UCL Université catholique de Louvain

Faculté de droit et de criminologie (DRT)

Les transferts de données à caractère personnel entre l'Union européenne et les Etats-Unis

Une évolution maîtrisée ou la boîte de Pandore ?

Mémoire réalisé par
Victoria Heinen

Promoteur(s)
François Jongen

Année académique 2016-2017
Master en droit

« Il faut des négociations et un travail collectif pour trouver l'équilibre réaliste des intérêts sur lequel seulement peut se fonder une paix solide »

Mikhaïl Gorbatchev, Conférence de Paix – 30 octobre 1991

Remerciements

Cette contribution constitue l'aboutissement de nombreuses recherches, réflexions et rencontres. Je tenais dès lors à remercier toutes les personnes qui ont pris le temps de me conseiller, de m'éclairer et de discuter avec moi des questions épineuses que soulève le droit de la protection des données à caractère personnel.

Merci à mon promoteur, François JONGEN, pour ses conseils avisés. Merci à Ralf BENDRATH[1] et Théodosios KOTTAS[2] de m'avoir transmis leur point de vue sur l'accord européen en la matière, tout en me permettant de découvrir le travail réalisé au sein des institutions de l'Union. Merci à Lucie HASNEDLOVÀ[3] d'avoir pris le temps de me rencontrer et de me plonger, par ses anecdotes, dans les coulisses de l'accord. Merci à Thierry LÉONARD[4] pour ses réflexions sur la protection des données. Merci à Rocco BELLANOVA[5] de m'avoir communiqué le résultat de ses recherches en matière de *Big Data*. Merci à Christopher KUNER[6] d'avoir accepté de discuter de l'efficacité du droit de la protection des données. Merci également à Philippe DE BACKER[7] et son équipe d'avoir répondu à mes questions.

[1] Ralph BENDRATH est le Conseiller principal en matière de politiques auprès de Jan Philipp ALBRECHT - Député européen du Groupe Vert/Alliance libre européenne.
[2] Théodosios KOTTAS est stagiaire dans le département justice et liberté de l'Agence des droits fondamentaux de l'Union européenne à Vienne.
[3] Lucie HASNEDLOVÀ est chargée de la justice et des affaires intérieures des Etats-Unis et du Canada au Service européen pour l'action extérieure (SEAE).
[4] Thierry LÉONARD est professeur à l'Université Saint-Louis et avocat spécialisé en droit des télécommunications et droit des nouvelles technologies au sein du Cabinet Ulys.
[5] Rocco BELLANOVA est chercheur à l'Université Saint-Louis en matière de vie privée et de protection des données dans le contexte de la sécurité et des technologies et pratiques de surveillance.
[6] Christopher KUNER est professeur de droit et coprésident de la 'Brussels Privacy Hub' de la Vrije Universteit Brussel (VUB) ; Conférencier à la faculté de droit de l'Université de Cambridge ; Professeur visiteur au département de droit de la London School of Economics and Political Science ; Avocat principal en matière de protection de la vie privée au cabinet Wilson Sonsini Goodrich & Rosati.
[7] Philippe DE BACKER est secrétaire d'Etat à la lutte contre la fraude fiscale, à la protection de la vie privée et à la Mer du Nord.

Introduction

1. La collecte et le traitement des données à caractère personnel vont conditionner le siècle qui vient. Les technologies numériques transforment les sociétés et les économies à travers le monde. Tout comme la libre circulation des biens et des personnes a été le moteur des relations économiques et politiques au cours du dernier siècle, le cadre en vertu duquel les données sont transférées à l'échelle mondiale façonnera les mêmes relations pour les années à venir[8]. L'Union européenne et les Etats-Unis sont au cœur de ces évolutions. Pour tirer pleinement profit de cette économie digitale, ils doivent collaborer sur la détermination de règles appropriées pour garantir la circulation efficace des données et promouvoir la croissance et l'innovation, tout en protégeant les droits fondamentaux.

2. Il est établi que la protection des données à caractère personnel est appréhendée de façon radicalement différente en Europe et aux Etats-Unis. Le problème principal aux yeux de l'Union est l'absence de législation américaine d'application générale qui régit la façon dont les entreprises sont autorisées à traiter les données. Au cours des années 90, ce déséquilibre législatif a commencé à poser problème[9]. D'une part, il était avéré que le droit américain ne rencontrait pas le niveau de protection adéquat requis par l'article 25 de la directive 95/46/EC[10] (ci-après, la directive) ; les transferts de données de l'Union vers les Etats-Unis auraient dès lors dû être prohibés. D'autre part, il était inconcevable d'interdire les transferts de données vers les Etats-Unis vu l'importance des relations commerciales entre les deux acteurs.

3. Ce double constat a mené les deux puissances à négocier les principes de la sphère de sécurité (ci-après, *Safe Harbor*), publiés par le ministère du commerce américain et approuvés par la décision de la Commission du 26 juillet 2000[11]. Les transferts de données en provenance de l'Union étaient dès lors autorisés vers les entreprises américaines ayant volontairement adhéré auxdits principes.

---

[8] Direction générale des Politiques externes du Parlement européen, « Transatlantic Digital Economy and Data Protection : State-of-Play and Future implications for the EU's External policies », *ISBN:978-92-823-8660-6*, 1er juillet 2016, p. 7.

[9] A. CASSART, « Les données personnelles expédiées aux U.S.A. arriveront-elles un jour à bon port ? », *J.L.M.B.*, n°2017/26, p. 1231.

[10] 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 du 23 novembre 1995.

[11] Décision (CE) 2000/520 de la Commission du 26 juillet 2000 conformément à la directive 95/46/EC 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 du 25 Août 2000.

4. Ayant fait l'objet d'abondantes critiques[12] dès ses balbutiements, *Safe Harbor* n'a pas résisté aux révélations d'Edward SNOWDEN concernant les activités des services de renseignement américains[13]. Les tentatives de restaurer la confiance entre les deux acteurs n'ont pas suffi, conduisant Maximilan SCHREMS à attaquer la validité de l'accord dans sa totalité.

5. Maximilian SCHREMS, citoyen autrichien, était utilisateur du réseau social Facebook depuis 2008. En vertu des conditions générales de Facebook, ses données, ainsi que celles de tous les abonnés résidant sur le territoire de l'Union, sont transférées au départ de la filiale irlandaise de Facebook sur des serveurs localisés aux Etats-Unis et ce, à des fins de traitement. Le 25 juin 2013, M. SCHREMS a déposé une plainte auprès de l'autorité de contrôle irlandaise, estimant que les révélations faites par Edward SNOWDEN ne permettaient plus de considérer que le droit et les pratiques des Etats-Unis conféraient un niveau de protection suffisant des données transférées. L'autorité irlandaise a rejeté la plainte, invoquant la décision (CE) n°2000/520, aux termes de laquelle la Commission reconnaissait, pour droit, le caractère adéquat du niveau de protection existant aux Etats-Unis. Saisie de l'affaire, la Haute Cour de justice irlandaise[14] a saisi la Cour de justice de l'Union sur question préjudicielle, amenant celle-ci à invalider l'accord *Safe Harbor*[15].

6. Dès février 2016, les Etats-Unis et l'Union européenne ont conclu un nouvel accord, dénommé 'Bouclier de protection des données UE-Etats-Unis'[16] (ci-après, l'accord). La rapidité des négociations se justifiait par le besoin de mettre un terme à l'insécurité crée par la 'mise à mort' de *Safe Harbor*. Ce nouvel accord a été négocié parallèlement à l'élaboration du

[12] Pour un exemple de critique par la doctrine : B. HAVELANGE et A.-C. LACOSTE, « Les flux transfrontaliers de données à caractère personnel en droit européen », *J.D.E.*, 2001, pp. 245-246 ; Pour une critique par le Parlement européen : 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.

[13] En 2013, les révélations d'Edward SNOWDEN concernant le programme PRISM et les activités des services de renseignement américains (NSA, national security agency) ont en effet levé le voile sur la surveillance généralisée, par les autorités publiques, des données transférées vers les Etats-Unis.

[14] High Court of Ireland, n°013/765/JR, *Maximilian Schrems c. Data Protection Commissioner*, 16 juillet 2014.

[15] C.J.U.E., C-2015/650, *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650.

[16] Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

nouveau règlement (UE) n°2016/679[17] (ci-après, le règlement), qui remplacera la directive à partir du 25 mai 2018. La protection des données était donc au centre de toutes les attentions.

7. L'objet de la présente contribution consistera ainsi à évaluer la compatibilité du nouvel accord avec les enseignements tirés de l'arrêt *Schrems* et les futures exigences posées par le règlement. Par choix, notre propos ne touchera qu'aux transferts de données à des fins commerciales et non pénales, judiciaires ou administratives. Nous suivrons l'idée selon laquelle une protection efficace des données des citoyens européens passe par l'édiction de principes forts mais aussi par la mise en place de voies de recours et de mécanismes de surveillance appropriés. Le droit n'est rien s'il ne prévoit pas les garanties de son respect. Notre hypothèse est que le nouvel accord ne remplit pas encore pleinement ces deux exigences ; notre espoir est que ses faiblesses seront corrigées lors du premier 'réexamen annuel conjoint' de l'accord, attendu à l'autonome.

8. La première partie de notre contribution visera à identifier le cadre légal régissant les transferts de données entre l'Union européenne et les Etats-Unis. Outre la réglementation desdits transferts (Chapitre 1), nous étudierons le nouveau champ d'application extraterritoriale du règlement et son intérêt dans le présent contexte (Chapitre 2). Des réflexions sur l'adoption d'un cadre international seront ensuite esquissées (Chapitre 3). La deuxième partie nous permettra d'évaluer les principes contenus dans l'accord (Chapitre 1) ainsi que ceux qui brillent par leur absence (Chapitre 2). Enfin, la troisième partie nous amènera à faire le bilan des voies de recours et des mécanismes de surveillance prévus par l'accord (Chapitre 1), pour ensuite nous intéresser au rôle des autorités nationales de protection des données (ci-après, les autorités de contrôle) (Chapitre 2).

[17] 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 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119 du 4 mai 2016.

Titre I – Les transferts internationaux de données à caractère personnel : cadre légal et perspective multidimensionnelle

9. Les échanges transnationaux de données à caractère personnel[18] mêlent deux dimensions dont les interactions suscitent la controverse : d'un côté, la réglementation des transferts internationaux de données et de l'autre, l'application extraterritoriale du droit européen.

10. Pour certains, cette distinction a perdu son intérêt dans le contexte des transferts internationaux de données en ce que tout transfert de données de l'Union vers un pays tiers constitue en tant que tel un traitement de données à caractère personnel au sens de la directive[19]. Or, ces transferts ne peuvent avoir lieu que vers un pays tiers offrant un niveau de protection 'substantiellement équivalent'[20] à celui qui existe en droit européen[21]. L'exigence d'un tel niveau de protection équivaudrait donc à une application extraterritoriale du droit européen[22].

11. Pour d'autres, cette exigence de protection 'substantiellement équivalente' ne revient pas à appliquer le droit européen de façon extraterritoriale, vu la marge d'appréciation laissée au pays tiers. En effet, le choix des moyens grâce auxquels les données sont protégées est laissé à l'entière discrétion du pays tiers ; c'est toutefois *le niveau* de protection qui doit être 'essentiellement équivalent' à celui prévu par la législation européenne[23]. Nous adhérons à cette théorie, en ce que considérer le contraire reviendrait à conclure que la directive 95/46/EC [ou le règlement, après mai 2018] jouit d'un effet direct dans le pays tiers, ce qui n'est pas le cas.

---

[18] Les données à caractère personnel sont définies par l'art. 4, §1, du règlement, comme étant « *toute information se rapportant à une personne physique identifiée ou identifiable* » ; sont notamment visés le nom, l'âge, un dossier médical, une empreinte digitale ou encore une photographie de la 'personne concernée'.

[19] Art. 2, b), de la directive : pour que la directive s'applique, les données doivent être 'traitées' ; cette notion est interprétée largement par la Cour de l'Union, qui considère le 'transfert' comme étant un 'traitement' de données ; C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 45.

[20] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 73. Voy. *infra* pour de plus amples développements sur la notion de 'niveau de protection substantiellement équivalent'.

[21] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 46.

[22] C. KUNER, "Paper n°14/2016 - Reality and illusion in EU Data Transfer Regulation Post Schrems", *Legal studies - Research Paper studies*, University of Cambridge, mars 2016, p. 10.

[23] Annexe II du présent document - Entretien avec Monsieur Théodosios KOTTAS, stagiaire à l'Agence des droits fondamentaux de l'Union européenne, réalisé à Vienne le 27 juin 2017, p. 87 ; C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 73 : « *le terme 'adéquat' figurant à l'article 25, paragraphe 6, de la directive 95/46 implique qu'il ne saurait être exigé qu'un pays tiers assure un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union* ».

12. Il convient cependant de distinguer cette problématique de celle du champ d'application étendu du règlement. Comme précisé par le contrôleur européen, les responsables et les sous-traitants qui ne sont pas établis dans l'Union seront soumis aux règles de droit européen tant que leurs activités de traitement seront liées à la vente de services ou de produits à des particuliers établis dans l'Union, ou à l'étude du comportement desdits individus. Dans ces situations, « *la certification prévue par le Bouclier vie privée ne dispensera pas les organismes certifiés de l'application des dispositions du cadre juridique de la protection des données de l'Union européenne dès lors que ces organismes entrent dans le champ d'application modifié du cadre* ». Dans cette hypothèse, le cadre juridique européen l'emportera sur les principes de l'accord, et lesdits organismes seront tenus de se conformer aux exigences du règlement. En effet, la règlementation des flux transfrontaliers ne se justifie que par l'absence d'application territoriale du droit européen.

13. Le droit de la protection des données à caractère personnel s'inscrit donc dans une perspective multidimensionnelle[24], requérant une bonne compréhension d'une part, du cadre légal régissant les transferts internationaux de données (Chapitre 1) et d'autre part, de l'application étendue du droit européen de la protection des données (Chapitre 2). Parallèlement, la globalisation des traitements de données et les difficultés occasionnées par l'absence d'harmonisation ont suscité des réflexions sur l'éventuelle adoption d'un cadre légal international (Chapitre 3).

Chapitre 1 – La règlementation des transferts internationaux de données

14. Le chapitre IV de la directive 95/46/EC prévoit les règles relatives aux transferts de données à caractère personnel vers des pays tiers. Après avoir brièvement analysé les trois socles permettant un tel transfert (Section 1), nous étudierons la notion clef de '*niveau de protection adéquat*' et son évolution au regard du nouveau règlement[25] et de l'arrêt *Schrems* (Section 2).

[24] Y. POULLET, "Transborder Data Flows and Extraterritoriality: the European Position", *Journal of International Commercial Law and Technology,* 2007, vol. 2, éd. n°3, p. 144.

[25] 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 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119 du 4 mai 2016 ; 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 ; Commission européenne, « Questions et réponses : la réforme de la protection des données », *Fiche d'information MEMO-15-6385*, 21 décembre 2015.

Section 1 – Le triptyque des standards permettant le transfert

15. A l'heure actuelle, les transferts internationaux de données à caractère personnel sont régis par les Articles 25 et 26 de la directive 95/46, applicables aux vingt-huit Etats membres de l'Union ainsi qu'aux trois membres de l'Espace économique européen[26]. Trois standards peuvent être invoqués afin de transférer des données personnelles de l'Union vers un pays tiers.

16. Premièrement, l'article 25[27] contient la règle de principe selon laquelle « *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* », tel qu'apprécié par une décision de la Commission européenne. Douze décisions ont à l'heure actuelle été adoptées[28].

17. Deuxièmement, l'article 26(1)[29] énonce une série de dérogations[30] autorisant, sous certaines conditions, le transfert des données vers un pays tiers n'assurant pas un niveau de protection adéquat. A titre illustratif, tel est le cas lorsque la personne concernée[31] a 'indubitablement donné son consentement'[32], lorsque le transfert est nécessaire à 'la sauvegarde de l'intérêt vital de la personne concernée'[33] ou encore dans l'hypothèse où ce transfert est rendu obligatoire pour la 'sauvegarde d'un intérêt public important'[34].

