauses dont la conformité doit être examinée par les autorités nationales compétentes[168].

58. Si le transfert se fonde par contre sur l'un des cas de figure prévus par l'article 26, 1., de la directive, ce transfert peut avoir lieu dans tout pays, qu'il dispose ou non d'un

159. COMMISSION EUROPÉENNE, « Overview on Binding Corporate rules », www.ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm, dernière mise à jour le 23 mars 2016 (consulté le 28 mars 2016).

160. G29, « Document de travail: transferts de données personnelles vers des pays tiers: application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données », *WP 74*, 3 juin 2003, p. 5; S. DHARAMVEER, *o.c.*, p. 215.

161. G29, « Document de travail: transferts de données personnelles vers des pays tiers: application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données », *WP 74*, 3 juin 2003; G29, « Liste de contrôle type. Demande d'approbation de règles d'entreprise contraignantes », *WP 102*, 25 novembre 2004; G29, « Document de travail relatif à une procédure de coopération en vue de l'émission d'avis communs sur le caractère adéquat de la protection offerte par les 'règles d'entreprise contraignantes' », *WP 107*, 14 avril 2005; G29, « Document de travail établissant une liste de contrôle type pour les demandes d'approbation des règles d'entreprise contraignantes », *WP 108*, 14 avril 2005; G29, « Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data », *WP 133*, 10 janvier 2007; G29, « Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes », *WP 153*, 24 juin 2008; G29, « Document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes », *WP 154*, 24 juin 2008; G29, « Document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes », *WP 155 rév. 04*, 24 juin 2008 (révisé en dernier lieu le 8 avril 2009); G29, « Document de travail 02/2012 établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes pour les sous-traitants », *WP 195*, 6 juin 2012; G29, « Avis 02/2014 relatif à un référentiel des exigences pour les règles d'entreprise contraignantes soumises aux autorités nationales responsables de la protection des données dans l'UE et les règles transfrontalières de protection de la vie privée soumises aux agents de responsabilisation de l'APEC en matière de RTPVP », *WP 212*, 27 février 2014; G29, « Explanatory Document on the Processor Binding Corporate Rules », *WP 204 rev. 01*, 19 avril 2013 (révisé en dernier lieu le 22 mai 2015).

162. N. PURTOVA, *o.c.*, p. 214.

163. Il s'agit d'une procédure européenne coordonnée pour qu'une entreprise ne doive pas s'adresser à plusieurs autorités de contrôle mais seulement à une qui contacte ensuite les autres autorités concernées: A. GROSJEAN, *o.c.*, p. 207.

164. COMMISSION EUROPÉENNE, « Overview on Binding Corporate rules », www.ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm, dernière mise à jour le 23 mars 2016 (consulté le 28 mars 2016).

165. COMMISSION EUROPÉENNE, « List of companies for which the EU BCR cooperation procedure is closed », www.ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm, dernière mise à jour le 23 mars 2016 (consulté le 28 mars 2016). Il est d'ailleurs intéressant de noter que ces BCR sont plus utilisées en France, aux Pays-Bas, en Allemagne et en Grande-Bretagne que dans tous les autres Etats membres de l'Union.

166. COMMISSION EUROPÉENNE, « Model Contracts for the transfert of personal data to third countries », www.ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm, dernière mise à jour le 2 décembre 2015 (consulté le 28 mars 2016).

167. Décision (CE) n° 2004/915 de la Commission du 27 décembre 2004 modifiant la décision n° 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers, *J.O.U.E.*, L. 385, 29 décembre 2004, p. 74 et s.; décision (UE) n° 2010/87 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.U.E.*, L. 39, 12 février 2010, p. 5 et s.

168. A. GROSJEAN, *o.c.*, p. 206. A noter que certaines autorités examinent également des demandes concernant des clauses contractuelles types mais simplement pour vérifier que les clauses utilisées correspondent effectivement aux clauses contractuelles types: COMMISSION EUROPÉENNE, « Frequently Asked Questions relating to transfers of personal data from the EU/EEA to third countries », www.ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf (consulté le 1er avril 2016), p. 26 et 27.

niveau de protection adéquat, et aucune autorisation préalable des autorités compétentes n'est nécessaire[169]. Ces cas sont prévus comme des dérogations et doivent être interprétés de manière restrictive: l'exception ne peut en effet pas devenir la règle[170].

59. Il existe ainsi la possibilité de demander le consentement de la personne concernée[171], de démontrer que le transfert de données est nécessaire[172] (1) pour la conclusion ou l'exécution de certains contrats[173], (2) pour « la sauvegarde d'un intérêt public important[174], ou pour la constatation, l'exercice ou la défense d'un droit en justice »[175], (3) pour la sauvegarde de l'intérêt vital de la personne concernée[176]; ou (4) si le transfert intervient au départ d'un registre public destiné à l'information du public[177]. Ces trois derniers cas de figure[178] ne sont cependant pas pertinents dans notre contexte de transferts commerciaux. Il reste donc les conclusions de contrats qui nous semblent être un fondement valide à un transfert européano-américain (p. ex. disposer du nom d'une personne qui désire louer une chambre d'hôtel) et le consentement de la personne concernée.

60. Concernant la possibilité de demander le consentement de la personne concernée, certains auteurs notent cependant qu'il est très peu probable que celui-ci puisse être valide considérant l'impossibilité pour la personne de savoir exactement ce à quoi elle consent concernant l'utilisation de ses données puisque, quand bien même nous pourrions imaginer une formule standard selon laquelle les entreprises expliquent que les services de renseignement américains pourraient avoir accès aux données avec une case à cocher pour le citoyen dont les données sont concernées, les services de renseignement sont pour le moins peu transparents sur le traitement de ces données, or le consentement doit être informé pour être valide (pour ne relever que cette critique-là)[179]. Néanmoins, les autorités allemandes estiment que, sous des conditions strictes, le consentement de la personne concernée peut être une base valide de transfert mais de tels transferts ne peuvent pas s'opérer de manière répétitive ou à grande échelle[180], ce qui rend cette base inutilisable pour de grands groupes transférant quotidiennement les données de leurs clients ou de leurs travailleurs.

61. L'annulation de la décision *Safe Harbor* ne condamne donc pas, en tant que tels, les transferts de données vers les Etats-Unis mais les rend plus compliqués puisqu'il ne s'agit plus d'avoir un seul cadre juridique pour l'ensemble des transferts effectués (les principes *Safe Harbor*) mais bien d'avoir des clauses y afférant dans chaque contrat prévoyant un transfert, de disposer de BCR dans les groupes de sociétés (solutions contractuelles) ou de se situer dans le champ précis de l'article 26, 1., de la directive (cas prévus par la législation).

62. Cependant, déjà en 2013, la Commission notait que certaines entreprises ne pourraient pas se satisfaire de ces options, comme c'est le cas de MasterCard qui traite avec des milliers de banques[181]. De même, dans certains Etats membres, la procédure d'approbation de BCR ou de clauses

169. G29, « Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 », WP 114, 25 novembre 2005, p. 8.
170. *Ibid.*, p. 8 et 9.
171. Article 26, 1., a), de la directive (art. 49, 1., a), du règlement).
172. Cette notion de nécessité est interprétée de manière très restrictive par le G29: G29, « Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 », *WP 114*, 25 novembre 2005, p. 15 et s.
173. Art. 26, 1., b) et c), de la directive (art. 49, 1., b) et c), du règlement).
174. Le G29 a déjà eu l'occasion de rejeter ce fondement « pour justifier le transfert de données relatives aux passagers des compagnies aériennes aux autorités américaines » car « la nécessité du transfert n'avait pas été établie et (…) il ne paraissait pas acceptable qu'une décision unilatérale d'un pays tiers, pour des raisons d'intérêt public qui lui sont propres, conduise à des transferts réguliers et massifs de données protégées par la directive » et « seuls des intérêts publics importants, définis comme tels par la loi nationale applicable aux responsables du traitement établis dans l'UE [peuvent] être valablement pris en compte dans ce contexte »: G29, « Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 », *WP 114*, 25 novembre 2005, p. 17.
175. Art. 26, 1., d), de la directive (art. 49, 1., d) et e), du règlement).
176. Art. 26, 1., e), de la directive (art. 49, 1., f), du règlement).
177. Art. 26, 1., f), de la directive (art. 49, 1., g), du règlement).
178. Pour de plus amples informations sur leur interprétation voir considérant 58 de la directive et G29, « Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 », *WP 114*, 25 novembre 2005, p. 17 et s.
179. S. CARRERA et E. GUILD, « Editorial: the end of Safe Harbor: what future for EU-US data transfers? », *M.J.*, 2015/5, p. 654; le G29 précise que, pour que ce consentement soit valable, il faut qu'il s'agisse d'une manifestation de volonté, libre, explicite, spécifique et informée: pour plus de détails voir G29, « Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/CE du 24 octobre 1995 », *WP 114*, 25 novembre 2005, p. 12-14. En outre, l'art. 44, 4., du règlement interdit l'utilisation du consentement de la personne concernée quand il s'agit d'activités poursuivies par les autorités publiques dans le cadre de l'exercice de leurs pouvoirs publics.
180. CONFERENCE OF DATA PROTECTION COMMISSIONNERS (DSK), « DSK Position Paper », www.datenschutz.hessen.de/ft-europa.htm#entry4601, 21 octobre 2015 (consulté le 5 avril 2016), p. 2.
181. COMMISSION EUROPÉENNE, « Communication de la Commission au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire », *Communication COM(2013) 847 final*, 27 novembre 2013, p. 5.

contractuelles[182] est très lourde (en Belgique, cette approbation doit prendre la forme d'un arrêté royal après avis de la Commission de la protection de la vie privée[183]).