18. Troisièmement, l'article 26(2)[35] prévoit diverses situations dans lesquelles un transfert de données peut être autorisé en raison de l'existence de 'garanties suffisantes' au regard de « *la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à*

[26] Islande, Lichtenstein et Norvège.
[27] Art. 45 du règlement.
[28] Andorre (décision 2010/625/EU), Argentine (décision 2003/490/EC), Canada (décision 2002/2/EC), Suisse (décision 2000/518/EC), Iles Féroé (décision 2010/146/EC), Guernesey (décision 2003/821/EC), Israël (décision 2011/61/EU), Ile de Man (décision 2004/411/EC), Jersey (décision 2008/393/EC), Nouvelle-Zélande (décision 2013/65/EU), Etats-Unis (décision 2016/1250/EU) toutes lues en combinaison avec la décision d'exécution (UE) 2016/2295 de la Commission du 16 décembre 2016 modifiant les décisions 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE et 2011/61/UE, et les décisions d'exécution 2012/484/UE et 2013/65/UE constatant, conformément à l'article 25, paragraphe 6, de la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par certains pays, *J.O.U.E.*, L 344/83 du 17 décembre 2016.
[29] Ces dérogations n'ont pas été reprises par l'art. 46 du règlement.
[30] Pour plus d'informations sur la mise en œuvre de cette disposition : G29, « Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/EC du 24 octobre 1995 », *WP114*, 25 novembre 2005.
[31] La notion de 'personne concernée' vise la personne physique identifiée ou identifiable par une information la concernant ; cette information étant alors qualifiée de 'donnée à caractère personnel'. Voy. art. 4, §1, du règlement.
[32] Art. 26, §1, a), de la directive.
[33] Art. 26, §1, e), de la directive.
[34] Art. 26, §1, d), de la directive.
[35] Art. 46, §2, du règlement.

l'égard de l'exercice des droits correspondants ». Il s'agit de 'garanties appropriées'[36] qui sont créés spécifiquement pour les besoins du transfert en cause[37]. Deux types de garanties ont ainsi été reconnus : les clauses contractuelles appropriées[38] et les règles d'entreprise contraignantes[39].

19. Ces règles sont capitales afin d'éviter que la protection conférée par la législation européenne ne soit anéantie par le seul transfert des données hors des frontières de l'Union. En l'absence d'un tel régime, il suffirait pour une entreprise de traiter lesdites données sur le territoire d'un pays tiers afin d'échapper au droit européen et corrélativement bafouer les droits des citoyens européens[40]. L'objectif de ces dispositions est donc de faciliter les transferts de données dans des contextes aussi variés que les interactions sociales, la croissance économique et le progrès technologique[41] tout en assurant une protection continue des droits des citoyens européens, même hors des frontières de l'Union[42].

Section 2 – L'exigence d'un niveau de protection adéquat

20. Dans un premier temps, nous analyserons la teneur du principe de '*niveau de protection adéquat*' et sa récente évolution (§1). Une étude du mécanisme de la '*décision d'adéquation*' sera ensuite entreprise, afin de comprendre le socle sur lequel repose les transferts de données à caractère personnel entre l'Union européenne et les Etats-Unis (§2).

§1- Le principe comme point de départ, article 25(1) de la directive

21. Non défini dans la directive, ce niveau de protection adéquat s'apprécie au regard de l'ensemble des circonstances relatives à un transfert ou à une catégorie de transferts de

[36] Art. 46, §1, du règlement.
[37] CEPD, "Position Paper - The transfer of personal data to third countries and international organizations by EU institutions and bodies", Bruxelles, 14 juillet 2014, p. 18.
[38] Art. 26, §2, de la directive et art. 46, §2, c) et d), du règlement. Sont visées (i) les clauses types de protection des données adoptées par la Commission et (ii) les clauses types de protection des données adoptées par une autorité de contrôle.
[39] Art. 46, §2, b), du règlement ; G29, « Document de travail : Transferts de données personnelles vers des pays tiers : Application de l'article 26, §2, de la directive UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données », *WP74*, 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.
[40] 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. 97 ; J.-M. VAN GYSEGHEM *et al.*, « La protection des données à caractère personnel en droit européen *», Journal européen des droits de l'homme*, 2014/1, p. 55 et s.
[41] C. KUNER, "Paper n°14/2016 …", *op. cit.*, p. 1.
[42] C. KUNER, *ibidem*.

données[43] ; en particulier, sont prises en compte « *la nature des données, la finalité et la durée du ou des traitements envisagés, le 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* »[44].

22. Un tel niveau de protection est réputé acquis lorsque les principes fondamentaux contenus dans la directive sont effectivement mis en œuvre dans le droit interne du pays tiers concerné[45]. En 1998, le Groupe de travail Article 29[46] (ci-après, G29) s'était déjà attelé à dresser une liste de base des conditions minimales devant être respectées, comprenant six principes essentiels : la limitation des transferts à une finalité spécifique, la qualité et la proportionnalité des données, la transparence, la sécurité, le droit d'accès, de rectification et d'opposition, et les restrictions aux transferts ultérieurs[47].

23. En outre, l'existence d'un dispositif de contrôle externe, sous la forme d'une autorité indépendante, est un impératif additionnel posé par le groupe de travail. Il suppose de remplir trois objectifs précis : assurer un niveau satisfaisant de respect des règles, apporter soutien et assistance aux personnes concernée et fournir des voies de recours appropriées[48]. Ce n'est que moyennant le respect de ces exigences et « *sous réserve du respect des dispositions nationales prises en application des autres dispositions de la directive* »[49], qu'un transfert peut en principe prendre place.

24. Le règlement préserve ce principe d'adéquation, laissant exclusivement[50] à la Commission le soin de décider « *qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou* [une] *organisation internationale* »[51] assure un niveau de

[43] G29, « Premières orientations relatives aux transferts de données personnelles vers des pays tiers – Méthodes possibles d'évaluation du critère adéquat de protection », *WP4*, 26 juin 1997, pp. 6-7.
[44] Art. 25, §2, de la directive.
[45] Agence des droits fondamentaux de l'Union européenne, *Handbook on European data protection law*, 2014, p. 133, pt. 6.3.
[46] Le G29 est un groupe de travail européen indépendant institué par l'article 29 de la directive et traitant des questions de la vie privée et de la protection des données à caractère personnel ; il sera remplacé par le 'Comité européen de la protection des données', établit à l'article 68 du règlement.
[47] G29, « Transfert des données personnelles vers des pays tiers : Application des articles 25 et 26 de la directive relative à la protection des données », *WP12*, 24 juillet 1998, pp. 6-7.
[48] G29, *ibidem*, p. 8.
[49] Art. 25, §1, de la directive.
[50] Notons que lors des négociations sur le règlement, le Parlement européen souhaitait que la Commission agisse par voie d'actes délégués – en application de l'art. 290 TFUE – conférant alors au Parlement le droit de révoquer la délégation ou d'exprimer des objections à l'acte délégué. Cette proposition a été clairement rejetée par les Etats membres ; Annexe I du présent document – Entretien avec Monsieur Ralf BENDRATH, Conseiller principal en matière de politiques auprès de Jan Philipp ALBRECHT (Député européen – Groupe Vert/Alliance libre européenne), réalisé à Bruxelles le 27 novembre 2016, p. 77.
[51] Art. 45, §1, du règlement.

protection adéquat. Cette évaluation a fait l'objet de diverses précisions, tant dans le règlement qu'à la lumière de l'arrêt *Schrems*.

25. Tout d'abord, le règlement étoffe les critères d'appréciation du niveau d'adéquation, y incluant notamment « *l'état de droit, le respect des droits de l'homme et des libertés fondamentales*, […] *les règles en matière de protection des données* »[52], « *l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes* […] »[53] ainsi que « *les engagements internationaux pris* […] *en particulier en ce qui concerne la protection des données à caractère personnel* »[54].

26. Ensuite, l'arrêt *Schrems* vient apporter un éclairage supplémentaire, précisant que l'exigence de « niveau de protection adéquat » - telle que contenue dans la directive – doit être comprise comme exigeant que ce pays tiers « *assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et droits fondamentaux substantiellement équivalent*[55] *à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la Charte* »[56]. La portée générale d'un tel enseignement laisse présager sa pérennité sous l'empire du règlement.

§2 – La décision d'adéquation au titre d'ultime solution, article 25(6) de la directive

27. Certains pays tiers, tels que les Etats-Unis, ne disposent pas du niveau de protection requis[57]. Ainsi, en vertu de l'article 25, paragraphe 6 de la directive 95/46[58], la Commission peut « *constater qu'un pays tiers assure un niveau de protection adéquat* […], *en raison de* […] *ses engagements internationaux* »[59]. Dès lors que la Commission adopte une décision en ce sens, le transfert des données à caractère personnel de l'Union vers le pays tiers concerné peut

[52] Art. 45, §2, a), du règlement.
[53] Art. 45, §2, b), du règlement.
[54] Art. 45, §2, c), du règlement.
[55] Souligné par nous.
[56] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 73.
[57] G29, « Avis n°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 », *WP15*, 26 janvier 1999, pp. 2-3 ; J.-P. MOINY, « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010/2, p. 265.
[58] Art. 45, §3, du règlement.
[59] Notons que les critères d'appréciation énoncés dans le cadre de l'article 25, §1, de la directive sont également applicables en l'espèce.

avoir lieu[60]. Cette décision est obligatoire pour les Etats membres, appelés à prendre toutes les mesures nécessaires afin de s'y conformer[61]. C'est en application de cette disposition que la décision *Safe Harbor*[62], suivie de l'accord *Privacy Shield* ont été adoptés.

28. Notons la particularité d'un tel système, ne s'appliquant pas à l'ensemble des transferts de données de l'Union vers le pays tiers[63]. Ainsi, l'accord dispose que « *les Etats-Unis assurent un niveau de protection adéquat des données à caractère personnel transférées, dans le cadre du bouclier de protection des données UE-Etats-Unis, de l'Union vers des organisation auto-certifiées aux Etats-Unis* »[64]. L'accord ne concerne donc pas le niveau général de protection prévu par la législation américaine, et ne s'applique qu'aux transferts réalisés vers « *des organisations américaines qui ont auto-certifié leur adhésion aux principes auprès du ministère du commerce et qui se sont engagés à les respecter* »[65]. Nous analyserons plus en détails les principes contenus dans l'accord (Titre II) ainsi que les voies de recours et les mécanismes de surveillance existants (Titre III).

Chapitre 2 – L'extraterritorialité renforcée du règlement (UE) n°2016/679

29. Il convient désormais de s'intéresser au champ d'application étendu du nouveau règlement. Une bonne compréhension de cette réforme (Section 1) est un préalable nécessaire à l'étude des critiques formulées à son encontre (Section 2).

---

[60] Av. gén. Y. BOT, concl. préc. C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 23 septembre 2015, C-362/14, ECLI:EU:C:2015:650, p. 2.

[61] Art. 25, §6, al. 2, de la directive ; A. DEBET *et al.*, *Informatique et libertés – La protection des données à caractère personnel en droit français et européen*, Issy-les-Moulineaux, Lextenso, 2015, p. 667.

[62] Décision (CE) 2000/520 de la Commission du 26 juillet 2000 conformément à la directive 95/46/EC 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 du 25 Août 2000.

[63] A. GROSJEAN, *op. cit.*, p. 199.

[64] Considérant 13 et art. 1, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016, pp. 3 et 35.

[65] Considérant 15, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016 ; Y. POULLET, « Internet et vie privée : entre risques et espoirs », *J.T.*, 2001, p. 161 ; R. NIMMER, « Internationally interactive law : perspectives on trans-border data control from the U.S. », *Défis du droit à la protection de la vie privée – Perspectives du droit européen et nord-américain, Cahiers du Centre de Recherches Informatique et Droit*, vol. 31, Bruxelles, Bruylant, 2008, p. 431.

Section 1 - Quand le droit européen étend ses tentacules

30. Le critère cardinal d'application du droit européen en matière de protection des données découle de la localisation du traitement sur le territoire de l'Union. Ceci suppose d'une part, que le responsable ou le sous-traitant détienne un établissement sur le territoire d'un Etat membre et qu'il y exerce une activité réelle et effective et d'autre part, que le traitement soit effectué dans le cadre des activités dudit établissement sur le territoire dudit Etat[66].

31. En l'absence d'établissement sur le territoire de l'Union, le droit européen continue à s'appliquer si le droit national d'un Etat membre est désigné en vertu d'une règle de droit international public du lieu d'établissement du responsable[67]. Désormais, le règlement sera également applicable lorsque les activités de traitement sont liées « *à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes ; ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* »[68].

32. Cette réforme a pour effet d'étendre la portée du droit européen aux entreprises non-européennes offrant des services sur internet[69]. Qualifié de '*lex loci solutionis*'[70], ce principe est perçu comme une victoire pour le groupe des verts au Parlement européen, obligeant de nombreuses entreprises à se conformer à l'ensemble du règlement, et non plus seulement aux 'faibles principes du Bouclier vie privée'[71] dans le cas des entreprises américaines.

---

[66] Art. 4, a), de la directive, repris par l'art. 3, §1, du règlement. Pour une meilleure compréhension de la notion d'établissement : F. COTON, « L''établissement' du responsable de traitement de données, une notion clé », *J.L.M.B.*, 2017/26, p. 1215-1220.

[67] Cette hypothèse spécifique recouvre le cas des ambassades, soumises au respect du droit européen malgré l'absence d'établissement sur le territoire de l'Union.

[68] Art. 3, §2, a) et b), du règlement ; La Commission souligne qu'un tel champ d'application aura pour effet de soumettre toutes les entreprises agissant auprès des mêmes individus à des conditions concurrentielles homogènes : 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.

[69] C. KUNER, « The European Commission's proposed data protection regulation: a Copernican revolution in European data protection law", *Bloomberg BNA Privacy and Security Law Report*, 6 février 2012, p. 6.

[70] En français, le principe du « lieu où se tient le marché » : J.-P. ALBRECHT, *The EU's Data Protection Reform*, Göttingen, AktivDruck, décembre 2015, p. 17.

[71] Annexe I du présent document, *op. cit*., p. 67.

Section 2 – Une extraterritorialité en manque de repères

33. La question de la légitimité d'une telle extension et l'évolution jurisprudentielle s'y attachant attireront en premier lieu notre attention (§1). Nous esquisserons ensuite les réticences[72] qu'elle suscite et les théories s'attelant à la limiter (§2).

§1 - La légitimité d'une extraterritorialité renforcée

34. Loin de faire l'unanimité, l'application extraterritoriale étendue du règlement est accueillie variablement par les commentateurs et experts.

35. Pour certains, cette extension témoigne de la volonté de répondre au caractère mondial des transferts, assurant une protection effective et continue des droits des citoyens européens[73]. L'Union se contente ainsi de conditionner la poursuite des relations commerciales au respect des standards européens de protection des données. La logique est identique à celle du marché unique[74] : les caractéristiques du produit doivent être conformes aux réglementations européennes, faute de quoi l'export au sein de l'Union sera refusé[75]. C'est donc à juste titre que le Président de la Commission qualifie ce nouveau marché de 'Marché unique du numérique'.

36. Pour d'autres, cette extension est le signe d'une Europe en quête d'un pouvoir de négociation accru par l'entremise d'un champ d'application étendu. Qualifiée d'intrusion déplacée dans les intérêts nationaux étrangers[76], cette extension est perçue comme une transition spectaculaire de l'approche du 'pays d'origine' vers celle du 'pays de destination'[77], augurant une application générale du règlement à l'ensemble du réseau internet.

37. Cette question n'a pas échappé à la Cour de justice, dont l'évolution jurisprudentielle témoigne d'une volonté de trouver au droit européen de la protection des données une juste place.

---

[72] C. KUNER, "Paper n°49/2015 - Extraterritoriality and International Data transfers in EU Data Protection Law", *Legal studies - Research Paper studies*, Cambridge University Press, août 2015, pp. 2-3.
[73] B. SVANTESSON, "A 'layered approach' to the extraterritoriality of data privacy laws", *International Data Privacy Law*, vol. 3, n°4, Oxford University Press, octobre 2013, p. 278.
[74] Dans ce sens, voy. Y. POULLET, "Transborder Data Flows …", *op. cit.*, p. 148.
[75] Annexe II du présent document, *op. cit.*, p. 87.
[76] C. KUNER, « Paper n°49/2015…", *op. cit.*, p. 2.
[77] C. WOLF, "White Paper - Overextended: jurisdiction and applicable law under the EU General Data Protection Regulation", *Future of Privacy Forum*, janvier 2013, https://docslide.net/documents/overextended-jurisdiction-and-applicable-law-under-the-eu-general-data-protection.html, p. 2.

38. En 2003, la Cour de justice semblait réticente à conférer au droit européen une portée trop étendue. Ainsi, elle a considéré qu'il n'y avait pas de transfert de données vers un pays tiers au sens de l'article 25 de la directive lorsqu'une personne charge des données sur la page internet d'un site hébergé dans l'Union. Dans le cas contraire, le régime spécial prévu par le Chapitre IV de la directive deviendrait un régime d'application générale, en ce que « *ce transfert serait nécessairement un transfert vers tous les pays tiers où existent les moyens techniques nécessaires pour accéder à internet* »[78].

39. La Cour semble pourtant aller plus loin dans l'arrêt *Schrems,* reliant le 'niveau adéquat de protection des données personnelles' visé par la directive au niveau élevé de protection des données prévu par la Charte[79]. La Cour requiert donc un niveau élevé de protection pour les transferts de données personnelles vers un pays tiers. Au regard de cette évolution, il semble probable qu'en 2017, la Cour serait plus hésitante à conclure que l'Article 25 de la directive [Article 45 du nouveau Règlement] ne s'applique pas au chargement de données personnelles sur une page internet, dès lors qu'il en résulte un accès dans des pays où le niveau de protection pourrait ne pas être adéquat[80].

40. Cette évolution jurisprudentielle témoigne de l'absence de frontières dans le monde numérique, exigeant de réinventer sans cesse les méthodes de protection des données personnelles et ce, quitte à essuyer les critiques.

§2 - Les théories de limitation de la portée extraterritoriale

41. D'une portée considérable, la compétence extraterritoriale issue de l'article 3 du règlement a défrayé la chronique, faisant surgir diverses théories vouées à en définir les contours. Bien que le règlement n'en consacre aucune, ces thèses permettent une mise en lumière des enjeux gravitant autour d'une applicabilité (trop ?) étendue du droit européen.

42. C'est au départ du risque d'inexécutabilité des décisions obtenues à l'encontre des responsables de traitements établis hors de l'Union que ces théories ont vu le jour. En effet, cette 'expansion géographique'[81] pourrait s'avérer inefficace vu l'absence de compétence des

[78] C.J.C.E., C-101/01 *Bodil Lindqvist*, 6 novembre 2003, ECLI:EU:C:2003:596, pt. 69.
[79] La Cour de justice de l'Union se pose ici en véritable garante des droits fondamentaux tels qu'inscrits dans la Charte de l'Union. Voy. en ce sens : C.J.U.E., C-131/12 *Google Spain SL et Google Inc. C. Agencia Espanola de Proteccion de Datos (AEPD) et Mario Costeja Gonzales*, 13 mai 2014, ECLI:EU:C:2014:317.
[80] C. KUNER, "Paper n°14/2016…", *op. cit.*, p. 10.
[81] C. WOLF, *op. cit.*, p. 4.

autorités de contrôle hors du territoire de l'Union. Le G29 avait à cet égard déjà suggéré en 2002 l'adoption d'une approche prudente et sélective, selon laquelle le droit européen ne s'appliquerait que lorsque « *le besoin s'en fait sentir, que cette protection est utile et que le degré d'applicabilité de la directive est correct* » [82] en gardant toutefois à l'esprit le cadre transfrontalier de la situation. Convaincus par cette approche, différents auteurs s'étaient ainsi attelés à imaginer les limites possibles de cette extraterritorialité, à l'aune de critères et de méthodes dont nous esquisserons brièvement les contours.

43. Selon C. KUNER, c'est vers un dépeçage de la réglementation en matière de protection des données qu'il faudrait aller, afin d'en extraire l'essence, qui serait alors présumée d'application extraterritoriale[83]. Les six principes fondamentaux dégagés par le G29 en 1998 pourraient à cet égard servir de point de départ. Cependant, le climat politico-juridique actuel soulève de nombreux doutes quant à la faisabilité d'une telle entreprise[84].

44. L'approche multicouches[85] conjecturée par D. SVANTESSON s'attelle, quant-à-elle, à scinder les dispositions du droit à la protection des données en trois strates (la prévention des abus, les droits et les aspects administratifs), les soumettant chacune à un test spécifique afin d'en déterminer l'éventuelle extraterritorialité. Plus pragmatique, cette méthode paraît répondre aux faiblesses de la logique binaire[86], proposant une délimitation plus sophistiquée de ladite portée extraterritoriale.

45. Enfin, C. WOLF promeut le principe du 'ciblage intentionnel', selon lequel le droit européen de la protection des données ne devrait s'appliquer que dans le cas où l'activité impliquant le traitement des données cible significativement des particuliers dans l'Union[87]. Issue des réflexions d'un *think thank* américain, cette approche est convaincante mais supposerait une refonte de l'article 3 du règlement. Ainsi, au lieu de simplement « *offrir des*

---

[82] G29, " Document de travail n°5035/01 : Application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE", *WP56*, 30 mai 2002, p. 10.

[83] C. KUNER, « Paper n°14/2016…", *op. cit.,* p. 15. Selon lui, les droits repris par l'article 8 de la Charte constitueraient, en partie, l'essence du droit fondamental à la protection des données, revêtant ainsi par nature une dimension extraterritoriale.

[84] Alors que les négociations sur le nouveau règlement ont suscité de vives dissensions, il semble peu probable qu'un accord puisse être trouvé sur le contenu même de « l'essence du droit à la protection des données ».

[85] B. SVANTESSON, *op. cit.*, pp. 279-284.

[86] Il s'agit de la logique suivie par le règlement, visant à déterminer selon une '*one-size-fits-all manner'* l'applicabilité d'une loi relative à la protection des données.

[87] C. WOLF, *op. cit*., p. 7 ; Ce 'ciblage' pourrait notamment consister dans le fait, pour le gestionnaire des données, de collecter des données personnelles dans le cadre de services expressément accessibles par – ou dirigés vers – des résidents de l'Union et ce, via l'affichage d'information dans une des langues de l'Union ; une autre hypothèse est l'envoi de publicités dans la langue de l'utilisateur ou pour des produits et services disponibles dans l'Union.

biens ou des services » ou « *suivre les comportements des résidents de l'Union* », l'entreprise devrait « *intentionnellement cibler* » lesdits résidents pour être soumise au droit européen. Moins invasive dans sa portée, cette approche appellerait cependant un accord sur la définition précise du 'ciblage intentionnel'.

46. Ce n'est donc aucune de ces approches limitatrices qui a été retenue, confirmant la volonté d'une application extraterritoriale renforcée. Cette extension était inévitable au regard de l'évolution des technologies et de la toute-puissance d'un grand nombre d'entreprises établies hors du territoire de l'Union, offrant des biens et des services sur internet au résident de l'Union, dont les données seront récoltées et envoyées à des fins de traitement hors de ladite Union[88]. En outre, les nombreux scandales qui ont éclaté tant en matière de surveillance que d'abus dans l'utilisation des données par le secteur privé, ne font que conforter l'idée de standards de protection faibles hors des frontières de l'Union. Cette 'dynamique d'expansion' comme nous l'appellerons, n'est finalement que le reflet d'une Europe revendiquant son existence propre, son modèle de société et ses standards.

47. Dans une perspective transatlantique, les insatisfactions européennes suscitées par le nouvel accord semblent donc trouver réconfort dans une application extraterritoriale d'un règlement dont les principes ont – presque et enfin – recueillis l'unanimité.

Chapitre 3 – Vers un cadre international pour la protection des données ?

48. La globalisation des traitements de données à caractère personnel et les difficultés suscitées par l'absence d'harmonisation appellent à envisager un cadre international pour la protection des données.

49. Cette invitation pour un système repensé émane tant d'entités privées[89] que publiques, souhaitant répondre à deux objectifs majeurs[90]. D'une part, éviter les brèches dans la protection des données. L'absence de normes harmonisées[91], voir l'absence de toute législation en la

[88] Voy. GDPR.expert, l'outil d'analyse du nouveau règlement européen, Cabinet Ulys, https://www.gdpr-expert.eu/article.html?id=3#difficultesprobables (consulté le 3 mars 2017).
[89] En 2007, Google réclamait l'adoption de normes mondiales de protection de la vie privée, affirmant qu'il était temps que les données – la marchandise la plus globalisée et transportable du monde – soient traitées de la même manière que tout autre objet du commerce international. Voy. https://publicpolicy.googleblog.com/2007/09/call-for-global-privacy-standards.html (consulté le 13 juillet 2017).
[90] C KUNER (C.), "An international Legal Framework for Data Protection: Issues and Prospects", *Computer Law & Security Review*, vol. 25, 2009, pp. 2-3.
[91] Notons cependant qu'en ce qui concerne l'Union, le règlement permettra aux entreprises concernées d'appliquer une législation mieux harmonisée et non plus les multiples transpositions de la directive en droit interne.

matière[92], soumet les traitements de données à de nombreux risques. D'autre part, faciliter les flux mondiaux de données[93]. Le nombre élevé de standards de protection crée pour les entreprises un fardeau de conformité et une plus grande insécurité[94]. L'exemple UE-U.S. est un plaidoyer puissant en faveur de l'adoption d'un cadre légal international, qui aurait permis de préserver les parties d'une multitude d'accords complexes et difficiles à suivre, ainsi que d'un gaspillage significatif de ressources tant lors des négociations qu'au cours du processus de rédaction[95].

50. De façon générale, l'opportunité d'adopter un régime légal international fait l'unanimité mais le consensus s'arrête à l'intention. La diversité des approches due à des facteurs historiques, culturels ou légaux fait obstacle à un accord sur la détermination du cadre légal à adopter[96]. Deux interrogations sont en ce sens cruciales.

51. La première question concerne le niveau auquel ces standards doivent être adoptés. Des standards trop abstraits pourraient compromettre une protection effective ; des standards trop détaillés risqueraient d'être difficilement implémentés en raison des nombreuses disparités culturelles existant à travers le globe[97].

52. La seconde concerne l'institution qui se chargera d'en superviser l'application. A cet égard, l'Organisation des Nations Unies serait la plus apte à remplir ce rôle et ce, malgré les avis divergents. Pour C. KUNER, bien que les Nations Unies ait le rayonnement universel nécessaire, le travail de ses organes juridiques, tels que la commission des Nations Unies pour le droit commercial international, démontre que l'atmosphère très politisée de l'organisation rend les tentatives d'harmonisation trop lentes et difficiles. Au contraire, pour P. DE HERT, il faut redécouvrir le rôle des Nations Unies dans la protection des données.

---

[92] Pour une comparaison des législations sur la protection des données à travers le monde, voy. https://www.dlapiperdataprotection.com/index.html (consulté le 7 juillet 2017).

[93] Sur l'importance pour l'Union d'établir un cadre légal de protection des données équilibré et attractif pour les 'géants du Web' : A. DESFORGES, « Les stratégies européennes dans le cyberespace », *Droits et souveraineté numérique en Europe*, Bruxelles, Bruylant, 2016, p. 85.

[94] Selon E. SCHMIDT (CEO de Google), l'une des conséquences dommageables de l'absence de standards globaux est la création d'une insécurité pour les entreprises, pouvant aller jusqu'à restreindre l'activité économique ; en effet, une organisation qui a des activités mondiales doit connaître les standards de protection applicables sur chacun des marchés où elle opère. Voy. http://peterfleischer.blogspot.be/2007/09/eric-schmidt-on-global-privacy.html (consulté le 13 juillet 2017).

[95] P. DE HERT et V. PAPAKONSTANTINOU, « Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency?", *I/S: a journal of Law and Policy for the Information Society*, vol. 9, éd. 2, 2013, p. 294.

[96] C. KUNER, "Paper n°48/2015 - The European Union and the Search for an International Data Protection Framework", *Groningen Journal of International Law*, vol. 2, éd. 1: Privacy in international law, août 2015, p. 59.

[97] C. KUNER, « An international Legal Framework…", *op. cit.*, p. 27.

53. La création d'une nouvelle agence onusienne chargée de la protection des données s'inscrirait dans une dynamique présent-futur. Elle permettrait tant de répondre aux préoccupations actuelles que d'assurer une coopération internationale pour l'avenir[98]. Les principes directeurs[99] des Nations Unies, adoptés en 1990, offriraient un cadre réglementaire adéquat tout en étant suffisamment flexible pour former le premier standard mondial[100]. Une fois établie, l'agence pourrait ensuite s'atteler à l'élaboration d'un cadre réglementaire international détaillé et complet.

54. Cette réflexion institutionnelle met en lumière le besoin d'une stratégie sur le long-terme. Résoudre efficacement les problèmes actuels est une cause noble, mais la nature des défis en cause impose avant tout d'élaborer un système réaliste et complet pour l'avenir[101]. C'est le besoin d'une véritable coopération internationale par le biais d'une institution fonctionnant à l'image de l'Organisation Mondiale de la Propriété intellectuelle, chargée de faire progresser la protection de ladite propriété intellectuelle. Le choix concerté de cet appui institutionnel est donc le préalable nécessaire à toute négociation sur la substance.

55. L'Union européenne s'est quant-à-elle positionnée sur un double tableau. Supportant la création d'un cadre international, elle ne manque cependant pas de diffuser largement ses propres standards à travers le monde, comme le confirme le nouveau champ d'application du règlement. Ainsi, la tension entre les tentatives de création d'un cadre global et l'affirmation continue du droit européen soulève des questions quant à la meilleure façon pour l'Union de promouvoir la protection des données au niveau mondial[102]. C'est la volonté européenne de développer des valeurs globales tout en affirmant des valeurs régionales, allant jusqu'à être qualifiée de « *beautiful illusion* »[103]. En l'absence d'un cadre international, il semble pourtant justifié que l'Union applique ses standards de protection dès que les données d'un citoyen européen sont concernées et ce, indépendamment de la localisation du traitement.

56. Quoi qu'il en soit, le succès d'éventuelles négociations sur l'adoption d'un cadre global requerra nécessairement une meilleure compréhension réciproque des différentes approches

[98] P. DE HERT et V. PAPAKONSTANTINOU, *op. cit.*, p. 323.
[99] Assemblée Générale des Nations Unies, « Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel », adoptée le 14 décembre 1990 dans la résolution 45/95 du 14 décembre 1990.
[100] P. DE HERT et V. PAPAKONSTANTINOU, *op. cit.* p. 323.
[101] P. DE HERT et V. PAPAKONSTANTINOU, *ibidem.*
[102] C. KUNER, "Paper n°48/2015…", *op. cit.*, p. 55.
[103] C. KUNER, "Paper n°14/2016…", *op. cit.*, p. 4.

culturelles et légales en la matière[104]. L'imposition unilatérale d'instruments et de standards régionaux comme socle de départ pourrait s'avérer controversé, altérant gravement – sinon irrémédiablement – toute chance de succès. Notons cependant la forte probabilité que le droit de l'Union serve d'assise à l'élaboration d'un tel cadre global[105].