63. Cette approbation par les autorités nationales compétentes, qui doivent, selon la Cour dans l'arrêt *Schrems*, pouvoir examiner en toute indépendance si les pays tiers disposent du niveau de protection adéquat[184], est d'ailleurs l'un des nœuds du problème actuel. En effet, là où la Grande-Bretagne estime que la fin du *Safe Harbor* ne change pas fondamentalement la donnée[185], les autorités allemandes de protection des données ont décidé que ni les clauses contractuelles ni des BCR ne pourraient remplacer le *Safe Harbor* et qu'elles ne délivreraient aucune nouvelle autorisation à cet égard[186] car les problèmes pointés du doigt par la Cour existent également en cas de clauses contractuelles ou de BCR (les agences nationales de renseignement peuvent également accéder à des données de citoyens européens transmises via ces mécanismes)[187]. De même, suite à la modification de la plainte de Schrems, qui ne porte désormais plus sur le *Safe Harbor* mais sur les clauses contractuelles standards adoptées par la Commission et utilisées par Facebook pour certains transferts, l'autorité irlandaise de protection des données estime qu'il faut interroger la Cour de justice sur leur légalité[188].

64. Il reste donc aux entreprises une marge de manœuvre variant selon les autorités de contrôle auxquelles elles ont affaire. L'Allemagne semble être à l'avant-garde de la protection des données à caractère personnel[189], suivie de près par la France notamment, qui n'a pas hésité à lancer des ultimatums à Facebook[190], ainsi que la Belgique dont l'autorité nationale de contrôle tente de combattre certaines politiques utilisées par Facebook[191], tandis que les autorités anglaises sont bien moins alarmistes[192,193].

182. Sauf les clauses contractuelles types de la Commission, directement applicables en droit belge sans mesures d'exécution: art. 10 protocole d'accord relatif aux clauses contractuelles entre le SPF Justice et la Commission de la protection de la vie privée, www.privacycommission.be/protocole-contrats-SPF-Justice-CPVP.pdf, 25 juin 2013, tel que modifié par *erratum* du 10 juin 2014 (consulté le 5 avril 2016). Nous nous permettons néanmoins de douter de cette application directe suite à l'arrêt *Schrems*.

183. Art. 22 de la loi du 8 décembre 1992; art. 11 protocole d'accord relatif aux clauses contractuelles entre le SPF Justice et la Commission de la protection de la vie privée, www.privacycommission.be/protocole-contrats-SPF-Justice-CPVP.pdf, 25 juin 2013, tel que modifié par *erratum* du 10 juin 2014 (consulté le 5 avril 2016); art. 32 et 33 protocole d'accord relatif aux règles d'entreprise contraignantes entre le SPF Justice et la Commission de la protection de la vie privée, www.privacycommission.be/protocole-bcr-cpvp-spf-justice_1.pdf, 13 juillet 2011 (consulté le 5 avril 2016); K. ROSIER, « Gestion et protection des données à caractère personnel dans la relation de travail », *o.c.*, p. 101.

184. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 57; CONFERENCE OF DATA PROTECTION COMMISSIONNERS (DSK), « DSK Position Paper », www.datenschutz.hessen.de/ft-europa.htm#entry4601, 21 octobre 2015 (consulté le 5 avril 2016), p. 1.

185. INFORMATION COMMISSIONER OFFICE, « Data transfers to the US and Safe Harbor – interim guidance », www.ico.org.uk/media/for-organisations/documents/1560653/data-transfers-to-the-us-and-safe-harbor-interim-guidance.pdf, 10 février 2016.

186. CONFERENCE OF DATA PROTECTION COMMISSIONNERS (DSK), « DSK Position Paper », www.datenschutz.hessen.de/ft-europa.htm#entry4601, 21 octobre 2015 (consulté le 5 avril 2016), p. 1; P. VALCKE, « VS niet langer een veilige haven voor uw persoonsgegevens », *R.W.*, 2015-2016, p. 522; S. CARRERA et E. GUILD, *o.c.*, p. 654.

187. J.P. MELTZER, *o.c.*

188. HIGH COURT OF IRELAND, 19 juillet 2016, *Data Protection Commissioner / Facebook Ireland Limited and Maximilian Schrems*, Case No. 2016/4809P, www.politico.eu/wp-content/uploads/2016/07/DPC-v.-Facebook-Final.pdf (consulté le 29 août 2016), p. 2-3. Il est à noter que cette décision ne vise pas à régler le sort même d'une possible question préjudicielle à la Cour de justice de l'Union mais se contente de préciser que la Cour Suprême irlandaise accepte d'entendre en tant qu' *amicus curiae*. La décision concernant un possible renvoi devant la Cour de justice n'est prévue que pour février 2017: K. LILLINGTON, « Watchdog takes bizarre legal route in data privacy case », *The Irish Times*, 28 juillet 2016 (consulté le 30 août 2016).

189. Comme en témoigne encore tout récemment l'opinion donnée par l'autorité de protection des données d'Hambourg (D. MEYER, *o.c.*) ou les amendes qu'elle a prononcées à l'encontre de trois entreprises qui utilisaient encore le *Safe Harbor* 6 mois après son annulation (C. PILTZ, « Hamburg Data Protection Watchdog Fines International Companies For Illegal Data Transfers », www.delegedata.de/2016/06/hamburg-data-protection-watchdog-fines-international-companies-for-illegal-data-transfers (consulté le 29 août 2016), 6 juin 2016).

190. CNIL, « Décision n° 2016-007 du 26 janvier 2016 mettant en demeure les sociétés FACEBOOK INC. et FACEBOOK IRELAND », www.cnil.fr/sites/default/files/atoms/files/d2016-007_med_facebook-inc-ireland.pdf (consulté le 5 avril 2016); CNIL, « La CNIL met publiquement en demeure FACEBOOK de se conformer, dans un délai de 3 mois, à la loi Informatique et Libertés », www.cnil.fr/fr/la-cnil-met-publiquement-en-demeure-facebook-de-se-conformer-dans-un-delai-de-trois-mois-la-loi, 9 février 2016 (consulté le 5 avril 2016).

191. Prés. Trib. Bruxelles, 9 novembre 2015, R.G. n° 2015/57/C, www.privacycommission.be/sites/privacycommission/files/documents/vonnis_fr.pdf; le Groupe de contact, créé au niveau européen suite à la révision par Facebook de ses conditions d'utilisation annoncées le 13 novembre 2014, dont fait partie la Belgique (avec la France, l'Espagne, les Pays-Bas et Hambourg) a ensuite demandé à Facebook de se conformer à ce jugement sur l'ensemble du territoire de l'Union européenne: « Déclaration commune des autorités de protection des données personnelles membres du Groupe de contact (Pays-Bas, France, Espagne, Hambourg et Belgique) », www.cnil.fr/Declaration_commune_Groupe_de_contact_Facebook.pdf, 4 décembre 2015 (consulté le 5 avril 2016). Ce jugement a cependant été réformé en appel mais sur base de questions procédurales, ce qui ne met donc pas fin au débat ni à la procédure au fond qui démarrera en 2017: COMMISSION DE LA PROTECTION DE LA VIE PRIVÉE, « La cour d'appel rejette les arguments contre Facebook », *Communiqué de presse*, www.privacycommission.be/fr/news/la-cour-dappel-rejette-les-arguments-contre-facebook, 30 juin 2016 (consulté le 30 août 2016); L. CO/BELGA, « Facebook gagne la bataille sur la vie privée en Belgique », *Le Soir*, 29 juin 2016 (consulté le 30 août 2016).

192. INFORMATION COMMISSIONER OFFICE, « Data transfers to the US and Safe Harbor – interim guidance », www.ico.org.uk/media/for-organisations/documents/1560653/data-transfers-to-the-us-and-safe-harbor-interim-guidance.pdf, 10 février 2016.

193. Pour d'autres différences entre les autorités nationales de contrôle, voir notamment: AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE, *La protection des données à caractère personnel dans l'Union européenne: le rôle des autorités nationales chargées de la protection des données*, 2010.

65. Le vœu de la Commission, partagé par le G29, d'une application uniforme de l'arrêt *Schrems* et du droit européen semble bien loin[194]. Seul le futur pourra désormais nous dire si ces différences sont vouées à disparaître rapidement par le biais du nouvel accord avec les Etats-Unis et/ou par le biais du nouveau règlement de manière générale ou si cela donnera naissance à une nouvelle forme de « forum shopping » pour les entreprises qui désirent s'établir en Europe.

2.3. L'ultimatum du Groupe 29: un jeu dangereux

66. Suite à l'arrêt *Schrems*, le G29 n'a pas tardé à réagir en demandant de toute urgence aux Etats membres et aux institutions européennes de négocier avec les Etats-Unis pour qu'un nouvel accord soit mis en place[195]. A cet égard, le G29, composé, pour rappel, des autorités de contrôle de chaque Etat membre, n'a pas hésité à poser comme deadline la fin du mois de janvier 2016. A défaut, le groupe prévient que les autorités nationales de contrôle s'engagent à prendre toutes les actions nécessaires et appropriées, y compris, le cas échéant, des mesures répressives coordonnées[196].

67. Bien que certains Etats ne semblent pas prêts à aller aussi loin[197], cette menace a été entendue par la Commission qui a négocié de manière assez rapide la conclusion d'un nouvel accord avec les Etats-Unis. L'arrêt de la Cour et l'ultimatum posé par le G29 semblent avoir donné l'impulsion manquante pour que le nouvel accord soit acté puisqu'avant cela des négociations étaient en cours depuis 2 ans mais n'avaient jamais abouti[198]. Notons qu'à défaut de respecter cet ultimatum, il est fort probable que certaines autorités nationales de contrôle auraient fait pression par d'autres ultimatums, si ce ne sont des actions, à l'encontre des entreprises concernées qui, à leur tour, auraient sollicité les institutions européennes[199], ce qui se faisait déjà en partie via des lettres ouvertes d'organisations touchées par la fin du *Safe Harbor* [200].

68. L'accord politique fut ainsi annoncé le 2 février 2016[201], soit seulement quelques jours après la deadline, mais les divers textes de l'accord en tant que tel, baptisé « *Privacy Shield* », n'ont été fournis que le 29 février 2016 par la Commission[202], suite à une autre deadline imposée par le G29[203].

69. Ce calendrier pousse certains à dire que la Commission a affirmé l'existence d'un accord pour respecter la deadline et s'est ainsi piégée elle-même vis-à-vis des Etats-Unis qui ont finalement pu se contenter d'attendre la fin du délai fixé par le G29 pour imposer leurs vues[204]. L'Union semblait pourtant en position de force suite à l'arrêt de la Cour[205] qui exprimait un point de vue fort sur l'accès aux données par les autorités américaines, accès qui semblait être le problème bloquant les négociations entamées entre la Commission et les Etats-Unis[206].

70. Cette rapidité peut néanmoins également se comprendre au vu de la position prise par la Commission d'affirmer que l'arrêt *Schrems* a « confirmé l'approche adoptée par la Commission depuis novembre 2013 »[207]. Si cet arrêt n'est qu'une confirmation et que les travaux ont déjà débuté, 3 mois étaient peut-être amplement suffisants pour finaliser un accord.

194. COMMISSION EUROPÉENNE, « La Commission publie des orientations sur les transferts transatlantiques de données et appelle à définir rapidement un nouveau cadre à la suite de l'arrêt rendu dans l'affaire *Schrems* », *Communiqué de presse IP/15/6015*, 6 novembre 2015, p. 1; COMMISSION EUROPÉENNE, « Questions et réponses: orientations sur les transferts transatlantiques de données, à la suite de l'arrêt *Schrems* », *Fiche d'information MEMO/15/6014*, 6 novembre 2015, p. 2; G29, « Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14) », *Communiqué de presse*, 16 octobre 2015, p. 1.

195. G29, « Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14) », *Communiqué de presse*, 16 octobre 2015, p. 1.

196. *Ibid.*; E. WÉRY et T. LÉONARD, « Données personnelles: le nouveau cadre juridique est attendu d'urgence », *Droit & Technologies*, 21 octobre 2015 (consulté le 23 mars 2016).

197. En témoignent les mots mesurés de l'autorité anglaise de contrôle dans son guide aux entreprises suite à l'invalidation du régime *Safe Harbor*: INFORMATION COMMISSIONER OFFICE, « Data transfers to the US and Safe Harbor – interim guidance », www.ico.org.uk/media/for-organisations/documents/1560653/data-transfers-to-the-us-and-safe-harbor-interim-guidance.pdf, 10 février 2016.

198. COMITÉ DES LIBERTÉS CIVILE, DE LA JUSTICE et DES AFFAIRES INTÉRIEURES (PARLEMENT EUROPÉEN),« Draft programme – Hearing: the nex EU-US Privacy Shield for commercial transfers of EU personal data to the US », *LIBE_OJ(2016)0317-1*, 17 mars 2016, p. 2; A. JENNOTE, « Pourquoi le Privacy shield est un bouclier bien trop frêle pour la vie privée des Européens », *o.c.*, p. 1.

199. Le rôle des pressions d'acteurs non étatiques est relevé par de nombreux auteurs, notamment: N. PURTOVA, *o.c.*, p. 204-221 et les nombreux auteurs cités; E. WÉRY et T. LÉONARD, « Données personnelles: le nouveau cadre juridique est attendu d'urgence », *o.c.*

200. US CHAMBER OF COMMERCE, « U.S. and European Business Groups Urge Agreement on Data Flows », www.uschamber.com/letter/us-and-european-business-groups-urge-agreement-data-flows, 19 janvier 2016 (consulté le 9 avril 2016), citant notamment DigitalEurope et l'Information Technology Industry Council.

201. « The new transatlantic data 'Privacy Shield': The Economist explains », *The Economist (Online)*, 3 février 2016.

202. COMMISSION EUROPÉENNE, « La Commission européenne présente le paquet 'bouclier de protection des données UE-Etats-Unis': des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données », *Communiqué de presse*, 29 février 2016.

203. G29, « Statement of the Article 29 Working Party on the consequences of the Schrems judgment », *Communiqué de presse*, 3 février 2016, p. 2.

204. J. MCNAMEE, directeur exécutif d'Edri (plateforme d'associations pour la défense des droits civils numériques), cité par A. JENNOTE, « Pourquoi le Privacy shield est un bouclier bien trop frêle pour la vie privée des Européens », *o.c.*, p. 3.

205. S. PEYROU, *o.c.*, p. 397; A. JENNOTE, « Le flou juridique après l'arrêt '*Facebook*' », *Le Soir*, 29 janvier 2016.

206. L. BEDNAROVA, « Vera Jourova: We will be strict with the US on Safe Harbour », *Euractiv.com*, 13 mars 2015 (mise à jour le 15 octobre 2015).

207. COMMISSION EUROPÉENNE, « Questions et réponses: orientations sur les transferts transatlantiques de données, à la suite de l'arrêt *Schrems* », *Fiche d'information MEMO/15/6014*, 6 novembre 2015, p. 2.

SECTION 3. UNE LUMIÈRE AU BOUT DU TUNNEL?

« *Si l'Europe parvient à mettre en place un régime juridique équilibré de protection des données à caractère personnel, elle deviendrait attractive pour les géants du web.* »[208].

3.1. Le *Privacy Shield*, laisser Big Brother agir en toute liberté?

71. « Tout nouvel accord devra satisfaire aux exigences énoncées dans l'arrêt de la Cour. »[209]. La Commission ne pouvait pas être plus claire sur le niveau de protection qui se doit d'être atteint dans tout futur accord entre l'Union et un pays tiers concernant les données personnelles.

72. Celui qui nous concerne a reçu une dénomination imagée: « bouclier de protection des données UE-Etats-Unis »[210]. Mais qui ou que ce bouclier protège-t-il? Les données des citoyens européens contre les intrusions constantes des agences de renseignement américaines? Les entreprises américaines des conséquences inévitables des programmes de surveillance de masse existant aux Etats-Unis[211]? La question reste ouverte. Ce bouclier, dévoilé en février 2016, les Etats-Unis ont contribué à le créer puisqu'il est le fruit du nouvel accord avec l'Union européenne concernant les transferts de données. Il comprend des « Privacy Shield Principles », rappelant les « Safe Harbor Principles », ainsi que divers documents annexés[212] (ci-après le « *Privacy Shield* »).

73. Les discussions concernant cet accord sont en réalité bien plus anciennes que 2016 ou que l'arrêt *Schrems* puisqu'elles ont débuté suite aux révélations de Snowden en 2013[213]. Snowden n'a en effet (et heureusement!) pas secoué que le seul Schrems. Néanmoins, la Commission fut bien lente à réagir et malgré des recommandations formulées en 2013 et des discussions lancées en 2014 avec les Etats-Unis[214], elle n'aura adopté aucune nouvelle décision avant que la Cour ne se charge de lui rappeler, durement, que la réalité américaine ne correspond pas à la législation européenne.

74. Pour savoir si le nouvel accord risque ou non d'être, à son tour, invalidé par la Cour, il faut se remémorer les critiques de cette dernière vis-à-vis du protocole *Safe Harbor*: le *Privacy Shield* répond-il aux exigences de la Cour telles que nous les avons précédemment énoncées, le niveau de protection est-il équivalent à celui prévu par le droit de l'Union[215]? Les changements apportés répondent-ils aux critiques ou sont-ils « purement cosmétiques »[216]?

75. Quatre changements principaux doivent être mentionnés[217].

76. Premièrement, sans critique de la Cour à ce sujet, les négociateurs européens et américains ont décidé de rester sur un système d'autocertification ouvert aux entreprises volontaires[218] et ce probablement pour ne pas devoir entreprendre une modification plus fondamentale de la législation américaine en la matière. Des mécanismes plus stricts de supervision sont cependant prévus pour contrôler ces entreprises (rappelons-nous que certaines entreprises étaient certifiées sous le système *Safe Harbor* alors même qu'elles n'en respectaient pas les principes), y compris la possibilité de les sanctionner ou de les exclure du système[219]. A cet égard, le

208. A. DESFORGES, « Les stratégies européennes dans le cyberspace », *Droits et souveraineté numérique en Europe*, Bruxelles, Bruylant, 2016, p. 85.
209. COMMISSION EUROPÉENNE, « La Commission publie des orientations sur les transferts transatlantiques de données et appelle à définir rapidement un nouveau cadre à la suite de l'arrêt rendu dans l'affaire *Schrems* », *Communiqué de presse IP/15/6015*, 6 novembre 2015, p. 1.
210. Ci-après nous parlerons du « Privacy Shield », nom anglais de la décision, plus usité et qui a notre préférence.
211. D. O'BRIEN et R. REITMAN, « The Privacy Shield is Riddled With Surveillance Holes », *Electronic Frontier Foundation*, 3 mars 2016.
212. Tels que des « engagements écrits du gouvernement américain concernant la mise en œuvre du dispositif, y compris des assurances sur les garanties et les conditions d'accès des pouvoirs publics aux données »: COMMISSION EUROPÉENNE,« La Commission européenne présente le paquet 'bouclier de protection des données UE-Etats-Unis': des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données », *Communiqué de presse IP/16/433*, 29 février 2016, p. 1; annexes I à VII, décision d'exécution (UE) n° 2016/1250 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.U.E.*, L. 207, 1er août 2016, p. 1 et s.
213. COMMISSION EUROPEENNE, « Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (*Schrems*) », *Communication COM(2015) 566 final*, 6 novembre 2015, p. 3.
214. *Ibid.*; J.P. MELTZER, *o.c.*
215. S. CARRERA et E. GUILD, *o.c.*, p. 655; N.N. LOIDEAN, *o.c.*, p. 13.
216. Formulation utilisée par le député européen allemand JAN PHILIPP ALBRECHT: A. JENNOTE, « Pourquoi le Privacy shield est un bouclier bien trop frêle pour la vie privée des Européens », *o.c.*
217. COMMISSION EUROPEENNE, « Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (*Schrems*) », *Communication COM(2015) 566 final*, 6 novembre 2015, p. 9 et 10; COMMISSION EUROPEENNE, « European Commission launches EU-U.S. Privacy Shield: stronger protection for transatlantic data flows », *Communiqué de presse IP/16/2461*, 12 juillet 2016, p. 1.
218. Considérants 14 et s. et annexe II, section III.6, décision d'exécution (UE) n° 2016/1250 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.U.E.*, L. 207, 1er août 2016, p. 1 et s.
219. COMMISSION EUROPÉENNE, « La Commission européenne présente le paquet 'bouclier de protection des données UE-Etats-Unis': des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données », *Communiqué de presse IP/16/433*, 29 février 2016, p. 2.