[104] C. KUNER, « Paper n°48/2015…", *op. cit.*, p. 66.
[105] A. DESFORGES, *op. cit.*, p. 85; Comme souligné par R. BENDRATH: beaucoup de pays adoptent des législations en matière de protection des données qui sont façonnées sur le modèle européen et ce, dans le but d'obtenir une décision d'adéquation de la Commission européenne ; Annexe I du présent document, *op. cit.*, p. 73.

Titre II – Les principes de la protection des données à caractère personnel (non) contenus dans l'accord 'Bouclier vie privée'

57. Il convient désormais de se plonger au cœur de l'accord afin d'analyser les principes dont l'application rythmera les échanges transatlantiques de données à caractère personnel. Négocié sous l'empire de la directive, l'accord consacre certains rudiments essentiels de la protection des droits fondamentaux des citoyens européens (Chapitre 1). Cependant, l'entrée en vigueur imminente du règlement[106] requiert d'anticiper certains amendements qui devront impérativement être apportés audit accord (Chapitre 2).

58. Notre étude veillera, autant qu'il se peut, à suivre une certaine systématicité. Nous aborderons d'abord le prescrit légal applicable à chaque principe, tant sous le champ d'application de la directive que celui du règlement. Les critiques formulées par le G29 et le contrôleur européen de la protection des données (ci-après, le contrôleur européen) suite à la divulgation d'une première version de l'accord serviront ensuite d'impulsion à une analyse critique du bien-fondé et de la faisabilité desdits principes au regard de cas d'application actuels.

Chapitre 1 – Examen des principes contenus dans l'accord

59. Ne pouvant prétendre à l'exhaustivité, une sélection de quatre principes servira de socle à nos développements. Amorçant avec le principe de conservation des données (Section 1), nous aborderons ensuite le traitement automatisé des données (Section 2), le principe de limitation des finalités (Section 3), le principe de choix (Section 4) et les limitations possibles à l'obligation d'adhésion audits principes (Section 5).

Section 1 – Le principe relatif à la conservation des données

60. Le principe de limitation de la conservation des données est un principe fondamental du droit européen de la protection des données. Consacré par la directive[107] et renforcé dans le règlement[108], ce dernier requiert que les données soient conservées uniquement pendant le

[106] 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.
[107] Art. 6, §1, e), de la directive.
[108] Art. 5, §1, e), du règlement.

temps nécessaire à la réalisation des objectifs ayant justifié la collecte des données ou leur traitement. En découle l'obligation de supprimer lesdites données dès l'instant où celles-ci ne sont plus nécessaires, sauf exceptions[109].

61. Dans son opinion du 13 avril 2016, le G29 s'inquiétait de l'absence de référence explicite à ce principe dans l'accord[110]. Cette carence permettait ainsi aux entreprises de conserver les données aussi longtemps qu'elles le souhaitent, même après avoir quitté l'accord. Cette crainte était partagée par le contrôleur européen, soulignant que seule la conservation des données traitées à des fins de renseignement était limitée à une période de cinq ans, « *à moins qu'il ne soit établi qu'elles répondent à un besoin de renseignement étranger autorisé ou* […] *qu'une conservation prolongée réponde aux intérêts de la sécurité nationale* [américaine] »[111]. Notons que cette formulation ne consolide pas le sort réservé à ces données, dont la durée de conservation dépendra de l'interprétation conférée à ces termes par le directeur du renseignement national américain.

62. Ces inquiétudes, manifestées en réaction à la divulgation d'une première version de l'accord, n'ont pas été ignorées. Les informations peuvent désormais être conservées sous une forme identifiant la personne concernée ou la rendant identifiable '*uniquement tant que cette conservation sert à atteindre l'objectif de traitement,* c'est-à-dire, les « *objectifs pour lesquels* [les données] *ont été collectées ou* […] *les objectifs approuvés ultérieurement par la personne concernée* »'[112]. S'en suivent diverses exceptions dont le contenu excède celui prévu par le futur règlement[113], permettant notamment la conservation prolongée des données pour des finalités de journalisme, de littérature et d'art[114].

---

[109] L'article 5, §1, e), du règlement prévoit des exceptions au principe de limitation de la conservation des données *:* « *les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques* », pour autant que les droits et libertés des personnes concernées soient protégés par des mesures techniques ou organisationnelles appropriées conformément à l'article 89, §1, du règlement.

[110] Pt. II. 5, de l'Annexe II, du Projet de décision sur le caractère adéquat du niveau de protection assuré par le bouclier de protection des données UE-Etats-Unis, publié le 27 février 2016.

[111] Pt. I, c), de l'annexe VI, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

[112] Pt. II. 5, b), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

[113] Art. 5, §1, e), du règlement.

[114] Pt. II. 5, b), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

63. Le contrôle de la conservation des données à caractère personnel est un enjeu majeur dans la gestion des risques liés à leur traitement. Plus attractives et lucratives que jamais, ces données stimulent les marchés, nous faisant glisser de l'ère du '*financial capitalism'* vers celle du '*data capitalism'*[115]. Ce phénomène de collecte et de commercialisation des données personnelles redessine la logique économique. Ces dernières se voient conférer le pouvoir de déterminer les valeurs financières et de redessiner l'exercice du pouvoir tout en s'introduisant dans les aspects les plus intimes de nos vies[116]. Nouvel or noir des économies modernes, les données personnelles émanent de plus en plus d'appareils connectés [américains] dont le nombre est amené à tripler d'ici 2020[117]. Leur conservation indue pourrait donc rapidement engendrer abus ou bévues.

64. Ainsi, l'industrie des 'données alternatives'[118] - vendant notamment des informations liées aux téléchargements d'application ou aux achats par cartes de crédit à des groupes d'investissement - a récemment fait l'objet de scandales pour avoir omis d'effacer de façon adéquate les données personnelles se trouvant sur le matériel vendu[119]. Ceci soulève la question de l'efficacité dans la mise en œuvre des règles de conservation, dont le contrôle ne semble pas aisé. En l'espèce, par crainte de poursuites judiciaires, ce sont les groupes d'investissement eux-mêmes qui ont alerté la commission fédérale du commerce, estimant que lorsque les choses vont mal, le plaignant se retourne toujours vers ceux qui ont les poches profondes[120].

65. Plus efficace qu'un mécanisme de contrôle externe, c'est un véritable autocontrôle qui s'est mis en place. Ceci présage de l'efficacité des sanctions financières mises en place par le règlement[121], dont la crainte suscitera peut-être, elle aussi, une forme d'autocontrôle. Cette illustration réaffirme l'importance d'un principe de conservation des données stricte et contrôlé, dont seul le temps permettra d'évaluer l'efficacité.

---

[115] J. THORNHILL, « Data capitalism is cashing in our privacy – for now », *FT*, jeudi 10 janvier 2017, p. 9.
[116] J. THORNHILL, *ibidem.*
[117] En 2020, le nombre d'appareils connectés pourrait s'élever à 20.8 milliards.
[118] Les données alternatives recouvrent tout ce qui est brut ou non-structuré, en comparaison aux dépôts des entreprises ou aux historiques des prix du marché. Pour plus d'information sur ce phénomène : M. TURNER, « This is the future of investing, and you probably can't afford it », 11 novembre 2015, http://www.businessinsider.com/hedge-funds-are-analysing-data-to-get-an-edge-2015-8 (consulté le 20 avril 2017).
[119] R. WIGGLESWORTH, « 'Alternative data' sellers fail to remove personal information, say hedge funds », *FT*, lundi 12 décembre 2016, p. 1.
[120] R. WIGGLESWORTH, *ibidem.*
[121] Art. 83, §5, du règlement : les autorités de contrôle disposeront désormais du pouvoir d'imposer une amende administrative pouvant s'élever jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire de l'entreprise.

Section 2 – Le traitement automatisé des données

66. La directive 95/46 reconnait à toute personne le droit de ne pas être soumis à « *une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement etc*. »[122].

67. Principe essentiel du droit à la protection des données, celui-ci est repris et précisé dans le nouveau règlement[123], y incluant expressément le profilage[124]. Cette disposition étend en outre les exceptions[125] possibles à cette interdiction, rappelant toutefois l'obligation pour le responsable de traitement de prendre toutes les mesures appropriées « *pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée* »[126]. Lorsqu'une décision automatisée produit des effets juridiques ou affecte de manière significative les personnes concernées, ces dernières disposent notamment du droit d'exprimer leur point de vue, d'obtenir une intervention humaine ou de contester la décision.

68. Soumis aux principes du droit à la protection des données, ces traitements automatisés appellent divers questionnements suscités par la difficulté de leur fonctionnement. Ainsi, en vertu du premier principe posé par le règlement, les données à caractère personnel doivent être traitées de manière « *licite, loyale et transparente* »[127]. Une brève analyse de l'application de ces trois impératifs aux traitements automatisés suffit à en comprendre la complexité.

69. En termes de licéité, le règlement pose le 'consentement explicite de la personne concernée' comme exemption à l'interdiction de prise de décision automatisée. Mais qu'est-ce qu'un consentement éclairé dans le cadre d'un traitement parfois intrinsèquement opaque ?

---

[122] Art. 15, et considérant 41, de la directive.
[123] Art. 22, §1, et considérant 71, du règlement.
[124] Art. 4, § 4, du règlement : Le profilage est défini comme étant « *toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique* ».
[125] Art. 22, §2, a), b) et c), du règlement.
[126] Art. 22, §3, du règlement.
[127] Art. 5, §1, a), du règlement.

Bien qu'une explication technico-scientifique soit possible, seule une information limpide permettra de satisfaire l'exigence d'un consentement éclairé[128].

70. En termes de loyauté, les exigences d'une impartialité sans faille sont également difficiles à préserver. Les algorithmes peuvent être biaisés à différents stades, tant dans leur conception que dans la sélection des données à traiter. Ainsi, la sous-représentation d'une minorité dans les données historiques est susceptible de renforcer la discrimination à leur égard dans le cadre d'un processus de recrutement par exemple[129].

71. L'identification et le contrôle de cette subjectivité est l'un des défis fondamentaux dans la conception et l'évaluation de ces nouvelles technologies[130]. Comme souligné par Giovanni BUTTARELLI, « *la technologie n'est pas neutre en termes de valeur* »[131], ce qui l'amène à penser que « *si nous inscrivions une approche éthique dans le développement de toutes les innovations significatives, nous encouragerions le progrès et assurerions une société qui repose sur les valeurs humaines* »[132]. C'est l'éthique comme remède face à ce qui nous dépasse. Ce binôme éthique-droit pourrait jouer tant au stade de la conception des algorithmes qu'à celui de la vérification périodique de leur bon fonctionnement[133].

72. En termes de transparence, le règlement impose de fournir à la personne concernée 'les informations utiles concernant la logique sous-jacente' au traitement automatisé[134]. L'objectif poursuivi par cette disposition impose d'interpréter cette exigence du point de vue de la personne concernée[135]. C'est donc logiquement une information non-technique de haut niveau qui devra être transmise plutôt que le code algorithmique[136]. Les législateurs nationaux ainsi

[128] C. KUNER (C.) *et al.*, « Machine learning with personal data: is data protection law smart enough to meet the challenge », *International Data Privacy Law*, vol. 7, n° 1, Oxford University Press, 2017, p. 1.
[129] C. KUNER *et al.*, *ibidem*, p. 2.
[130] C. KUNER *et al.*, *ibidem.*
[131] G. BUTTARELLI, « La vie privée et l'émergence des nouvelles technologies – Le point de vue de l'Union européenne », La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux. Actes du colloque du 17 octobre 2016, Sénat de Belgique, Bruxelles, 2016, p. 26.
[132] G. BUTTARELLI, *ibidem*.
[133] Un 'groupe consultatif sur l'éthique' a été institué par la décision 2016 C 33/01 du contrôleur européen de la protection des données du 3 décembre 2015 instituant un groupe consultatif externe sur les dimensions éthiques de la protection des données (groupe consultatif sur l'éthique), *J.O.U.E.*, C 33/1 du 28 janvier 2016. Ce groupe a pour but de mieux comprendre les relations entre la technologie, les droits de l'homme, les marchés et les modèles d'entreprise au XXIème siècle, sous l'angle éthique. Celui-ci met surtout l'accent sur les implications et les conséquences pour le droit à la protection des données dans le contexte de l'environnement numérique.
[134] Art. 13, §2, f), et art. 14, §2, g), du règlement.
[135] C. KUNER *et al.*, *op. cit.*, p. 2.
[136] C. KUNER *et al.*, *ibidem.*

que les Cours et Tribunaux pourraient aller jusqu'à contraindre les contrôleurs de données à fournir une explication détaillée dans des cas spécifiques[137].

73. Rempart contre une 'gouvernementalité algorithmique'[138], cette exigence semble pourtant difficilement applicable. La situation des Pays-Bas en est un exemple instructif. Parvenant à détecter la quasi-totalité des cas de fraude grâce à l'utilisation du *Big Data*, les autorités néerlandaises seraient cependant incapables de fournir les raisons d'un résultat particulier en cas de contestation[139]. Ceci démontre que transformer le *Big Data* en renseignements est le travail des algorithmes[140] ; il ne reste plus qu'à en comprendre le fonctionnement, faute de quoi leur contrôle ne sera que chimère.

74. Inclus dans la directive, précisé dans le règlement et faisant l'objet d'une Convention spécifique du Conseil de l'Europe[141], ce principe n'a pourtant pas retenu l'attention des négociateurs de l'accord. Or, comme souligné par le G29[142] et le contrôleur européen[143], le progrès technique rend désormais indispensable la mise en place de garanties légales en cas de décisions automatisées[144]. L'évolution rapide des nouvelles technologies permet à un nombre croissant d'entreprises d'adopter des systèmes de prise de décision automatisée, laissant les individus concernés sans recours face à des ordinateurs toujours plus puissants.

75. Bien qu'actuellement passées sous silence, les négociations sur ce point semblent avoir été postposées au premier 'réexamen conjoint du fonctionnement du bouclier vie privée'[145]. Judicieuse manœuvre politique, ce report témoigne de la complexité soulevée par cette question

---

[137] Considérant 71 du règlement, qui n'a cependant pas un caractère obligatoire ; C. KUNER *et al*., *op. cit*., p. 2

[138] A. ROUVROY et T. BERNS, « Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation ? », *Politique des algorithmes. Les métriques du web*, Réseaux, vol. 31, n°177, 2013, pp. 163-196 ; M. GUGAIN et C. LABBÉ, *L'Homme Nu. La dictature invisible du numérique*, Paris, Robert Laffont, 2016, p. 31.

[139] Annexe II du présent document, *op. cit*., p. 80.

[140] C. CHACE, *Surviving AI. The Promise and peril of artificial intelligence*, Three Cs Publishing, 2015, p. 20.

[141] Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *STE 108*, Strasbourg, 28 janvier 1981.

[142] G29, "Opinion n°01/2016 on the EU-U.S. Privacy Shield draft adequacy decision", *WP238*, 13 avril 2016, p. 17.

[143] CEPD, « Avis n°4/2016 concernant le 'Bouclier vie privée UE-Etats-Unis (Privacy Shield). Projet d'adéquation », 30 mai 2016, p. 9.

[144] Sur l'importance d'encadrer les algorithmes prédictifs, voy. Conseil d'Etat français, Etude annuelle 2014 – Le numérique et les droits fondamentaux, *EDCE*, n°65, France, 2014.

[145] Considérant 25 et annexe I, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

et de la difficulté déjà anticipée d'un compromis. Quoi qu'il en soit, le principe devra au minimum répondre aux exigences posées par le nouveau règlement[146].

76. A l'aune de ces incertitudes, le développement des algorithmes a suscité chez les commentateurs des réactions variables. Pour certains, nous avançons vers une démocratie fragilisée assortie d'une augmentation des inégalités[147]. Les démocraties s'essouffleraient, autant que leur système de représentation, entrainant « *un mode de société où Etat nation et classe politique vont s'évaporer jusqu'à disparaitre* »[148]. Pour d'autres, les décisions automatisées peuvent être soumises à des mécanismes de responsabilité et de gouvernance grâce auxquels les avantages escomptés l'emporteront sur les préjudices potentiels[149].