G29 se demande cependant quels sont les pouvoirs exacts des autorités américaines pour contrôler les organisations autocertifiées et enquêter sur les violations du *Privacy Shield*[220].

77. Ensuite, il semblerait qu'au niveau des garanties procédurales offertes aux personnes dont les données sont concernées par un transfert, des efforts ont été mis en place, notamment par la possibilité pour ces personnes de s'adresser à leur autorité nationale de contrôle[221], par l'adoption d'une législation américaine ouvrant les recours judiciaires aux citoyens européens en cas de traitement de leurs données (Judicial Redress Act)[222] ainsi que par la création d'un service de médiation (« ombudsperson ») pour permettre un recours des citoyens européens en matière de plaintes et demandes d'informations concernant les services de renseignement américains[223].

78. A cet égard, le G29 estime que, bien qu'on puisse observer une amélioration, l'architecture des recours offerts aux individus est bien trop complexe et les recours possibles trop nombreux[224], ce qui risque de ne pas satisfaire l'exigence de l'existence d'un mécanisme de recours efficace pour les individus[225]. De même, le G29 doute de l'indépendance et de l'efficacité de l'ombudsperson[226] (qui n'a par ailleurs pas encore été nommée malgré l'entrée en vigueur du *Privacy Shield* le 1er août dernier).

79. Troisièmement, la critique de la Cour visant l'absence de révision et de contrôle du système *Safe Harbor* semble avoir été entendue puisqu'un mécanisme de réexamen annuel est mis en place[227] avec la possibilité d'une suspension du régime le cas échéant. Il faudra cependant voir en pratique si ces mécanismes seront ensuite appliqués puisque la décision *Safe Harbor* prévoyait également à l'époque un examen régulier et une suspension possible[228], ce qui ne fut pas suivi d'effets, la Commission ayant seulement émis des recommandations en 2002, 2004 et 2013 et aucune suspension n'ayant eu lieu malgré les révélations de Snowden[229]. Le G29 a d'ailleurs demandé des précisions sur ce mécanisme et désirait que les parties s'accordent sur ses modalités à l'avance[230], craignant sans doute qu'en l'absence de telles précisions, le mécanisme finisse dans les mêmes oubliettes que le mécanisme prévu par la décision *Safe Harbor*.

80. Enfin, du point de vue de l'accès généralisé aux données par les autorités américaines, l'accord prête le flanc à la critique car il ne rencontre pas les exigences posées par la Cour. En effet, bien que les Etats-Unis se soient engagés à s'abstenir d'un accès non ciblé ou de masse aux données européennes stockées sur leur territoire[231], cet engagement est constellé d'exceptions. La Commission présente cet engagement comme l'une des améliorations majeures obtenues par l'Union mais il faut le replacer dans son contexte: suite aux révélations de Snowden, Barack Obama avait fait publier une directive présidentielle pour encadrer les activités de renseignement, directive prévoyant que la collecte de données par ces services doit être ciblée[232]. L'engagement des Etats-Unis envers l'Union n'est donc qu'une simple copie de cette directive datant de janvier 2014 et non une avancée extraordinaire comme semble le clamer la Commission. L'application de cette directive, citée dans l'annexe VI du *Privacy Shield*, démontre, et c'est là que le bât blesse, que le principe d'absence de collecte massive de données s'accompagne en fait de six exceptions libellées dans des termes tellement larges (notamment cybersécurité, lutte contre

220. G29, « Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision », *WP 238*, 13 avril 2016, p. 30.
221. *Ibid.*, p. 1; COMMISSION EUROPÉENNE, « Le 'bouclier de protection des données UE-Etats-Unis': foire aux questions », *Fiche d'information MEMO/16/434*, 29 février 2016, p. 1.
222. Judicial Redress Act of 2015, Public Law 114-126, www.congress.gov/114/plaws/publ126/PLAW-114publ126.pdf, 24 février 2016; COMMISSION EUROPÉENNE, « La Commission européenne présente le paquet 'bouclier de protection des données UE-Etats-Unis': des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données », *Communiqué de presse IP/16/433*, 29 février 2016, p. 1.
223. COMMISSION EUROPÉENNE, « La Commission européenne présente le paquet 'bouclier de protection des données UE-Etats-Unis': des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données », *Communiqué de presse IP/16/433*, 29 février 2016, p. 2.
224. En effet, il est possible de s'adresser à l'organisation qui utilise les données de l'individu en question mais aussi de s'adresser notamment à la Federal Trade Commission, à une autorité nationale européenne de contrôle, à un panel d'arbitres ou à une ombudsperson (par contre, il n'existe aucune possibilité d'agir directement devant les juridictions compétentes des Etats membres de l'Union): G29, « Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision », *WP 238*, 13 avril 2016, p. 27.
225. *Ibid.*, p. 3, 26, 27 et 43; art. 47 de la charte des droits fondamentaux de l'Union européenne.
226. *Ibid.*, p. 4 et 45-51.
227. COMMISSION EUROPÉENNE, « La Commission européenne présente le paquet 'bouclier de protection des données UE-Etast-Unis': des garanties solides pour restaurer la confiance dans les transferts transatlantiques de données », *Communiqué de presse IP/16/433*, 29 février 2016, p. 2.
228. Art. 3, 4. et 4, décision (CE) n° 2000/520 de la Commission du 26 juillet 2000.
229. PARLEMENT EUROPÉEN, « Résolution sur le programme de surveillance de la NSA, les organismes de surveillance dans divers Etats membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures (2013/2188(INI)) », *P7_TA(2014)0230*, 12 mars 2014, p. 12 et 13; « 'Privacy Shield': ne sacrifions pas nos droits sur 'l'autel du pragmatisme'! », *Association européenne pour la défense des Droits de l'Homme*, www.aedh.eu/Privacy-Shield-ne-sacrifions-pas.html (consulté le 10 avril 2016).
230. G29, « Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision », *WP 238*, 13 avril 2016, p. 4, 14 et 15.
231. COMMISSION EUROPÉENNE, « Le 'bouclier de protection des données UE-Etats-Unis': foire aux questions », *Fiche d'information MEMO/16/434*, 29 février 2016, p. 3.
232. Directive présidentielle n° 28 (PPD-28), www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities, 17 janvier 2014; COMMISSION EUROPÉENNE, « Le 'bouclier de protection des données UE-Etats-Unis': foire aux questions », *Fiche d'information MEMO/16/434*, 29 février 2016, p. 4.

le terrorisme, menaces criminelles transnationales, détection et neutralisation de certaines activités menées par des puissances étrangères[233]) qu'en pratique les autorités américaines auront accès de manière généralisée aux données quand elles le désirent[234], ce que la Cour avait expressément condamné[235], de même que le G29 qui le répète dans son avis concernant tout spécialement le *Privacy Shield*[236].

81. Le G29 souligne également que le *Privacy Shield* manque de clarté et de cohérence au niveau du langage et de la terminologie usités[237] et que certains principes fondamentaux du droit européen de protection des données ne sont pas explicitement prévus[238].

82. De manière peu surprenante, les acteurs concernés du côté européen ne sont globalement pas convaincus par le nouvel accord, contrairement aux acteurs américains qui réagissent de manière plus positive[239]. Cela se comprend aisément: les acteurs européens concernés voient leurs droits fondamentaux bafoués tandis que les acteurs américains concernés désirent qu'un nouvel accord soit mis en place pour pallier l'insécurité actuelle. Les entreprises accueillent plutôt bien ce nouvel accord[240] qui les libère d'une position difficile puisque nous avons pu démontrer à quel point les autres fondements pour réaliser des transferts sont remplis d'incertitudes.

83. M. Schrems, parmi d'autres[241], a critiqué ce nouvel accord et estime que, malgré de nombreuses améliorations, cet accord ne répond pas aux critiques principales de la Cour[242]. Le Parlement européen partage cette opinion[243] et le G29 a, malgré les commentaires parfois positifs dans son avis sur le *Privacy Shield*, confirmé cela[244]. Son avis n'a d'ailleurs plus été sollicité suite aux quelques changements minimes adoptés par la Commission durant les mois de mai et juin avant l'adoption définitive du texte le 12 juillet dernier[245]. Le G29 a néanmoins spontanément donné son avis fin juillet pour prévenir que tous les problèmes n'étaient pas réglés mais qu'ils laisseraient le *Privacy Shield* « vivre » durant une année avant de revenir à la charge[246]. La Cour pourrait également confirmer la position du G29 quand elle sera amenée à se prononcer sur ce nouvel accord, ce qui ne saurait tarder puisque des requêtes en annulation ont été

233. Annexe VI, décision d'exécution (UE) n° 2016/1250 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.U.E.*, L. 207, 1er août 2016, p. 1 et s.; COMMISSION EUROPÉENNE,« Le 'bouclier de protection des données UE-Etats-Unis': foire aux questions », *Fiche d'information MEMO/16/434*, 29 février 2016, p. 4; A. JENNOTE, « Pourquoi le Privacy shield est un bouclier bien trop frêle pour la vie privée des Européens », *o.c.*

234. A. JENNOTE, « Pourquoi le Privacy shield est un bouclier bien trop frêle pour la vie privée des Européens », *o.c.*; EUROPE VERSUS FACEBOOK, « European Commission presents EU-US 'Privacy Shield' », www.europe-v-facebook.org/PA_PS.pdf, V1.3, 29 février 2016, p. 1.

235. C.J.U.E., 6 octobre 2015, C-362/14, *Maximillian Schrems / Data Protection Commissioner*, ECLI:EU:C:2015:650, point 94.

236. G29, « Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision », *WP 238*, 13 avril 2016, p. 4, 11, 12 et 34-40.

237. *Ibid.*, p. 2 et 12-14.

238. Ainsi, les transferts subséquents depuis des organisations soumises aux principes *Privacy Shield* ne sont pas suffisamment réglementés et ni le principe de limitation de la durée de conservation des données, ni l'obligation de supprimer les données une fois qu'elles ne sont plus nécessaires pour réaliser le but pour lequel elles ont été collectées ne sont prévus: G29, « Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision », *WP 238*, 13 avril 2016, p. 3, 17, 20, 21, 57 et 58.

239. S. TRENDALL, « Paranoid and Void? », *Channelweb.co.uk*, 22 février 2016, p. 6 et 7.

240. DIGITALEUROPE, « John Higgins' speech delivered at LIBE Public Hearing on #PrivacyShield », www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2141&PortalId=0&TabId=353, 17 mars 2016 (consulté le 1er avril 2016), p. 2; INFORMATION TECHNOLOGY INDUSTRY COUNCIL, « ITI Welcomes Public Release of Text of EU-U.S. Privacy Shield », www.itic.org/news-events/news-releases/iti-welcomes-public-release-of-text-of-eu-u-s-privacy-shield, 29 février 2016.

241. S. TRENDALL, *o.c.*, p. 6 et 7; C. STUPP, « Commission wants EU-US Privacy Shield by end of June », *Euractiv.com*, 29 février 2016 (mise à jour le 1er mars 2016); D. O'BRIEN et R. REITMAN, « The Privacy Shield is Riddled With Surveillance Holes », *Electronic Frontier Foundation*, 3 mars 2016; lettre d'une coalition d'associations telles que Access Now, American Civil Liberties Union, Amnesty International USA, *Digital Rights Ireland*, Electronic Frontier Foundation ou European Digital Rights, à Isabelle Falque-Pierrotin (présidente du G29), Claude Moraes (président de la Commission LIBE) et Pieter de Gooier (ambassadeur et représentant permanent des Pays-Bas auprès de l'Union européenne), www.edri.org/wp-content/uploads/2016/03/PrivacyShield_Letter_Coalition_March2016.pdf, 16 mars 2016; « 'Privacy Shield': ne sacrifions pas nos droits sur 'l'autel du pragmatisme'! », *Association européenne pour la défense des Droits de l'Homme*, www.aedh.eu/Privacy-Shield-ne-sacrifions-pas.html (consulté le 10 avril 2016).

242. N. LOMAS, « Draft Text of EU-U.S. Privacy Shield Deal Fails to Impress the Man Who Slayed Safe Harbor », www.techcrunch.com/2016/02/29/lipstick-on-a-pig, 29 février 2016. Il est à noter cependant que, si la Cour est amenée à se prononcer, elle pourrait devoir examiner le droit américain en lui-même lors d'un recours éventuel contre le *Privacy Shield*, ce qu'elle n'a pas dû faire pour le *Safe Harbor*: S. CRESPI, « La nouvelle décision d'adéquation (*Privacy Shield*) pour les transferts des données personnelles de l'Union européenne vers les Etats-Unis », *J.D.E.*, 2016, p. 262.

243. PARLEMENT EUROPEEN, « EU-US 'Privacy Shield' for data transfers: further improvements needed, MEPs say », *Communiqué de presse 20160524IPR28820*, 26 mai 2016.

244. G29, « Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision », *WP 238*, 13 avril 2016, p. 2, 33, 57 et 58. En outre, le G29 précise que de nouveaux problèmes pourraient encore être découverts car elle n'a disposé que d'un timing assez restreint pour se prononcer et a pu manquer certains problèmes: G29, « Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision », *WP 238*, 13 avril 2016, p. 10.

245. Aucun Etat n'a voté à l'encontre du nouveau texte mais 4 Etats (Autriche, Bulgarie, Croatie et Slovénie) se sont abstenus et l'Allemagne et la France, malgré leur accord, ont promis de surveiller sa mise en œuvre: M. REES,« Données personnelles: le Privacy Shield EU-US finalisé, prêt à être attaqué », *NextInpact.com*, 12 juillet 2016 (consulté le 30 août 2016); COUNCIL OF EUROPEAN NATIONAL TOP-LEVEL DOMAIN REGISTRIES, « EU Policy Update – July 2016 », *Centr.org*, 15 juillet 2016 (consulté le 30 août 2016).

246. G29, « Statement on the decision of the European Commission on the EU-U.S. Privacy Shield », *Communiqué de presse*, 26 juillet 2016, p. 1.

déposées devant le Tribunal[247]. Il semble donc que le *Privacy Shield* provoque une levée de boucliers.

84. Les entreprises peuvent adhérer au *Privacy Shield* depuis le 1er août 2016 mais elles doivent rester prudentes puisque sa validité est déjà mise en doute. Les entreprises, à ce stade, bien que réceptrices au nouvel accord, ne sont d'ailleurs pas opposées à une législation plus protectrice des données puisque ce n'est pas tant leur accès aux données qui est critiqué mais plutôt l'accès concédé aux autorités américaines auxquelles ces entreprises sont contraintes de transmettre ces données[248]. Leur désir principal est finalement de disposer de règles claires et précises. Celles qu'il faut convaincre de changer de système à long terme sont donc les autorités américaines, ce qui ne semble pas être chose aisée tant celles-ci tiennent à jouer les Big Brother…[249]

3.2. Le règlement: se rattraper sans avoir à forcer la main des Américains?

85. Le *Privacy Shield* devra, quoiqu'il en soit, être renégocié au moment de l'entrée en vigueur du nouveau règlement en matière de protection des données[250]. L'Union européenne tente en effet depuis plusieurs années de réformer sa législation sur les données à caractère personnel pour assurer un niveau de protection plus élevé[251].

86. La législation actuellement en vigueur date, il est vrai, de 1995 et ne répond donc pas aux exigences de notre ère numérique[252]. Sans s'attarder sur la question de savoir si un jour une législation pourra être considérée comme « à jour » tant les progrès technologiques actuels avancent à une vitesse phénoménale, nous allons voir quels changements cette nouvelle réglementation apporte en matière de transferts internationaux de données et en quoi cela pourrait permettre de cadenasser les transferts vers les Etats-Unis.

87. La nouvelle réglementation se compose de deux instruments: un règlement général sur la protection des données[253] et une directive de protection des données dans le domaine de la coopération policière et judiciaire[254]. Nous nous intéresserons seulement au premier puisque notre étude ne porte que sur les aspects commerciaux de la matière.

88. Le nouveau règlement a fait l'objet d'un accord politique du *triumvirat* européen le 15 décembre 2015, plus de 3 ans après la proposition de règlement formulée par la Commission européenne[255]. Il vient d'être adopté et entrera en vigueur en 2018[256]. La directive actuelle s'appliquera donc jusque-là. De manière générale, ce règlement sera un soulagement pour les entreprises qui n'auront plus qu'à appliquer une législation paneuropéenne unique et non les diverses transpositions en droit national de la directive actuelle[257].

---

247. TUE, affaire pendante, *Digital Rights Ireland / Commission*, T-670/16; TUE, affaire pendante, *La Quadrature du Net e.a. / Commission*, T-738/16; P. SAYER, « L'accord Privacy Shield pris en tenaille par 2 actions judiciaires », *LeMondeInformatique.fr*, 4 novembre 2016. En outre, la Cour vient tout juste de rendre une décision à l'encontre de l'accès généralisé indifférencié à des données personnelles, ce qui confirme une fois de plus sa volonté de protéger celles-ci: CJUE 21 décembre 2016, *Tele2 Sverige AB / Post- och telestyrelsen* et *Secretary of State for the Home Department / David Davis, Tom Watson, Peter Brice et Geoffrey Lewis*, C-203/15 et C-698/15, ECLI:EU:C:2016:572 ; G29, « Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision », *WP 238*, 13 avril 2016, p. 39; D. VERHAEGHE, « (Data) privacy waarborgen bij toepassing van 'Big Data', 'Data mining' en 'profilering' in de financiële sector », *R.B.F.*, 2016/2, p. 150; E. WERY, « Les Etats ne peuvent pas imposer une obligation générale de conservation de données », *Droit & Technologies*, 21 décembre 2016.

248. A. DESFORGES, *o.c.*, p. 85; D. FILIPPONE, « Microsoft refuse de fournir certaines données clients au gouvernement US », *LeMondeInformatique.fr*, 4 septembre 2015; J. RIBEIRO, « Google, Facebook et Microsoft prêts à soutenir Apple face au FBI », *LeMondeInformatique.fr*, 26 février 2016; D. FILIPPONE, « La situation s'envenime entre Apple et le ministère de la Justice US », *LeMondeInformatique.fr*, 11 mars 2016.