77. Les craintes sont légitimes et les espoirs justifiés. Il ne faut cependant pas oublier que les prises de décision humaines sont également empreintes de subjectivité, consciente ou inconsciente[150]. Ceci a amené certains auteurs à imaginer un algorithme dont l'objet consisterait à vérifier la licéité, la loyauté et la transparence des décisions humaines ou automatisées[151]. Alors que le règlement prévoit l'intervention humaine en cas de décision automatisée, c'est le système inverse que certains préfèreraient voir triompher. A accueillir dans son principe, cette idée semble à l'heure actuelle relever de l'utopie. C'est la quête d'une impartialité décisionnelle que l'être humain n'a pas été pleinement en mesure de fournir. Les technologies en seront-elles capables ?

Section 3 – Le principe de (l'intégrité des données et) limitation des finalités

78. Une organisation ne peut traiter des données à caractère personnel « *d'une manière incompatible avec la finalité pour laquelle elles ont été initialement collectées ou avec une*

[146] Notons que le droit américain ne protège les décisions prises sur la base d'un traitement automatisé que dans trois cas particuliers, chacun d'entre eux faisant l'objet d'un acte spécifique : the Equal Credit Opportunity, the Fair Credit Reporting Act et the Fair Housing Act.
[147] C. O'NEIL, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Allen Lane, 2016.
[148] M. DUGAIN et C. LABBÉ, *op. cit.*, p. 31. Les auteurs estiment que les élections politiques deviendront obsolètes vu la capacité du *Big Data* à déterminer, en temps réel, la réaction de tout individu à toute proposition relative à l'organisation collective de la société.
[149] C. KUNER *et al.*, *op. cit.*, p. 2.
[150] C. KUNER *et al.*, *ibidem.*
[151] J. KROLL *et al.*, "Accountable algorithms", *University of Pennsylvania Law Review*, vol. 165, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765268 (consulté 7 juillet 2017).

finalité approuvée ultérieurement par la personne concernée »[152]. Ainsi, lorsque des données sont transférées de l'Union vers les Etats-Unis, l'exportateur européen devrait expressément informer l'organisation américaine des finalités pour lesquelles lesdites données ont été initialement collectées[153]. Ceci est essentiel afin de déterminer un éventuel changement de finalité après le transfert - déclenchant l'application du principe de 'notification et de choix'- et participerait à l'allocation des risques et à la détermination des responsabilités[154].

79. Limpide dans le règlement, ce principe a pourtant été pauvrement consacré dans l'accord. Deux inquiétudes soulevées par le G29 suffisent à le démontrer, bien que celles-ci soient *in fine* restées sans réponse.

80. Premièrement, la notion de 'compatibilité du traitement' n'est appréhendée que par le truchement d'une liste exemplative non-exhaustive[155] contenant quelques situations-types. Le règlement apporte à cet égard plus de précisions, grâce à l'instauration de cinq critères d'appréciation de cette compatibilité[156]. Non-exhaustifs, ceux-ci confèrent à l'examen de compatibilité un caractère plus objectif et instaure une sécurité juridique accrue.

81. Deuxièmement, l'accord prévoit que le traitement soit limité aux seules informations 'pertinentes à des fins de traitement'[157]. Pour le G29, le caractère pertinent de l'information ne suffit pas à rendre le traitement proportionné ; le traitement aurait dû être limité aux données 'nécessaires pour le traitement considéré'.

82. D'apparence théorique, ce principe de 'limitation des finalités' n'a pourtant pas tardé à se retrouver au cœur d'un scandale. WhatsApp, appartenant à Facebook depuis 2014, avait annoncé au mois d'août 2016 qu'elle s'apprêtait à partager les données de ses utilisateurs avec

---

[152] Pt. II. 5, de l'annexe II, et considérant 21, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[153] G29, "Opinion n° 01/2016… », *op. cit.*, p. 24.
[154] G29, *ibidem*.
[155]Pt. II. 5, a), note (1), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016 : : *« Selon les circonstances, les finalités de traitement compatibles peuvent par exemple comprendre celles qui ont raisonnablement pour objectif les relations avec la clientèle, le respect de la réglementation et les considérations juridiques, l'audit, la sécurité et la prévention de la fraude, la préservation ou la défense des droits de l'organisation reconnus par la loi, ou d'autres finalités conformes aux attentes d'une personne raisonnable compte tenu du contexte dans lequel s'inscrit la collecte ».*
[156] Art. 6, §4, du règlement.
[157] Pt. II. 5, a), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

le réseau social. En réaction à cette annonce, le G29 avait adressé une lettre ouverte à l'entreprise[158], exprimant sa vive inquiétude concernant le partage d'information réalisé au sein de la 'famille d'entreprises Facebook' pour des finalités qui n'étaient pas comprises dans les conditions d'utilisation et la politique de confidentialité de l'entreprise au moment où les utilisateurs existants ont souscrit au service de messagerie ; le G29 exigeait l'arrêt du partage des données jusqu'à ce que des garanties juridiques appropriées soient apportées.

83. Une brève lecture de la politique de confidentialité de WhatsApp[159] suffit à saisir les craintes suscitées dans le chef du G29. Après avoir précisé que Facebook pouvait utiliser les informations fournies par WhatsApp afin de « *faire des suggestions de produits* […] *et afficher des offres et des publicités pertinentes* », le texte continue en précisant qu'en fait, « *Facebook n'utilisera pas* [les] *messages WhatsApp dans un but autre que celui d'aider* [WhatsApp] *à exploiter et fournir* [ses] *services* ». Texte court et termes flous semblent être le rempart utilisé par la 'famille d'entreprises Facebook', s'aménageant une marge de manœuvre confortable en cas de changement de cap ultérieur.

84. Après l'Allemagne[160] et le Royaume-Uni, c'est donc dans toute l'Union que Facebook a dû cesser d'exploiter les données à caractère personnel des utilisateurs de WhatsApp[161]. Outre le manque de clarté sur l'utilisation des données et les doutes relatifs à la validité du consentement des utilisateurs[162], c'est aussi une confiance rompue que ce scandale met à jour. En 2014, Facebook et WhatsApp avaient en effet déclaré publiquement qu'un partage de données entre les deux entités n'aurait jamais lieu. Selon la Commission européenne, Facebook

[158] I. FALQUE-PIERROTIN, Présidente du G29, « Lettre ouverte à WhatsApp », Bruxelles, 27 octobre 2016, https://www.cnil.fr/sites/default/files/atoms/files/20161027_letter_of_the_chair_of_the_art_29_wp_whatsapp.pdf

[159] Politique de confidentialité de WhatsApp, https://www.whatsapp.com/legal/#privacy-policy-affiliated-companies (consulté le 20 avril 2017).

[160] BfDI, « Press Release – Administrative order against the mass synchronization of data between Facebook and WhatsApp", 27 septembre 2016, https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Press_Release_2016-09-27_Adminstrative_Order_Facebook_WhatsApp.pdf; M. MURGIA et G. CHAZAN, "Germany bans Facebook-WhastApp sharing', *FT*, mercredi 28 septembre 2016, p. 3.

[161] M. MURGIA et G. CHAZAN, "Germany bans Facebook-WhatsApp sharing", *FT*, mercredi 28 septembre 2016, p. 13.

[162] M. TUAL, « Facebook cesse d'exploiter les données des utilisateurs européens de WhatsApp », *Le Monde*, 18 novembre 2016, http://www.lemonde.fr/pixels/article/2016/11/17/facebook-cesse-d-exploiter-les-donnees-des-utilisateurs-europeens-de-whatsapp_5032943_4408996.html (consulté le 22 avril 2017).

lui a fourni des « *informations trompeuses* »[163] au moment du rachat, dans le but d'obtenir son feu vert ; une manœuvre qui a coûté cher au géant américain[164].

85. La condamnation Facebook-WhatsApp par la Commission européenne s'inscrit tant sur le terrain de la protection des données que sur celui du droit de la concurrence. Ce constat souligne deux choses. Premièrement, la tension croissante entre le droit européen de la protection des données et le modèle économique d'entreprises telles que Facebook ou Google. Deuxièmement, la difficulté pour les autorités de concurrence de réglementer un marché sans prix, où les individus échangent leurs données contre des services gratuits[165].

86. A cet égard, l'utilisation par la Commission du droit de la concurrence en matière de protection des données a fait l'objet de réactions variables ; pour certains,[166] cela est prometteur mais pour d'autres[167], c'est effrayant. La raison de ce scepticisme trouve son fondement dans une comparaison UE-U.S. Alors que le droit de l'Union comprend le droit à la protection des données et le droit à la vie privée, les Etats-Unis ne connaissent que ce dernier[168]. Dès lors, un litige américain en matière de protection des données relève du seul contrat conclu encore l'entreprise et le consommateur concernés[169]. Ne disposant d'aucune compétence en la matière, l'Etat n'a d'autre choix que de faire jouer le droit de la concurrence. Une telle justification est inexistante au sein de l'Union.

Section 4 – Le principe 'choix'

87. L'accord fonctionne sur la base d'un système de 'droit de refus' ou principe 'choix', selon lequel les personnes concernées doivent se voir offrir la possibilité de décider si leurs

[163] Commission européenne, « Concentrations : la Commission affirme que Facebook a communiqué des informations trompeuses sur le rachat de WhatsApp », *Communiqué de Presse*, *IP-16-4473*, 20 décembre 2016 ; M. MURGIA et R. TOPLENSKY, « Facebook fined over WhatsApp deal », *FT*, jeudi 18 mai 2017, p. 11.
[164] Facebook a été condamné à une amende de 110 millions d'euros ; Commission européenne, « Mergers : Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover », *Communiqué de Presse, IP/17/1369*, 18 mai 2017.
[165] R. TOPLENSKY *et al.*, "Facebook faces more hurdles after Europe fine", *FT*, 22 mai 2017, p. 9.
[166] Y. POULLET, « Le point de vue de la société sur le sentiment de traçabilité », La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux. Actes du colloque du 17 octobre 2016, Sénat de Belgique, Bruxelles, 2016, p. 63.
[167] Annexe II du présent document, *op. cit.*, p. 85.
[168] F. GIRARD, « La notion de vie privée aux Etats-Unis », *Le droit à l'oubli numérique*, Bruxelles, Larcier, 2015, p. 200 et s.
[169] Dans ce sens, voy. C. MANNY, « Incomplete privacy : how federal law misses problems connected to the U.S. consumer data base industry », *Défis du droit à la protection de la vie privée – perspectives du droit européen et nord-américain, Cahiers du Centre de Recherches Informatique et Droit*, vol. 31, Bruxelles, Bruylant, 2008, p. 72 et s.

données à caractère personnel peuvent : (i) être divulguées à une tierce personne ou (ii) être utilisées « *dans un but matériellement différent du ou des objectifs pour lesquels les données ont été initialement collectées ou du ou des objectifs approuvés ultérieurement* » par elles[170].

88. D'une manière générale, ce principe vise à assurer que les données à caractère personnel sont collectées et utilisées suivant les attentes et les choix de la personne concernée[171]. Ce système ne correspond cependant pas à celui applicable par défaut en droit européen, régi par le système inverse[172]. Soumis à de vives critiques du Groupe des verts au Parlement européen, ce principe 'choix' serait tant inadapté dans son principe qu'indument restrictif dans son application[173]. Afin d'en comprendre la teneur, nous analyserons l'avis du G29 pour ensuite évaluer de façon plus globale l'efficacité d'un tel système binaire.

89. En ce qui concerne l'accord, ce droit de refus – bien que clairement mentionné – n'est pas explicité dans ses modalités[174]. En réaction à cette carence, le G29 s'était notamment attelé à formuler deux recommandations, accueillies très variablement.

90. Premièrement, le G29 invoquait qu'une 'opportunité individualisée' d'exercer ce droit de refus devait être offerte par l'entreprise à toute personne concernée, avant que les données à caractère personnel ne soient divulguées ou réutilisées. Une simple référence à ce droit dans la politique de confidentialité de l'entreprise ne peut - à elle seule - suffire. Cela dépendra donc de la volonté des entreprises d'investir leurs consommateurs du pouvoir de dire 'non'.

91. Deuxièmement, un 'droit général de contestation' aurait dû être proposé dans l'accord. Celui-ci devant être compris comme le droit pour la personne concernée de solliciter la fin du traitement chaque fois qu'il existe des raisons impérieuses et légitimes concernant sa situation personnelle. Cette idée figure déjà dans le règlement[175], mais n'est précisée dans l'accord qu'en cas d'action de marketing direct[176]. Le G29 recommandait qu'un tel droit soit explicitement

[170] Considérant 22 et pt. II. 2, a), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[171] Pt. III. 12, a), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[172] Système du *opt-in*.
[173] Le droit de refus n'est en effet possible que dans les deux hypothèses mentionnées.
[174] Seule l'hypothèse d'une 'action de marketing direct' bénéficie de plus amples précisions, tant temporelles que techniques.
[175] Considérant 47 du règlement.
[176] Pt. III. 12, a), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

reconnu, à tout moment, et au-delà des seuls cas de marketing direct. Cette revendication est cependant restée sans réponse[177].

92. Après avoir brièvement exposé le principe du 'droit de refus' et les recommandations du G29, il convient de prendre du recul quant au bien-fondé d'un tel système. En effet, le débat ne devrait pas être réduit à un simple choix consistant soit, à exiger des entreprises de recueillir l'approbation du client avant de vendre ses données à caractère personnel soit, autorisant celles-ci à les utiliser à moins que le client n'en décide autrement. Pour être plus efficace, cette dynamique binaire devrait s'accompagner de consommateurs mieux informés, disposant de plus d'options[178]. Nous esquisserons ici deux pensées, soulignant les faiblesses du système en place et les espoirs suscités par un système repensé.

93. Premièrement, les utilisateurs d'internet ne connaissent pas suffisamment le monde numérique et les dossiers digitaux les concernant. Les données personnelles sont difficilement accessibles[179] et très éparses. Une réglementation raisonnable impliquerait donc une 'dynamique informationnelle active'[180] et non réactive de la part des entreprises. La partie faible, le consommateur, devrait ainsi recevoir l'information et non la requérir ; la divulgation des informations devrait à tout le moins être 'à portée de clic'[181] et des notifications périodiques[182] relatives aux informations collectées devraient être envoyées.

94. Cette vision, exigeant la mise à nu des entreprises, souligne qu'en matière de protection des données, il y a des 'forts' – les entreprises - et des 'faibles' – les consommateurs. Le système actuel fonctionne selon une dynamique exigeant des faibles qu'ils s'informent, qu'ils choisissent et qu'ils réagissent, alors que les entreprises continuent à collecter des données dont l'étendue est généralement connue mais individuellement ignorée. Bien que renforcé et précisé, le droit de refus prévu dans l'accord semble donc illusoire en l'absence de consommateurs dûment tenus informés.

---

[177] Commission des libertés civiles, de la justice et des affaires intérieures, "Draft Motion n°2016/3018 (RSP) for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-U.S. Privacy Shield", 7 décembre 2016, p. 5, pt. 8.

[178] « Digital privacy is more than just opting in or out », *FT*, Samedi 1er avril 2017, p. 8.

[179] A titre personnel, nous avons entrepris les démarches nécessaires auprès de Facebook afin d'obtenir le résumé des données collectées à notre égard ; aucune réponse n'a été reçue.

[180] Par l'entremise de ce concept, nous affirmons que les entreprises ne devraient pas réagir aux demandes d'information faites par les consommateurs, mais informer elles-mêmes ponctuellement les consommateurs des données collectées à leur égard et ce, pour qu'ils puissent exercer leurs droits de façon éclairée.

[181] « Digital privacy is more than just opting in or out », *FT*, Samedi 1er avril 2017, p. 8.