249. Cette conclusion est d'autant plus vraie depuis que M. Trump a été élu président des Etats-Unis. Ce dernier a en effet déjà adopté un Executive Order diminuant les droits à la vie privée de citoyens qui ne sont ni américains, ni résidents de longue durée, face aux agences de renseignement américaines: Section 14, Executive Order: Enhancing Public Safety in the Interior of the United States, 25 janvier 2017.

250. G29, « Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision », *WP 238*, 13 avril 2016, p. 3 et 15.

251. COMMISSION EUROPÉENNE, « Protection des données dans l'UE: l'accord sur la réforme proposée par la Commission va booster le marché unique numérique », *Communiqué de presse IP/15/6321*, 15 décembre 2015, p. 1; T. VAN CANNEYT et G. GOOSSENS, « The general data protection regulation: 10 things company lawyers should know », *Cah. Jur.*, 2016/1, p. 1.

252. R. SCHOEFS, « Witte rook voor nieuwe privacyverordening », *Juriskrant*, 2016 (liv. 321), p. 16.

253. Règlement (UE) n° 2016/679.

254. Directive (UE) n° 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L. 119, 4 mai 2016, p. 89 et s.; COMMISSION EUROPÉENNE, « Communication from the Commission to the European Parliament and the Council – Transatlantic Data Flows: Restoring Trust through Strong Safeguards », *Communication COM(2016) 117 final*, 29 février 2016, p. 4.

255. COMMISSION EUROPÉENNE, « Protection des données dans l'UE: l'accord sur la réforme proposée par la Commission va booster le marché unique numérique », *Communiqué de presse IP/15/6321*, 15 décembre 2015, p. 1.

256. COMMISSION EUROPÉENNE, « Communication from the Commission to the European Parliament and the Council – Transatlantic Data Flows: Restoring Trust through Strong Safeguards », *Communication COM(2016) 117 final*, 29 février 2016, p. 7; COMMISSION EUROPÉENNE, « Reform of EU data protection rules », www.ec.europa.eu/justice/data-protection/reform/index_en.htm, dernière mise à jour le 21 avril 2016 (consulté le 22 avril 2016).

257. Il existe malgré toute une certaine marge de manœuvre des Etats mais sur des points du règlement que nous n'examinons pas ici. Voir: T. VAN CANNEYT et G. GOOSSENS, *o.c.*, p. 1 et 2. Ce nouveau règlement évite aussi d'autres problèmes tels que des conflits de lois ou de juridictions, problèmes qui se sont posés dans l'affaire précitée du 9 novembre 2015 devant le tribunal de première instance de Bruxelles: Prés. Trib. Bruxelles, 9 novembre 2015, R.G. n° 2015/57/C, www.privacycommission.be/vonnis_fr.pdf; S. DE SMEDT, « Belgium – The New Data Protection Hub? », *E.D.P.L.*, 2015, p. 218.

89. Les changements ne sont en revanche pas révolutionnaires en ce qui concerne directement les transferts[258]. Le règlement vise surtout à légaliser des pratiques existantes ou à clarifier certains concepts, par exemple en consacrant expressément le droit à l'oubli numérique existant en principe en pratique depuis l'arrêt *Google Spain*[259,260], en prévoyant expressément l'application de la réglementation européenne aux entreprises non établies sur le territoire de l'Union si elles offrent des biens ou des services à des citoyens européens ou surveillent le comportement d'individus sur ce même territoire[261], en clarifiant l'utilisation des dérogations au principe du niveau de protection adéquat[262] ainsi qu'en précisant les relations entre les entreprises et les autorités de contrôle (principe du guichet unique et suppression des notifications)[263]. Il y a désormais également une mention expresse aux BCR[264] et d'autres instruments de transferts sont créés[265].

90. Les décisions d'adéquation de la Commission seront en outre mieux entourées: le règlement prévoit en effet les éléments à prendre en compte lorsque la Commission veut décider qu'un pays tiers dispose du niveau de protection adéquat et cela comprend l'accès aux données par les autorités du pays en question[266]. Cela permettra sans doute à la Commission de disposer de plus de moyens de pression face aux Etats-Unis puisqu'à défaut de restriction claire dans la décision d'adéquation à l'accès aux données par les autorités américaines, la décision risquera grandement d'être annulée par la Cour voire de ne pas être respectée par les autorités nationales dès l'entrée en vigueur du règlement.

91. L'un des changements qui ne satisfera certainement pas les entreprises est en revanche l'introduction dans le règlement[267] de sanctions administratives qui pourront atteindre 20 millions d'euros ou 4% du chiffre d'affaires mondial annuel de l'entreprise[268] en cas de manquement aux obligations prévues par le règlement[269]. Ce système de sanctions, bien supérieures à ce qui se faisait auparavant[270], pourrait être l'incitant nécessaire pour que des entreprises telles que Google ou Facebook s'exécutent[271]. De même, les mesures prévues par l'article 58, 2., telles que les suspensions de flux de données vers des pays tiers, devraient don-

258. M. MAIRLOT, « Big Data et vie privée: mariage possible? », *D.B.F.-B.F.R.*, 2015, p. 448; pour un détail des changements, voir T. VAN CANNEYT et G. GOOSSENS, *o.c.*, p. 1 et s. et S. PEYROU, « Le nouveau règlement général européen relatif à la protection des données à caractère personnel: un texte à la hauteur de ses ambitions », *R.A.E.-L.E.A.*, 2016/1, p. 103 et s.

259. Art. 17 et considérants 65 et 66 du règlement; COMMISSION EUROPÉENNE,« Questions et réponses: la réforme de la protection des données », *Fiche d'information MEMO/15/6385*, 21 décembre 2015, p. 1; J.-P. GUÉDON, « Renforcement de la protection des données personnelles, *AJ Pénal*, 2016, p. 53.

260. Cette consécration légale permettra peut-être d'éviter à la Cour de justice de l'Union d'être saisie d'un litige concernant ce fameux droit à l'oubli puisque, pas plus tard qu'en avril et mai dernier, les Cours Suprêmes belge et française se sont exprimées sur la question de manières qui peuvent sembler contradictoires et qui jettent dès lors un flou sur la manière dont l'arrêt *Google Spain* doit être interprété: Cass. (1re ch.), 29 avril 2016, C.15.0052.F; Cass. fr. (civ.), 12 mai 2016, 15-17.729; E. WÉRY, « Le droit à l'oubli peut-il aller jusqu'à entraîner la modification des archives de presse? », *Droit & Technologies*, 8 juin 2016.

261. Art. 3 et considérants 23 et 24 du règlement; COMMISSION EUROPÉENNE, « Communication from the Commission to the European Parliament and the Council – Transatlantic Data Flows: Restoring Trust through Strong Safeguards », *Communication COM(2016) 117 final*, 29 février 2016, p. 5; COMMISSION EUROPÉENNE, « Questions et réponses: la réforme de la protection des données », *Fiche d'information MEMO/15/6385*, 21 décembre 2015, p. 3. La Commission ajoute que cela permettra d'éviter des déséquilibres concurrentiels, que l'application de la réglementation à toutes les entreprises agissant auprès des mêmes individus créera des conditions de concurrence homogènes.

262. Art. 49 et considérants 111, 112 et 113 du règlement; COMMISSION EUROPEENNE, « Communication from the Commission to the European Parliament and the Council – Transatlantic Data Flows: Restoring Trust through Strong Safeguards », *Communication COM(2016) 117 final*, 29 février 2016, p. 7.

263. COMMISSION EUROPÉENNE, « Questions et réponses: la réforme de la protection des données », *Fiche d'information MEMO/15/6385*, 21 décembre 2015, p. 3; COMMISSION EUROPÉENNE, « Protection des données dans l'UE: l'accord sur la réforme proposée par la Commission va booster le marché unique numérique », *Communiqué de presse IP/15/6321*, 15 décembre 2015, p. 2; J.-P. GUÉDON, « Renforcement de la protection des données personnelles », *AJ Pénal*, 2016, p. 53; T. VAN CANNEYT et G. GOOSSENS, *o.c.*, p. 6 et 9.

264. Art. 4, 20, 46, 2., b) et 47 et considérants 108 et 110 du règlement; N. PURTOVA, *o.c.*, p. 213.

265. Tels que le code de conduite prévu à l'art. 40 et la certification conforme à l'art. 42: art. 40, 41 et 42 et considérants 77, 98, 99 et 100 du règlement; A. GROSJEAN, *o.c.*, p. 210.

266. Art. 45, 2. et considérants 104 et 105 du règlement; COMMISSION EUROPEENNE, « Communication from the Commission to the European Parliament and the Council – Transatlantic Data Flows: Restoring Trust through Strong Safeguards », *Communication COM(2016) 117 final*, 29 février 2016, p. 6.

267. La directive ne prévoyait pas de sanctions et renvoyait cette responsabilité aux Etats membres (art. 24 de la directive).

268. Sanctions proportionnées au poids économique de l'entreprise, ce qui rappelle le droit de la concurrence avec lequel F. LE BAIL compare le nouveau règlement: F. LE BAIL, « Protection de la vie privée et des données personnelles: l'Europe à l'avant-garde », *New frontiers of antitrust – 2013*, Bruxelles, Bruylant, 2013, p. 108.

269. Art. 83 et considérants 148, 150 et 151 du règlement; COMMISSION EUROPÉENNE, « Communication from the Commission to the European Parliament and the Council – Transatlantic Data Flows: Restoring Trust through Strong Safeguards », *Communication COM(2016) 117 final*, 29 février 2016, p. 5; J.-P. GUÉDON, « Renforcement de la protection des données personnelles », *AJ Pénal*, 2016, p. 53; O. TAMBOU,« La CNIL donne une leçon de droit européen à notre ami américain Facebook », *Dalloz Actualité*, 23 février 2016.

270. A titre d'exemple, les sanctions prévues par le droit belge sont seulement pénales et se limitent à une amende de maximum 100.000 EUR (Chapitre VIII loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5.801 et s.) et les sanctions prévues par le droit français, administratives et pénales, se limitent à une amende de maximum 300.000 EUR (art. 47 et 50 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, disponible sur *legifrance.gouv.fr*), montants manquant d'effet dissuasif.

271. Voir notamment A. VAN DE MEULEBROUCKE, « De algemene verordening gegevensbescherming », *R.W.*, 2015-2016 (liv. 40), p. 1562 qui parle de « game changer ».

ner plus de poids à ce règlement et en permettre une meilleure application pratique[272].

92. Ces sanctions pourront en effet être prises par les autorités nationales de contrôle dont les pouvoirs seront renforcés[273] et, comme nous l'avons vu, certaines d'entre elles sont très actives dans le domaine. Ainsi, dans un futur proche, la mise en demeure lancée par la CNIL pourrait finir par coûter très cher à un géant tel que Facebook[274]. A défaut d'imposer des règles plus protectrices dans l'accord *Privacy Shield*, ces sanctions potentielles pourraient permettre une meilleure protection des données, du moins dans leur utilisation par les entreprises. Les citoyens, ainsi que des organisations ou associations qui œuvrent à la protection des données, pourraient également se retourner contre les entreprises[275].

93. Ainsi, les critères devant être remplis pour qu'un pays soit considéré comme disposant du niveau de protection adéquat et les sanctions mises en place pourraient permettre de limiter les ingérences dans les droits fondamentaux des citoyens européens, que ce soit par les entreprises ou par les agences nationales, et ce sans devoir négocier avec les Etats-Unis ou n'importe quel autre pays tiers puisque ces principes seront inscrits dans le règlement même, applicable à toutes les données à caractère personnel transférées depuis le territoire de l'Union européenne. Tous les acteurs actifs en Europe se devront ainsi de suivre les mêmes règles.

CONCLUSION

« *We need this global approach. Trust in our technologies without borders is at this prize.* »[276].

94. Un bilan peut être tiré à ce stade. En effet, malgré les changements intervenus en 20 ans (qu'ils soient législatifs, technologiques, sécuritaires ou commerciaux), les mêmes critiques reviennent et se répètent. Ces critiques sont émises par tous les acteurs européens, que ce soit le Parlement, la Commission, la Cour de justice, le G29, la doctrine ou les citoyens[277]. Ces critiques, les entreprises américaines commencent petit à petit à s'y rallier pourvu finalement qu'un accord fort soit mis en place pour remplacer l'incertitude actuelle[278]. Ces critiques, l'Union y a finalement mieux répondu dans le règlement que dans l'accord *Privacy Shield* dont l'annulation est déjà demandée[279]. Ce règlement constituera probablement un fondement plus clair à suivre pour les entreprises concernées.

95. En pratique, les étapes par lesquelles il faut passer afin de transférer des données à caractère personnel de manière légale vers les Etats-Unis (ou tout autre pays tiers d'ailleurs) restent, fondamentalement, les mêmes dans la directive et dans le futur règlement[280].

96. En effet, en présence d'un transfert de données à caractère personnel vers un pays tiers[281], suite à la récolte légale des données sur le territoire de l'Union, il faudra d'abord vérifier si ce pays et les circonstances entourant le transfert

272. Art. 58, 2. et considérant 129 du règlement. D'autres sanctions pourront également être prévues par les Etats membres selon l'art. 84 du règlement mais ce n'est pas une nouveauté par rapport à la directive (art. 24).

273. Chapitre VI et considérants 117 et s. du règlement; T. VAN CANNEYT et G. GOOSSENS, *o.c.*, p. 10. Sous l'empire de la directive et surtout des législations nationales la transposant, certaines autorités nationales de contrôle n'ont pas le pouvoir d'imposer des amendes, ce qui est notamment le cas en Belgique ou au Royaume-Uni: AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE, *La protection des données à caractère personnel dans l'Union européenne: le rôle des autorités nationales chargées de la protection des données*, 2010, p. 34.

274. Alors qu'actuellement le montant d'une sanction suivant une mise en demeure en France se limite à 150.000 EUR ou 300.000 EUR en cas de récidive: art. 47 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, disponible sur *legifrance.gouv.fr*.

275. Art. 75, 76 et 77 et considérants 111 et s. du règlement; T. VAN CANNEYT et G. GOOSSENS, *o.c.*, p. 11.

276. Y. POULLET, « Transborder Data Flows and Extraterritoriality: The European Position », *o.c.*, p. 153.

277. Les arrêts *Google Spain* et *Schrems* ont notamment été des initiatives citoyennes. La CNIL a également reçu un nombre record de plaintes en 2015, de 36% supérieur à l'année précédente, ce qui démontre la volonté des citoyens de protéger leurs données: CNIL, *Rapport d'activité 2015*, www.cnil.fr/sites/default/files/atoms/files/cnil-36e_rapport_annuel_2015.pdf, p. 8 et 9.

278. En effet, certaines entreprises tentent, dans l'ère « post-Snowden » de rassurer leurs utilisateurs et tentent de montrer qu'ils sont prêts à avancer dans le sens d'une plus grande protection: A. DESFORGES, *o.c.*, p. 85; D. FILIPPONE, « Microsoft refuse de fournir certaines données clients au gouvernement US », *o.c.*; LE MONDE.FR et AFP, « La justice estime que Microsoft n'a pas à transmettre aux Etats-Unis des données stockées en Europe », *LeMonde.fr*, 14 juillet 2016 (consulté le 30 août 2016); E. WÉRY, « Cloud: l'absence de protection des données en droit américain pourrait bénéficier aux sociétés européennes », *Droit & Technologies*, 27 avril 2016; UNITED STATES DISTRICT COURT (western district of Washington at Seattle), Microsoft Corporation v. The United States Department of Justice, and Loretta Lynch, in her official capacity as Attorney General of the United States, *complaint for declaratory judgment (disponible sur:* www.droit-technologie.org/upload/actuality/doc/1789-1.pdf*)*, 14 avril 2016. *Contra*: P. SATER et S. LEBLAL, « 200 sociétés ont adhéré au Privacy Shield », *LeMondeInformatique.fr*, 26 août 2016 (consulté le 30 août 2016); CNIL, décision n° 2016/058 du 30 juin 2016 mettant en demeure la société Microsoft Corporation, *disponible sur* www.cnil.fr/sites/default/files/atoms/files/2016-058-med_microsoft_corporation.pdf (consulté le 30 août 2016).

279. TUE, affaire pendante, *Digital Rights Ireland c. Commission*, T-670/16; TUE, affaire pendante, *La Quadrature du Net e.a. c. Commission*, T-738/16; P. SAYER, « L'accord Privacy Shield pris en tenaille par 2 actions judiciaires », *LeMondeInformatique.fr*, 4 novembre 2016.

280. S. CRESPI, « La nouvelle décision d'adéquation (*Privacy Shield*) pour les transferts des données personnelles de l'Union européenne vers les Etats-Unis », *J.D.E.*, 2016, p. 259.

281. Il faut donc vérifier s'il s'agit bien d'un « transfert », s'il y a bien des « données à caractère personnel » en jeu et si ce transfert a bien lieu vers « un pays tiers » donc un pays hors Espace économique européen.

démontrent qu'il existe un niveau adéquat de protection pour ces données[282]. Si c'est le cas, le transfert peut alors avoir lieu. Dans le nouveau règlement, des règles plus spécifiques existent pour que la Commission détermine si ce niveau adéquat est atteint ou non, ce qui rendra cette première étape plus aisée à franchir, que ce soit pour la Commission ou pour les autorités nationales de contrôle lorsqu'elles sont saisies d'une plainte à cet égard.

97. Si la protection n'est pas équivalente à celle de l'Union, il faudra vérifier si les parties concernées ont mis en place des garanties adéquates pour protéger ces données (p. ex. des clauses contractuelles, des BCR, ou encore, dans le règlement, un code de conduite ou une certification). A nouveau, si c'est le cas, le transfert pourra avoir lieu[283]. Dans le cas contraire, il reste possible de transférer les données dans le cadre des dérogations légales au principe du niveau adéquat de protection[284], dérogations qui sont mieux explicitées dans le règlement[285].

98. Les décisions de la Commission, telles que la décision *Safe Harbor* et la décision *Privacy Shield*, permettent seulement de s'arrêter à la première étape et d'offrir aux entreprises un cadre général pour transférer des données à un responsable basé aux Etats-Unis. Les clauses contractuelles, les BCR, les exceptions prévues par l'article 26, 1., de la directive (art. 49, 1., du règlement) continuent à exister et sont, selon nous, une toile de fond bien plus prudente à adopter que les décisions précitées dont la première fut invalidée par la Cour qui, petit à petit, dessine les contours du « niveau de protection adéquat » et risque bien d'invalider la seconde si elle n'est pas modifiée.

99. Comme le dit si bien S. Peyrou, « [d]ans un contexte mondialisé où l'échange de données a crû de façon exponentielle, et où l'identité numérique de tout un chacun est exploitée aussi bien par des sociétés multinationales pour des raisons lucratives que par les Etats pour des motifs sécuritaires, le juge européen construit ainsi pas à pas une protection robuste en indiquant les limites à ne pas franchir »[286].

100. Grâce aux arrêts *Digital Rights Ireland*, *Google Spain* et *Schrems*, l'interprétation de la Cour est désormais claire: la protection des données personnelles est un droit fondamental. Permettons-nous donc d'aller au-delà de la question de la légalité ou non du *Privacy Shield* pour prendre un peu de recul et tenter de voir quelle solution pourrait être trouvée pour assurer la protection des données à caractère personnel en tant que droit fondamental dans ce monde numérique qui est actuellement le nôtre sans pour autant restreindre les nombreux avantages qu'il offre.