[182] *ibidem.*

95. Deuxièmement, comme en atteste la célèbre citation de Tim Cook « *si c'est gratuit, vous êtes le produit* », nous sommes passés à un modèle économique nouveau où les services ne sont plus échangés contre de l'argent mais contre des données personnelles[183]. Selon certains[184], la prochaine révolution est imminente, et impliquera de donner aux consommateurs le contrôle de leurs données.

96. Cette 'émancipation' pourrait passer par l'offre d'un choix nouveau, dont la logique binaire ne s'apprécierait plus sous l'angle des entreprises mais des consommateurs. Il s'agirait de permettre aux clients de payer l'utilisation de Google ou de Facebook[185], restaurant un modèle économique ancien aux côtés du modèle actuel. La contrepartie financière impliquerait de ne plus voir de publicités et d'obtenir la garantie qu'aucune information à caractère personnel n'est collectée. Selon ses chiffres[186], chaque utilisateur américain rapporterait à Facebook la somme de six dollars par mois contre deux dollars pour un européen[187]. Les utilisateurs du réseau social pourraient faire le choix de payer cette somme, profitant des capacités technologiques de Facebook à des fins de protection et non plus de collecte des données[188]. Pour certains, cette possibilité serait précieuse et pour d'autres, elle serait l'occasion de comprendre les concessions qu'ils réalisent, tous les jours.

Section 5 – Les limitations à l'obligation d'adhésion aux principes

97. L'accord prévoit diverses exemptions aux principes[189] dont l'évaluation dépend d'une parfaite connaissance du droit américain, tant fédéral qu'étatique. Le G29 avait à cet égard

[183] C. DEFRAIGNE, « Mot de bienvenue », La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux. Actes du colloque du 17 octobre 2016, Sénat de Belgique, Bruxelles, 2016, p. 9.
[184] J. THORNHILL, *op. cit.*, p. 9.
[185] « Digital privacy is more than just opting in or out », *FT*, Samedi 1er avril 2017, p. 8.
[186] Facebook Reports Fourth Quarter and full Years 2016, 1er février 2017, Californie, https://s21.q4cdn.com/399680738/files/doc_financials/2016/Q4/Facebook-Reports-Fourth-Quarter-and-Full-Year-2016-Results.pdf
[187] Ces chiffres concernent l'année 2016.
[188] Abstraction faite des considérations relatives à la faisabilité d'un tel système pour l'entreprise et des coûts que la création de ce nouveau modèle générerait pour Facebook.
[189] Pt. I. 5, de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016 : « *L'adhésion aux principes peut être limitées par : a) les exigences relatives à la sécurité nationale, l'intérêt public et le respect de la législation ; b) les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation puisse démontrer que le non-respect des principes est limité dans la mesure nécessaire pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir ; ou c) les exceptions ou les dérogations prévues par la directive ou par le droit national, à condition que ces exceptions ou dérogations soient appliquées dans des contextes comparables* […] ».

souligné la difficulté d'évaluer la portée de ces exceptions et leur caractère justifiable dans une société démocratique. C'est pourquoi le groupe de travail en appelait à une Union vigilante et continument informée des modifications législatives ou réglementaires survenant aux Etats-Unis, qui seraient de nature à affecter une pleine adhésion aux principes[190].

98. Les récentes élections américaines ont confirmé les craintes du G29, amenant l'Union à déclarer qu'elle continuera à « *suivre de près* […] *le moindre changement aux Etats-Unis qui pourrait avoir un impact sur les droits des Européens en matière de protection de leurs données personnelles* ». Les réformes américaines sont désormais lancées, rythmant les réactions et les inquiétudes outre-Atlantique.

99. Ainsi, après avoir appelé les agences gouvernementales à s'assurer que leur politique de vie privée excluait les non-citoyens américains et les non-résidents permanents[191], Donald TRUMP continue à semer le trouble en Europe. Le 3 avril 2017, le Président américain a en effet promulgué l'abrogation des règles relatives à la protection des données à caractère personnel des utilisateurs sur internet[192]. Alors que les fournisseurs d'accès à internet étaient soumis à l'obligation de recueillir l'accord des consommateurs avant de vendre leurs données, ils sont désormais libres de toute contrainte. Cette illustration confirme le besoin d'une Europe vigilante face à une Amérique en voie de dérèglementation, risquant de *« refroidir tous les alliés internationaux qu'*[elle] *aurait pu conserver si* [elle] *avait choisi une autre orientation* »[193].

[190] G29, "Opinion n°01/2016… », *op. cit.*, p. 17.
[191] La 14ème clause du décret anti-immigration promulgué par le Président Donald TRUMP – et désormais partiellement remis en vigueur par la Cour Suprême des Etats-Unis, dans l'attente de l'examen du dossier en octobre 2017 - dispose que : *« les agences gouvernementales devront, dans la mesure où ceci est compatible avec la loi en vigueur, s'assurer que leur politique de vie privée exclut les non-citoyens américains et les non-résidents permanents des protections offertes par le Privacy Act au regard des informations personnelles* ». J.-P. ALBRECHT avait immédiatement réagi par un Twitt, posté le 26 janvier 2017 à 10 :45 : « *if it is true, the EU Commission has to immediately suspend the Privacy Shield* […]".
[192] « Digital privacy is more than just opting in or out », *FT*, Samedi 1er avril 2017, p. 8.
[193] E. MOROZOV, « Trump rouvre le marché des données personnelles », *Le Monde diplomatique*, 31 mars 2017, https://blog.mondediplo.net/2017-03-31-Trump-rouvre-le-marche-des-donnees-personnelles (consulté le 15 avril 2017).

Chapitre 2 – Vers une inéluctable mise à jour de l'accord

100. Comme souligné par le contrôleur européen, une solution relative aux transferts de données de l'Union vers les Etats-Unis ne peut prétendre à une quelconque stabilité sans la prise en compte des nouvelles exigences posées par le règlement[194]. La Commission est donc appelée à prendre toutes les mesures nécessaires afin d'assurer une pleine conformité de l'accord[195]. C'est dans cette optique que nous analyserons deux des principes nouvellement adoptés par le règlement : la protection des données dès la conception et la protection des données par défaut (Section1) ainsi que la portabilité des données (Section 2).

Section 1 – La protection des données dès la conception et la protection des données par défaut[196]

101. Après avoir défini les contours de ces nouvelles exigences, nous supputerons leurs implications pratiques pour les entreprises établies aux Etats-Unis.

102. Développé à l'initiative du préposé à la protection des données de l'Etat d'Ontario au Canada[197], le principe de 'protection des données dès la conception'[198] oblige le responsable du traitement à prendre des « *mesures techniques et organisationnelles appropriées* » - tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même – afin de « *répondre aux exigences du règlement et de protéger les droits de la personne concernée* »[199]. Ainsi, pour chaque nouvelle application, service ou produit traitant des données à caractère personnel, le plus haut niveau possible de protection des données devra être offert[200].

---

[194] CEPD, « Avis n°4/2016 concernant le 'Bouclier vie privée UE-Etats-Unis (Privacy Shield) Projet d'adéquation », 30 mai 2016, p. 2.

[195] Commission des Libertés civiles, de la justice et des affaires intérieures, "Draft Motion n°2016/3018 (RSP) for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-U.S. Privacy Shield", 7 décembre 2016, p. 5, pt. 14.

[196] Art. 25 du règlement. En anglais: 'Privacy by design' et 'Privacy by default'.

[197] A. CAVOUKIAN, "Operationalizing Privacy by Design: a guide to implementing strong privacy practices", Information and Privacy Commissioner, Ontario, Canada, décembre 2012, p. 1, http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf

[198] Pour plus d'information, BfDI, « Privacy by design », 19 mars 2010, https://link-springer-com.uaccess.univie.ac.at/content/pdf/10.1007%2Fs12394-010-0055-x.pdf

[199] Art. 25, §1, du règlement.

[200] CNDP, « Privacy by Design : le respect de la vie privée dès la conception », Grand-Duché du Luxembourg, 18 mai 2015, https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/ (consulté le 11 juillet 2017).

103. Le principe de 'protection des données par défaut' est intrinsèquement lié au premier, obligeant le responsable du traitement à prendre les mesures appropriées afin de garantir que, par défaut, « *seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées* »[201] et ce, au regard de la quantité de données traitées, de leur durée de conservation et de leur accessibilité.

104. La volonté du législateur européen est de rendre plus dynamique et plus efficace la protection des droits fondamentaux[202] en renforçant les principes classiques de nécessité, de finalité, de proportionnalité et de transparence par le truchement de nouveaux principes[203]. Pour ce faire, « *de nouvelles manières innovantes d'être informé de ce qui est fait avec leurs données et d'exercer un contrôle sur celles-ci* »[204] doivent être proposées aux personnes concernées. Cela confirme le besoin déjà mentionné d'une 'dynamique informationnelle active'.

105. Dans le contexte transatlantique, l'accord n'a quant-à-lui pas encore consacré ces principes. Il est dès lors important d'en appréhender les potentielles implications et les difficultés au départ d'un cas concret : WhatsApp et la protection des données dès la conception. Deux points de vue peuvent être adoptés en l'espèce, entrainant des conclusions antagonistes.

106. Selon le premier, WhatsApp respecte l'exigence de 'protection des données dès la conception'. L'application a récemment mis en place le '*chiffrement de bout en bout'*, assurant que les messages, photos, vidéos, messages vocaux et documents ne pourront pas être lus ni écoutés par WhatsApp ou des tiers[205]. Réduire au minimum le traitement de données personnelles est ainsi un moyen efficace de mettre en œuvre ce principe et d'améliorer la sécurité des données[206]. Moins la collecte des données est grande, plus les chances de conformité avec le droit de la protection des données sont élevées. Selon ce point de vue, l'approche adoptée par WhatsApp parait donc être en ligne avec le texte et l'esprit du règlement.

---

[201] Art. 25, §2, du règlement.
[202] CEPD, « Avis n°7/2015 - Relever les défis des données massives : un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition des comptes », 19 novembre 2015, p. 4.
[203] Voy. GDPR.expert, l'outil d'analyse du nouveau règlement européen, Cabinet Ulys, https://www.gdpr-expert.eu/article.html?id=25#ouvaton (consulté le 14 juillet 2017)
[204] CEPD, « Avis n°7/2015… », *op. cit.*, p. 17, pt. 4.
[205] Politique de confidentialité de WhatsApp, https://www.whatsapp.com/legal/#privacy-policy-affiliated-companies (consulté le 14 juillet 2017).
[206] Art. 25 et considérant 78 du règlement ; K. BRAHMBHATT, « Privacy by design – is there such a thing as too much?", Londres, 12 avril 2016, http://aodigitalhub.com/2016/04/12/privacy-design-thing-much/ (consulté le 15 juillet 2017).

107. Selon le second, WhatsApp met en danger la sécurité (inter)nationale. Alors que le nouveau règlement promet d'harmoniser l'application du droit européen de la protection des données au sein de l'Union, celui-ci risque aussi de creuser davantage le fossé entre le régulateur européen et les agences gouvernementales à travers le monde[207]. Le problème soulevé par le '*chiffrement de bout en bout*' est la création corrélative d'une sorte de '*Dark net*' sur lequel des activités illicites peuvent avoir lieu en toute discrétion, risquant de mettre en péril la sécurité de la population. Cherchant à se conformer au principe de 'protection des données dès la conception', WhatsApp pourrait donc se retrouver dans une situation comparable à celle de la 'marque à la pomme' dans la récente affaire *Apple c. FBI*[208].

108. Cette crainte doit cependant être relativisée compte tenu du type d'information visé par le cryptage. Seul le contenu au sens strict est ici concerné (les photos, le texte etc.) et non pas les métadonnées générées par l'utilisation de services tels que WhatsApp[209]. La localisation, l'identité des utilisateurs ou encore la durée des appels sont des données collectées par le fournisseur de télécommunication[210]. Le recoupement de ces métadonnées, disponibles pour les autorités publiques, permet déjà la création de profils précis grâce à une méthode de 'chainage'[211].

109. Cette question du cryptage a fait l'objet d'un regain d'activité suite aux attaques de Londres en mars 2017. Le gouvernement britannique a en effet sollicité la création d'une 'porte dérobée' au sein du service de messagerie Whatsapp, qui lui permettrait d'accéder à l'ensemble

---

[207] K. BRAHMBHATT, *op. cit.* ; 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.

[208] Le procès a été abandonné par le FBI en mars 2016 car l'agence gouvernementale était finalement parvenue à déverrouiller l'IPhone du tueur de San Bernardino sans l'aide d'Apple ; J. RIBEIRO, "Google, Facebook et Microsoft prêts à soutenir Apple face au FBI », *LeMondeInformatique.fr*, 26 février 2016.

[209] Notons la différence fondamentale entre l'Union européenne et les Etats-Unis. En Europe, la vie privée commence avec les métadonnées. Outre Atlantique, les métadonnées ne sont pas couvertes par la vie privée ; Ceci est confirmé dans la célèbre affaire United States Supreme Court, n° 78-5374, *Smith c. Maryland*, 442 U.S. 735, du 20 juin 1979 : la Cour suprême américaine a jugé que les métadonnées téléphoniques ne jouissaient pas de la protection prévue par le quatrième amendement de la Constitution américaine, contrairement au contenu de la conversation téléphonique pour lequel la délivrance d'un mandat était nécessaire. La Cour avait ainsi appliqué la doctrine de la 'tierce partie', en vertu de laquelle un individu renonce à la protection de ses données à caractère personnel lorsqu'il fournit volontairement une information à une tierce partie. Les numéros de téléphone n'étaient donc pas protégés en ce qu'ils avaient été volontairement communiqués à la compagnie téléphonique lors de la composition dudit numéro ; G. RAPAILLE, « La protection de la vie privée dans le domaine de la sécurité et de la vie publique », La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux. Actes du colloque du 17 octobre 2016, Sénat de Belgique, Bruxelles, 2016, p. 35.

[210] Annexe II du présent document, *op. cit*., p. 90.

[211] E. KINDT, « Vie privée et vie publique en Belgique », La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux. Actes du colloque du 17 octobre 2016, Sénat de Belgique, Bruxelles, 2016, p. 46 ; Pour plus d'information sur la question, voy. S. NIKOLTCHEV, « Les données à caractère personnel sont-elles vraiment privées ? », *Observatoire européen de l'audiovisuel*, IRIS *plus*, Strasbourg, 2013.

des données historiques. Les réactions semblent cependant unanimes : une telle mesure affaiblirait la protection de millions d'individus sur le net[212] et réduirait à néant les bienfaits résultant d'une 'protection dès la conception'[213] en exigeant du système qu'il soit intentionnellement conçu faillible. Seul un dialogue transfrontalier et l'adoption d'une stratégie commune semblent donc susceptibles de dénouer ce nœud gordien.

Section 2 – La portabilité des données

110. Consacré par l'article 20 du règlement, ce nouveau droit confirme le mouvement entamé vers une reprise du contrôle des données par la personne concernée. Cette dernière dispose désormais du droit, en cas de traitement automatisé, de « *recevoir les données à caractère personnel* [la] *concernant, qu'*[elle] *a fourni à un responsable du traitement*[214]*, dans un format structuré, couramment utilisé, lisible par machine et interopérable*[215]*, et de les transmettre à un autre responsable du traitement* »[216]. Pour ce faire, le traitement doit reposer soit sur le consentement préalable de la personne concernée soit sur l'exécution d'un contrat auquel elle est partie[217]. Ce droit ne porte en outre pas atteinte aux droits et libertés de tiers[218].