101. Pour cela, il est impératif de trouver un équilibre entre les données conçues en tant que droit fondamental, les données conçues en tant que bien de commerce (la valeur des données à caractère personnel des citoyens européens pourraient atteindre près de 1.000 milliards d'euros par an d'ici à 2020[287]) et les données conçues en tant que mine d'informations pour les autorités étatiques.

102. Ces trois approches ne sont pas incompatibles, il n'est pas paradoxal pour le règlement (et la directive avant lui) de vouloir protéger les données tout en assurant la libre circulation de celles-ci, mais une balance des intérêts (commerciaux, sécuritaires et de protection des droits fondamentaux) doit intervenir. Plus encore, il faut que l'ensemble des acteurs le fassent de la même manière.

103. La réglementation concernant les données personnelles est, selon nous, vouée à être sans cesse bafouée si elle reste cantonnée à l'Union européenne, bien que celle-ci tente coûte que coûte d'en étendre les effets et qu'elle a réalisé des avancées considérables dans le nouveau règlement à cet égard. Une telle réglementation devrait être mondiale[288] pour être effective car le monde numérique n'a pas de frontières. La prochaine question à se poser est cependant de savoir jusqu'à quel point les Etats sont prêts à faire confiance et à élargir les compétences d'une organisation internationale pour ce faire[289] et à quel point les visions actuelles, différentes, de la protection des données peuvent se concilier.

104. En outre, cette conciliation ne doit pas aboutir à diminuer le niveau de protection actuel en Europe. K. Lenaerts, président de la Cour, estime que l'Europe ne doit pas avoir honte de ses principes de base[290]: « the rule of law is not for

282. Ce test sera facilité pour les Etats pour lesquels la Commission a décidé que c'était le cas mais suite à l'arrêt *Schrems*, une décision de la Commission décidant qu'un pays dispose d'un niveau de protection adéquat ne suffit pas pour rejeter la plainte d'une personne qui estime que ce n'est pas le cas. Il faudra donc aller plus loin dans l'analyse que par le passé.

283. A moins bien sûr que la Cour de justice de l'Union européenne n'invalide entre-temps les mécanismes contractuels: K. LILLINGTON, *o.c.*

284. Pour de plus amples détails sur les différentes étapes successives: COMMISSION EUROPÉENNE, « Frequently Asked Questions relating to transfers of personal data from the EU/EEA to third countries », www.ec.europa.eu/justice/data-protection/international-transfers/files/international_transfers_faq.pdf (consulté le 1er avril 2016), p. 4 et s.

285. Art. 49, 1., du règlement.

286. S. PEYROU, *o.c.*, p. 398.

287. COMMISSION EUROPÉENNE, « Questions et réponses: la réforme de la protection des données », *Fiche d'information MEMO/15/6385*, 21 décembre 2015, p. 3.

288. C. KUNER, « *Google Spain* in the EU and international context », *MJ*, 2015, p. 160 et 161.

289. Y. POULLET, « Transborder Data Flows and Extraterritoriality: The European Position », *o.c.*, p. 153.

290. Le droit à la protection des données personnelles est consacré par la charte de l'Union mais aussi par la Constitution dans de nombreux Etats membres, notamment le Portugal, l'Espagne, la Suède, l'Estonie, la Slovaquie, la Hongrie, l'Autriche, la Pologne, la Lituanie ou la Finlande: J.P. MIFSUD BONNICI, « Exploring the non-absolute nature of the right to data protection », *International Review of Law, Computers & Technology*, 2014, p. 137.

sale »[291]. Cependant, C. Kuner estime que si les Etats-Unis et l'Union européenne, pour ne citer que ces deux grandes puissances, ne travaillent pas mieux ensemble et ne trouvent pas des standards communs, il est difficile d'imaginer qu'ils puissent résoudre les défis posés par les avancées technologiques, la globalisation économique et le pouvoir grandissant des pays d'autres régions vis-à-vis du droit à la protection des données personnelles[292].

105. L'Europe a un rôle à jouer dans ce dossier. Si elle a réussi, grâce aux arrêts de la Cour, à modifier les règles pour des géants tels que Google ou Facebook, il lui est tout à fait loisible d'imposer sa volonté à d'autres entreprises[293] et, via ce processus, de l'imposer à d'autres Etats[294]. L'Union peut en effet utiliser le pouvoir économique des données pour en instaurer une meilleure protection. Les géants du web ont besoin d'un territoire tel que celui de l'Union et sont prêts à en suivre les règles pour autant que celles-ci soient claires[295]. En effet, « la confiance du public dans les produits et services de l'économie numérique dépend en grande partie du respect des règles de protection des données par l'industrie. Le respect de ces règles constitue un facteur concurrentiel fondamental pour les acteurs numériques; il assurera la durabilité du développement de l'industrie numérique, au bénéfice de celle-ci comme de celui des consommateurs »[296]. Dans l'ère numérique actuelle, des nouvelles entreprises fleurissent d'ailleurs dans le but même de protéger les données[297] et un géant tel que Microsoft a récemment décidé de transférer ses données cloud en Europe pour une meilleure protection[298]. Le nouveau règlement pourrait ainsi devenir la pièce maîtresse de la protection des données et permettre à l'Union de développer des stratégies d'influence en s'appuyant sur le caractère mondial du monde numérique[299].

106. La mise en balance d'intérêts divergents tels que la protection des données à caractère personnel pour les individus, la valeur économique de ces données pour les entreprises et l'utilisation de celles-ci à des fins sécuritaires par les autorités étatiques, américaines ou européennes, est une question extrêmement complexe à résoudre[300]. L'un prend souvent le pas sur les deux autres et le gagnant de ce combat homérique n'est pas toujours le même selon l'époque ou la région concernée. Un juste équilibre devrait pourtant être trouvé entre ces trois intérêts[301] et ce rapidement et mondialement au risque de voir naître des batailles sans fin entre individus, entreprises et gouvernements. Mais qui osera et pourra prendre en charge le nettoyage des écuries d'Augias et à qui une telle réglementation sera-t-elle finalement bénéfique? Qui tirera son épingle du jeu? Ces questions restent, à ce jour, ouvertes.

107. Quoiqu'il en soit pour le futur, nous dansons depuis presque 20 ans une valse à mille temps sous les étoiles américaines et européennes. Entre négociations longues de plusieurs années, accords douteux, programmes de surveillance, plaintes d'individus et pressions d'entreprises, plusieurs danseurs se font sans cesse écraser les orteils et ne demandent qu'une chose: que cette valse américano-européenne trouve enfin sa juste mesure.

---

291. V. POP, « ECJ President on EU Integration, Public Opinion, Safe Harbour, Antitrust », *The Wall Street Journal*, 14 octobre 2015.
292. C. KUNER, *o.c.*, p. 163.
293. A. DESFORGES, *o.c.*, p. 85.
294. La Suisse et Israël ont ainsi suivi la position de la Cour de justice de l'Union européenne et ont suspendu leurs propres protocoles avec les Etats-Unis suite à l'invalidation du système *Safe Harbor*: préposé fédéral à la protection des données et à la transparence (PFPDT), « Suite de l'arrêt concernant l'accord '*Safe Harbor*': indications utiles pour la transmission de données aux Etats-Unis », www.edoeb.admin.ch/datenschutz/00626/00753/00970/01320/index.html?lang=fr, dernière mise à jour le 27 janvier 2016 (consulté le 10 avril 2016); Israeli Law, Information and Technology Authority (ILITA), « Court of Justice of the European Union Invalidates the Safe Harbor Arrangement for Transfer of Personal Data from Europe to the United States », traduction non officielle, www.iapp.org/media/pdf/resource_center/ILITA_SH_Statement.pdf (consulté le 10 avril 2016). L'Union impose aussi son point de vue via l'application extraterritoriale de sa législation, prévue notamment à l'art. 3 du règlement.
295. Certaines entreprises ne sont pas favorables aux accès des autorités américaines: D. FILIPPONE, « La situation s'envenime entre Apple et le ministère de la Justice US », *o.c.*; J. RIBEIRO, « Google, Facebook et Microsoft prêts à soutenir Apple face au FBI », *o.c.*
296. G29, « Déclaration commune des autorités européennes de protection des données réunies au sein du groupe de l'article 29 », *WP 227*, 26 novembre 2014, p. 3.
297. M. HAMBLEN, « Sieve, ultime système de contrôle d'accès aux données privées », *LeMondeInformatique.fr*, 21 mars 2016.
298. E. WÉRY, « Cloud: l'absence de protection des données en droit américain pourrait bénéficier aux sociétés européennes », *Droit & Technologies*, 27 avril 2016.
299. A. DESFORGES, *o.c.*, p. 85.
300. R. CAUCHOIS, « La protection des données personnelles en Europe et la compétitivité des entreprises européennes », *Quelle protection des données personnelles en Europe*, Bruxelles, Larcier, 2015, p. 160.
301. Nous ne mentionnons ici que trois intérêts pour rendre notre propos plus synthétique mais d'autres intérêts peuvent être pris en compte. A titre d'exemple, les individus ne veulent pas seulement protéger leurs données, ils veulent également les utiliser de plus en plus dans le cadre des « objets connectés »: C. BRION, H. WAEM et Y. HENDRICKX, « The Big Cloud of Things is watching you: le droit de la vie privée et l'Internet des objets », *in* J.-A. DELCORDE (dir.), *La révolution digitale et les start-ups*, Bruxelles, Larcier, 2016, p. 213 et s. Dans le même ordre idée, les discussions actuelles à propos des données personnelles des joueurs de « Pokémon Go » montrent que les jeunes se font de plus en plus à l'idée que leurs données soient sans cesse utilisées: M. COLINET, « Pokémon GO: 'La notion de vie privée a été redéfinie' », *Le Soir*, 26 août 2016.