111. Notons que le champ d'application de ce principe est particulièrement large. Il vise tant les relations purement commerciales que les relations de travail ou encore celles avec un prestataire financier[219]. En permettant à la personne concernée de récupérer et de réutiliser ses

[212] M. MURGIA, « WhatsApp sends clear message over demands for decryption », *FT*, 28 mars 2017, p. 15.
[213] K. BRAHMBHATT, *op. cit.*
[214] Ce droit ne concerne que les données que la personne concernée a *elle-même fournies* au responsable de traitement. Sont ainsi visées tant les données délibérément et activement fournies (âge, adresse postale etc.) que celles ayant été générées et collectées à partir de ses activités, de par l'utilisation d'un dispositif ou d'un service (données de localisation, historique de recherche etc.). Voy. O. GUERGUINOV et T. LÉONARD, « GDPR. Droit à la portabilité des données : analyse des lignes directrices du G29 », 28 décembre 2016, https://www.droit-technologie.org/actualites/gdpr-droit-a-portabilite-donnees-analyse-lignes-directrices-g29/ (consulté le 18 juillet 2017).
[215] Le choix des moyens techniques à mettre en œuvre afin d'assurer la réalisation de ce droit devra nécessairement résulter d'un accord, à tout le moins tacite, entre les responsables de traitement. Pour des suggestions quant à la mise en œuvre du droit à la portabilité des données : G29, "Guidelines on the right to data portability", *WP242*, adoptées le 13 décembre 2016 et révisées le 5 avril 2017.
[216] Considérant 68 et art. 20, §1, du règlement.
[217] Art. 20, §1, a) et b), du règlement.
[218] Art. 20, §4, du règlement. Par exemple, la personne concernée pourrait demander qu'un répertoire de contacts crée dans le cadre de l'utilisation d'un service de messagerie soit transmis à un autre responsable. L'utilisation par ce dernier dudit répertoire à des fins de marketing serait susceptible de porter préjudice aux droits des tiers inclus dans le répertoire, en l'absence d'une relation contractuelle ou d'un consentement préalable.
[219] O. GUERGUINOV et T. LÉONARD, *op. cit.*

données, cette disposition facilite la libre circulation de ces dernières et renforce la concurrence entre les différents prestataires de services[220].

112. Bien que l'utilité d'octroyer un 'droit à la portabilité des données' soit claire, la meilleure façon de le faire a suscité des doutes. Ainsi, au lieu d'être attribué par le biais du règlement, celui-ci aurait pu trouver son fondement dans le droit [européen] de la concurrence, comme c'est le cas aux Etats-Unis. Certains[221] ont ainsi vu dans l'étude de cette alternative l'occasion d'une remise en question. Nous esquisserons brièvement lesdites réflexions et les enseignements corrélatifs retirés d'une telle comparaison.

113. Premièrement, c'est la pertinence d'une application du droit européen de la concurrence aux violations du' droit à la portabilité des données' qui a été soupesée ; ces dernières pouvant créer un effet anticoncurrentiel tel que le 'verrouillage'[222] de la personne concernée. En effet, les données collectées via les services en ligne sont précieuses sous deux aspects. D'une part, elles représentent un avantage concurrentiel majeur, permettant d'offrir aux clients des réponses mieux adaptées et des services de meilleure qualité. D'autre part, elles détiennent une valeur monétaire intrinsèque via le développement d'une publicité ciblée[223]. Généralement, cette collecte massive de données permet aux premiers fournisseurs d'un service de créer des barrières à l'entrée pour les nouveaux arrivants. Bien que présent en toile de fond, le droit européen de la concurrence a pourtant été jugé inadapté pour régler de telles situations. Les conditions posées par l'article 102 du TFUE - réglementant les abus de position dominante - semblent difficilement applicables aux services en ligne, réduisant ses chances d'application dans le présent contexte[224].

114. Deuxièmement, c'est le 'droit à la portabilité des données' tel que consacré par le règlement qui a fait l'objet d'une évaluation. Mise à part les incertitudes relatives à sa mise en œuvre, ce droit est accueilli au titre d'un premier pas prometteur dont le large champ d'application satisfait. Ainsi, ce droit ne s'appliquera pas seulement aux entreprises jouissant d'une position dominante – comme le requiert le droit de la concurrence – mais à l'ensemble

[220] O. GUERGUINOV et T. LÉONARD, *ibidem.*
[221] B. VAN DER AUWERMEULEN, « How to attribute the right to data portability in Europe: A comparative analysis of legislations", *Computer Law & Security Review: The International Journal of Technology Law and Practice,* n° 33, 2017, pp. 57-72.
[222] Ce concept vise le comportement des fournisseurs de service qui ont tendance à conserver les données collectées et à entraver la réutilisation par le consommateur des données qu'il a lui-même fournies. Dans ce sens, les entreprises rendent plus lourd et couteux le changement vers un nouveau fournisseur de service ; G29, "Annex II to the Guidelines on the Right to Data Portability - Frequently asked Questions", *WP242,* 13 décembre 2016.
[223] B. VAN DER AUWERMEULEN, *op. cit*., p. 58.
[224] B. VAN DER AUWERMEULEN, *ibidem*, p. 72.

des responsables de traitement ou sous-traitants, indépendamment de leur établissement dans l'Union. Le règlement est donc considéré comme étant la meilleure chance pour un 'droit à la portabilité des données' d'être efficacement attribué en Europe[225].

115. Dans le contexte des transferts transatlantiques de données à caractère personnel, l'accord devra donc à nouveau être amendé afin de satisfaire aux exigences européennes. C'est indispensable au regard de la *ratio* du présent principe dont la logique requiert impérativement de couvrir des organisations américaines telles que Google, Apple, Facebook et Amazone, traitant une quantité sans égal de données à caractère personnel. Quoi qu'il en soit, le champ d'application étendu du règlement participera également à en assurer une large couverture, au-delà des frontières de l'Union.

[225] B. VAN DER AUWERMEULEN, *ibidem.*

Titre III – Les voies de recours et les mécanismes de surveillance

116. Pendant longtemps, l'étude de la protection des données à caractère personnel est restée cantonnée aux dimensions légales et technologiques ; peu d'attention a été accordée aux voies de recours et à la compréhension du travail des organes de réglementation, dont les autorités de contrôle sont les plus proéminentes. Or, comme le suggère l'adage '*Privacy law on the ground rather than on the books*', toute loi doit être assortie d'un mécanisme de mise en œuvre qui permet au droit d'assurer son respect et son développement[226].

117. Dans le contexte transatlantique, l'affaire PRISM, suivie d'autres polémiques[227] tant sécuritaires que commerciales ont, à cet égard, permis de mettre en lumière le caractère parfois illusoire de la protection offerte aux citoyens, faisant jaillir un besoin de garanties renforcées et de voies de recours simplifiées[228]. Après avoir dépeint les mécanismes contenus dans l'accord (Chapitre 1), nous examinerons en détails le fonctionnement des autorités de contrôle (Chapitre 2) dont l'importance a été réitérée tant dans le règlement qu'à l'occasion de l'arrêt *Schrems*.

Chapitre 1 – Panorama des mécanismes contenus dans l'accord Bouclier Vie Privée

118. En vertu du principe '*voies de recours, application et responsabilité*' et pour protéger efficacement la vie privée, il convient de mettre en place des « *mécanismes robustes permettant d'assurer le respect des principes, de ménager un droit de recours aux personnes concernées par le non-respect des principes et de sanctionner les organisations qui n'ont pas appliqué les principes alors qu'elles s'y sont engagées* »[229]. Au minimum, ces mécanismes doivent inclure des voies de recours individuelles (Section 1), un système de supervision (Section 2) et des conséquences en cas de non-respect des principes contenus dans l'accord (Section 3)[230]. L'étude

[226] C. RAAB et I. SZEKELY, « Data protection authorities and information technology », *Computer Law & Security Review: The International Journal of Technology Law and Practice*, n° 33, 2017, p. 2.
[227] Notons par exemple les révélations du 4 octobre 2015 relatives à l'existence d'un logiciel interne au service de messagerie Yahoo – conçu à la demande d'un service de renseignement américain non-identifié – afin de surveiller automatiquement l'apparition de certains mots-clefs dans les courriels de ses utilisateurs.
[228] C.J.U.E., C-293/12 et C-594/12 *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e.a.*, 8 avril 2014, ECLI:EU:C:2014, pts. 35, 45, 62 et 66.
[229] Considérant 26 et Annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[230] Pt. II. 7, de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

de ces trois composantes permettra de jauger la faisabilité du système mis en place et d'en tirer les enseignements nécessaires, applicables à la généralité des transferts internationaux de données à venir.

Section 1 – La pléiade des voies de recours individuelles

119. Une première exigence concerne la mise en place de systèmes de recours indépendants et facilement accessibles[231], « *permettant d'étudier et de résoudre rapidement et sans aucun frais toute plainte et tout litige en se référant aux principes et d'accorder des dédommagements lorsque la loi applicable ou les initiatives du secteur privé le prévoient* »[232]. C'est dans cette optique que l'accord prévoit un système de recours en cascade[233].

120. Premièrement, les consommateurs peuvent introduire une plainte auprès de l'entreprise auto-certifiée[234], qui devra répondre dans un délai de 45 jours suivant le dépôt de celle-ci[235]. Comme déjà établi dans l'accord *Safe Harbor*, les entreprises doivent adhérer à un mécanisme de recours indépendant afin de régler les litiges demeurés non-résolus[236]. Pour ce faire, les entreprises disposent d'un choix : recourir au règlement extrajudiciaire des litiges, ou se soumettre au contrôle d'une autorité chargée de la protection des données[237]. Notons que la plupart des entreprises choisissent la première alternative, utilisant des organismes américains[238] dont la sympathie envers le monde de l'industrie ne laisse que peu de doutes. En cas de choix pour la seconde alternative, l'autorité dispose de 60 jours à partir du dépôt de la plainte pour conseiller l'entreprise, qui aura 25 jours pour se mettre en conformité. A défaut,

---

[231] 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. 1.
[232] Pt. II. 7, a), i), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[233] Commission européenne, *Guide to the EU-U.S. Privacy Shield*, Belgique, 2016, pp. 15-16.
[234] Considérant 38, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[235] Pt. III. 11, d) et i), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[236] Considérant 40, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016: Ces mécanismes de recours indépendants peuvent se trouver, soit dans l'Union, soit aux Etats-Unis.
[237] La surveillance par une autorité de contrôle est obligatoire dans l'hypothèse où l'entreprise traite des données personnelles relatives aux ressources humaines. Ceci implique qu'en qualité d'employé, une personne concernée de l'Union pourra toujours se rendre auprès de son autorité locale afin d'introduire une plainte concernant le transfert de ces dites données à une entreprise certifiée.
[238] Par exemple, Better Business Bureau ou TRUSTe (utilisé par Facebook notamment).

l'autorité peut transférer la plainte à la commission du commerce américain ; celle-ci sera cependant libre de n'enquêter que sur les cas individuels pertinents pour le bon fonctionnement d'un marché concurrentiel.

121. Si la situation de non-conformité perdure, le ministère du commerce américain pourra prononcer le retrait de l'entreprise de la 'liste Bouclier vie privée'. Soulignons qu'à la différence des autorités de contrôle, ledit ministère n'est pas un organisme indépendant – comme requis par le droit européen – mais une branche du gouvernement des Etats-Unis d'Amérique. Majoritairement américaine, cette supervision trouve toutefois son contrepoids dans le pouvoir des autorités de contrôle de suspendre à tout moment les transferts de données vers l'entreprise concernée. Ce pouvoir a été réitéré dans l'arrêt *Schrems*[239] et consacré tant dans l'accord[240] que dans le nouveau Règlement[241].

122. Deuxièmement, les personnes concernées de l'Union pourront introduire une plainte directement auprès de leur autorité de protection des données qui, le cas échéant, transmettra celle-ci au ministère du commerce américain. Celui-ci s'est engagé à tout mettre en œuvre pour faciliter le règlement de la plainte avec l'organisation certifiée[242]. Soumises à un ordre de priorité[243] dont la teneur précise n'a pas été révélée, certaines plaintes pourraient néanmoins rester lettre morte.

123. Troisièmement, les plaintes non-résolues ou réglées de façon non-satisfaisante pourront - à titre résiduaire - être portées devant un panel d'arbitres[244]. Le ministère de commerce américain et la Commission européenne désigneront un groupe de 20 arbitres[245], parmi lesquels

---

[239] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 101.

[240] Considérant 142 et art. 3 de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

[241] Art. 58, §2, j), du règlement.

[242] Annexe I, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

[243] Pt. II. 7, e), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016 ; Cet ordre de priorité sera déterminé au regard des « *principes déférés par le ministère et par les autorités des Etats membres de l'Union européenne* ».

[244] Annexe I, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

[245] Annexe I, pt. F, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

les parties feront un choix[246]. Les pouvoirs de ce panel se limitent cependant à déterminer si l'entreprise mise en cause a violé ses obligations, sans pouvoir s'immiscer dans les dérogations prévues par l'accord ou entreprendre une analyse de conformité générale dudit accord. Seule une mesure de réparation 'équitable non-pécuniaire propre à chaque personne'[247], pourra découler de cette procédure d'arbitrage. Basé aux Etats-Unis, ce mécanisme arbitral sera soumis au contrôle des juridictions américaines.

124. Bien qu'extensif, ce système en cascade - ou '*patchwork*'[248] - a suscité de nombreux scepticismes, tant chez les commentateurs que dans le chef du G29 et du contrôleur européen. De façon générale, le G29 déplore la complexité et le manque de clarté du système mis en place, compromettant l'exercice effectif des droits des personnes concernées. Qualifiées de longues, opaques, formalistes et inintelligibles pour l'individu moyen[249], ces procédures quasi-judiciaires contrarieraient l'objectif même de leur existence, c'est-à-dire fournir une alternative plus rapide, moins formaliste et plus abordable[250]. Diverses critiques plus pragmatiques sont ensuite formulées.

125. Tout d'abord, l'accord n'assure pas que les institutions compétentes soient habilitées à examiner dans les faits les pratiques en vigueur au sein des entreprises. A titre illustratif, l'absence du pouvoir d'inspecter les serveurs et logiciels rendra ainsi les consommateurs incapables de prouver leurs allégations[251].

126. Ensuite, aucune des options prévues par l'accord n'est directement applicable dans le chef du consommateur. Les décisions du Panel d'arbitres, par exemple, ne pourront être exécutées qu'après un passage devant un Tribunal américain.

127. Enfin, comme déjà mentionné, les procédures seront tenues sur le sol américain, devant des avocats américains, en vertu du droit américain et en anglais[252]. Convergeant majoritairement vers les Etats-Unis, ces mécanismes mettent en péril d'une part, la capacité des

[246] Les parties peuvent choisir entre un et trois arbitres.
[247] Annexe I, pt. B, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[248] J.-P. ALBRECHT, "Privacy Shield – Press Breakfast by MEP Jan Albrecht", Parlement européen, Bruxelles, 12 juillet 2016, p. 2, http://europe-v-facebook.org/PA_PS.pdf
[249] C. KUNER, «Paper n°14/2016 …", *op. cit.,* p. 4.
[250] Agence des droits fondamentaux de l'Union européenne, *Handbook on European law relating to access to justice,* 2016, p. 49.
[251] J.-P. ALBRECHT, "Privacy Shield…", *op. cit.,* p. 2.
[252] J.-P. ALBRECHT, "Privacy Shield…", *ibidem.*

consommateurs à exercer leurs droits[253] ; d'autre part, la capacité des autorités de contrôle de l'Union à surveiller les procédures en cours. Le G29 avait sur ce point déjà attiré l'attention de la vice-Présidente de la Commission dans le contexte de feu *Safe Harbor*. En effet, le droit de porter plainte devant une juridiction nationale *européenne* et la possibilité d'introduire une demande d'indemnisation *dans l'Union* sont, selon le G29, des exigences essentielles pour une protection efficace des données personnelles[254]. Cela dépendra donc de la volonté des organisations certifiées d'offrir de telles possibilités dans leurs politiques de confidentialité.

Section 2 – Le système de supervision : une coquille vide ?

128. Outre des voies recours individuelles, des procédures de suivis doivent être adoptées permettant de vérifier que « *les renseignements et les indications fournies par les organisations sur leurs pratiques en matière de protection de la vie privée sont exactes et que ces pratiques sont mises en œuvre conformément aux déclarations des organisations et, en particulier, en ce qui concerne les cas de non-conformité* »[255]. Nous analyserons dans un premier temps le système d'auto-certification sur lequel repose l'accord pour ensuite appréhender le système de supervision mis en place.

129. L'accord repose sur un système d'auto-certification[256] - qui n'a pas comme tel été jugé contraire au droit de l'Union[257] - en vertu duquel les organisations américaines s'engagent à

[253] G29, "Opinion n° 01/2016 …", *op cit.*, p. 28 : le G29 va jusqu'à proposer deux pistes pour pallier ce risque. D'une part, le système pourrait investir l'autorité de contrôle du pouvoir de représenter la personne concernée, d'agir en son nom ou de servir d'intermédiaire. D'autre part, des clauses de compétence spécifiques devraient être prévues par les entreprises afin de permettre à la personne concernée d'exercer ses droits sur le territoire de l'Union.

[254] G29, "Letter from I. FALQUE-PIERROTIN, President of the WP29, to Vice-President Reding", Bruxelles, 10 avril 2014, *Ares(2014)1139376*, pp. 4-5.

[255] Pt. II. 7, a), ii), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

[256] Considérant 14, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016; 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.

[257] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 81.

respecter un certain nombre de principes de protection de la privée, publiés par le ministère américain du commerce et repris dans l'accord[258].

130. Afin d'octroyer cette certification, il incombe au ministère de vérifier si « *la politique de* [l'organisation] *en matière de protection de la vie privée est conforme aux principes* »[259]. Un contrôle substantiel préalable est donc requis, permettant d'opérer un premier contrôle de conformité dès l'entrée[260]. Les choses deviennent cependant plus confuses à la lecture des engagements dudit ministère[261], ne reprenant que des actions à caractère presque administratif[262]. Prétendument plus détaillée, cette lettre sème le trouble sur l'étendue du contrôle préalable devant être opéré par celui-ci. Déjà mise en lumière par le G29[263], cette ambiguïté n'a pas été corrigée dans la version finale de l'accord.

131. Cette ambivalence souligne qu'il est indispensable de s'assurer qu'un véritable contrôle de fond est opéré, afin d'éviter la présence d'organisations dont la politique en matière de protection des données ne présente pas les standards requis. En l'absence d'un contrôle d'admissibilité stricte, ce manquement pourrait causer un préjudice grave et irréparable aux droits de la personne concernée[264].

132. Une supervision étroite des organisations doit ensuite être maintenue après la certification. Comme le rappelle la Cour de l'Union, la fiabilité d'un système d'auto-certification repose essentiellement sur la mise en place de « *mécanismes efficaces de détection et de contrôle permettant d'identifier et de sanctionner, en pratique, d'éventuelles violations des règles assurant* […] *la protection des données à caractère personnel* »[265]. L'absence d'un

---

[258] Annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

[259] Considérant 32, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

[260] Notons qu'il s'agit d'une amélioration par rapport à l'accord *Safe Harbour*, pour lequel aucune vérification préalable ni preuve du respect des principes n'était imposées ; G29, « Avis n°4/2000 sur le niveau de protection assuré par 'les principes de la sphère de sécurité' », *WP32*, 16 mai 2000, p. 3 ; 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.

[261] Annexe I, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

[262] Par exemple, la vérification des coordonnées de l'organisation, la mention d'une déclaration d'adhésion aux principes ou la mention des mécanismes de recours disponibles.

[263] G29, "Opinion n°01/2016 …", *op. cit.*, p. 28.

[264] G29, "Opinion n°01/2016 …", *ibidem.*

[265] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 81.

tel contrôle par une autorité américaine figure au rang des motifs ayant justifié l'annulation de l'accord *Safe Harbor*[266]. Cette lacune préoccupait les entreprises européennes, y voyant un avantage concurrentiel majeur offert à leurs homologues américains[267]. C'est par le truchement de deux mesures que l'accord tente ainsi de répondre aux exigences nouvellement posées par la Cour, sans grande conviction.

133. Premièrement, l'accent a été mis sur une plus grande transparence au profit de la personne concernée. Outre les organisations auto-certifiées, la liste[268] communiquée par le département du commerce américain comprend également le nom des organisations qui en ont été retirées et les raisons de ce retrait[269]. Cela permettra au consommateur soucieux de la protection de ses données d'être mieux informé lorsqu'il choisira son fournisseur de service.

134. Deuxièmement, il semble que la commission du commerce américain et le ministère du commerce américain soient investis de certains pouvoirs d'investigation en cas de plainte ; le ministère pouvant notamment agir par le biais de l'envoi de questionnaires. Le G29 s'inquiète cependant de savoir si une telle approche suffit à répondre aux exigences d'efficacité posées par la Cour. Ainsi, le pouvoir des autorités américaines de mener des investigations *in-situ* dans les locaux de l'organisation n'est pas clair[270] ; l'*exequatur* des décisions des autorités européennes sur le territoire des Etats-Unis n'est pas davantage garantie[271].

Section 3 – Les conséquences en cas de non-respect des principes : entre intimidation et dissuasion

135. Enfin, les organisations qui ont souscrit aux principes doivent être tenues de « *résoudre les problèmes qui découlent du non-respect de ceux-ci et d'assumer les conséquences qui en*

[266] A. CASSART, *op. cit*., p. 1235.
[267] En effet,, une entreprise européenne qui est en concurrence avec une entreprise américaine qui, en pratique, ne respecte pas les principes contenus dans l'accord, se trouve nécessairement dans une position concurrentielle désavantageuse ; 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.
[268] Pour un accès à la liste complète des entreprises auto-certifiées, voy. https://www.privacyshield.gov/list
[269] Annexe I, et pt. II. 1, de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016 ; Cet ajout répond à la recommandation n°4 faite par la Commission européenne dans le cadre de *Safe Harbor* : 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. 22.
[270] CEPD, « Avis n°4/2016 … », *op. cit.*, p. 10.
[271] G29, "Opinion n°01/2016 …", *op. cit.*, p. 30.

résultent » par le biais de « *sanctions suffisamment dissuasives pour garantir le respect des principes par les organisations* »[272]. L'accord prévoit notamment deux conséquences dont le caractère dissuasif a rapidement – et à juste titre - été remis en cause par le G29[273].

136. D'une part, dans le cadre d'un transfert ultérieur, toute organisation demeure responsable du traitement des informations qu'elle collecte au titre de l'accord et qu'elle transfère ensuite à un tiers agissant pour son compte en qualité de mandataire. L'organisation assumera les conséquences d'un traitement ultérieur non-conforme aux principes, sauf si elle apporte la preuve qu'elle n'est pas responsable des évènements ayant causé le préjudice[274].

137. D'autre part, toute organisation qui fait l'objet d'une ordonnance judiciaire ou d'une ordonnance de la commission du commerce américain est tenue de rendre publique la partie relative à l'accord[275]. Ceci participerait à assurer une plus grande transparence au profit des consommateurs ; la crainte d'une réputation salie pourrait également inciter les organisations du pays de l'Oncle Sam à plus de conformité.

Chapitre 2 – Les autorités de contrôle : une évolution du statut de spectateur à celui d'acteur

138. L'importance du rôle joué par les autorités de contrôle - telle que récemment mis en exergue dans le règlement et par la Cour de justice dans l'arrêt *Schrems*[276] - suppose d'en étudier la substance. Avant toute chose, nous reviendrons sur les origines de ces institutions dont l'évolution et le particularisme méritent notre attention (Sections 1). S'en suivra l'examen de l'indépendance, des compétences et des pouvoirs de ces autorités (Section 2).

[272] Pt. II. 7, a), iii), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[273] G29, "Opinion n°01/2016...", *op. cit.,* p. 30.
[274] Pt. II. 7, d), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[275] Pt. II. 7, e), de l'annexe II, de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.
[276] Un autre arrêt relatif aux pouvoirs des autorités de contrôle a été rendu le même mois par la Cour de l'Union : C.J.U.E, C-230/14 *Weltimmo s.r.o. c. Nemzeti Adatvedelmi es Informacioszabadsag Hatosag*, 1er octobre 2015, ECLI:EU:C:2015:639.

Section 1 – L'essor des autorités de contrôle comme garant d'un droit de la protection des données en action

139. Après avoir identifié le fondement légal et la *ratio* des autorités de protection des données (§1), nous mettrons en lumière les enjeux gravitant autour de ces institutions (§2) et le particularisme dont elles font état (§3).

§1 – Le fondement légal et la *ratio* des autorités de contrôle

140. C'est dans la Convention n°108 du Conseil de l'Europe, conclue en 1981, que les autorités de contrôle trouvent leurs origines. Alors que l'article 4 invite les Parties contractantes à prendre, dans leur droit interne, « *les mesures nécessaires pour donner effet aux principes de base pour la protection des données* », l'article 10 poursuit en requérant la mise en place de « *sanctions et recours appropriés* ». C'est la mise en lumière de l'exigence de protection effective, tout en laissant aux Etats le soin d'en établir les modalités. L'adoption de la directive 95/46 sur la protection des données personnelles a cependant sonné le glas de cette liberté initialement reconnue.

141. Par souci d'uniformisation et d'efficacité, l'article 28 de la directive requiert désormais, dans chaque Etat membre, l'établissement d'une autorité publique chargée de veiller au respect de la directive, en toute indépendance. Considérées comme étant « *un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel* »[277], ces autorités de contrôle se sont ainsi vu reconnaître divers pouvoirs, tels que le pouvoir d'investigation, d'intervention ou le pouvoir d'ester en justice[278]. Nous verrons que le règlement constitue le prolongement logique de cette dynamique d'uniformisation que la directive n'avait pas su pleinement assurer[279].

142. L'existence de ces autorités de contrôle témoigne de la nature particulière du droit fondamental à la protection des données personnelles. Ce droit est réputé requérir un 'support structurel'[280], par la mise en place d'une autorité indépendante, dotée de pouvoirs et de

[277] Considérant 62, de la directive.
[278] Art. 28, §3, de la directive.
[279] S. PEYROU, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la C.J.U.E », *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence*, sous la direction de R. TINIÈRE et C. VIAL, Bruxelles, *Bruylant*, 1ère éd., avril 2015, p. 222.
[280] P. HUSTINX, « Introduction. The role of data protection authorities », *Défis du droit à la protection de la vie privée*, sous la coordination de PÉREZ ASINARI (M.-V.) et PALAZZI (P.), Bruylant, 2008, p. 564.

ressources appropriés. Nul autre droit fondamental, excepté le droit à un procès équitable, ne dépend ainsi structurellement du rôle accordé à une autorité indépendante afin d'en assurer son respect et son évolution[281].

143. Malgré l'importance de ces autorités de contrôle et les efforts croissants d'uniformisation de leurs pratiques au sein de l'Union, l'Agence des droits fondamentaux de l'Union européenne avait sonné l'alarme en 2013[282]. Soulignant un manque de pouvoirs et de ressources appropriés, l'Agence en appelait à davantage de coordination et d'homogénéité. L'appel semble avoir désormais été entendu par les négociateurs du nouveau règlement.

§ 2 – Les autorités de contrôle au centre de l'arrêt *Schrems*

144. Le renvoi préjudiciel formé par la Haute Cour de justice d'Irlande invitait la Cour de l'Union à préciser l'étendue des pouvoirs des autorités de contrôle face à des dysfonctionnements dans l'application de la décision 2000/520[283]. Ainsi, « *eu égard aux articles 7, 8 et 47 de la Charte et sans préjudice des dispositions de l'article 25, paragraphe 6, de la directive 95/46, le Commissaire indépendant chargé d'appliquer la législation sur la protection des données saisi d'une plainte relative au transfert de données à caractère personnel vers un pays tiers (en l'occurrence les Etats-Unis) dont le plaignant soutient que le droit et les pratiques n'offriraient pas des protections adéquates à la personne concernée, est-il absolument lié par la constatation contraire de l'Union contenue dans la décision 2000/520 ? Dans le cas contraire, peut-il ou doit-il mener sa propre enquête en s'instruisant de la manière dont les faits ont évolué depuis la première publication de la décision de la Commission ?* »[284].

145. Selon Maximilian SCHREMS, l'appréciation de la Commission quant au caractère adéquat du niveau de protection existant dans un pays tiers n'empêchait pas l'autorité nationale d'enquêter sur une plainte visant à remettre en cause ce constat. La Commission n'était pas de cet avis, estimant que la compétence des autorités de contrôle se limitait aux cas individuels, tandis que le réexamen général d'une décision d'adéquation relevait de sa compétence[285]. Le 6

[281] P. HUSTINX, *ibidem*.
[282] Agence des droits fondamentaux de l'Union européenne, *Report on the access to data protection remedies in EU Member States*, 2013, p. 9.
[283] Av. gén. Y. BOT, *op. cit.*, pt. 5.
[284] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 36.
[285] Av. gén. Y. BOT, *op. cit.*, pt. 59.

octobre 2015, la Cour de justice de l'Union a tranché en faveur de M. SCHREMS[286], précisant toutefois que lesdites autorités ne disposent pas de la compétence de constater elles-mêmes l'invalidité d'un tel acte. C'est sans surprise que la Cour s'en réserve la compétence exclusive[287].

146. Comme souligné par l'Avocat Général Yves BOT, les autorités de contrôle doivent pouvoir se forger leur propre opinion quant au niveau général de protection existant dans un pays tiers[288] et ce, afin de préserver un juste équilibre entre d'une part, le respect du droit fondamental à la vie privée et d'autre part, les intérêts (commerciaux) qui commandent une libre circulation des données à caractère personnel[289].

147. Bien que jouant un rôle essentiel d'uniformisation des conditions de transfert applicables au sein de l'Union, une décision d'adéquation adoptée par la Commission ne saurait restreindre les attributions des autorités de contrôle lorsqu'elles sont confrontées à des allégations de violations de droits fondamentaux[290]. Ce, d'autant plus qu'il est constant, à la lecture de l'article 25, paragraphe 2, de la directive 95/46, que le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de diverses circonstances, tant factuelles que juridiques. Ainsi, « *si l'une de ces circonstances évolue et apparaît comme étant de nature à remettre en cause le caractère adéquat du niveau de protection offert par un pays tiers, l'autorité nationale de contrôle saisie d'une plainte doit pouvoir en tirer les conséquences par rapport au transfert contesté* »[291].

148. C'est avec 'toute la diligence requise'[292] qu'il incombe alors à l'autorité d'examiner la demande telle que formulée, afin de conclure au bien-fondé ou au rejet de celle-ci. Dans la première hypothèse, l'autorité se voit reconnaître le pouvoir d'ester en justice, afin d'amener les juridictions nationales, le cas échéant, à procéder à un renvoi préjudiciel près la Cour de

[286] La Cour de justice a tranché conformément aux conclusions de l'Av. gén. Y. BOT.
[287] Dans ce sens : C.J.C.E., C-314/85 *Foto-Frost c. Hauptzollamt Lübeck-Ost*, 22 octobre 1987, pts. 15-20, ECLI:EU:C:1987:452 ; C.J.C.E., C-344/04 *International Air Transport Association et European Low Fares Airline Association c. Department for transport*, 10 janvier 2006, ECLI:EU:C:2006/10, pt. 27.
[288] Av. gén. Y. BOT, *op. cit.*, pt. 61.
[289] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 42.
[290] Av. gén. Y. BOT, *ibidem*, pt. 93.
[291] Av. gén. Y. BOT, *op. cit.*, pt. 82.
[292] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 63.

justice aux fins de l'examen de la validité de la décision attaquée[293]. Dans la seconde hypothèse, la personne ayant introduit ladite demande doit avoir accès aux voies de recours juridictionnelles afin de contester la décision lui faisant grief devant les juridictions nationales. Celles-ci sont ensuite tenues de surseoir à statuer et de saisir la Cour de justice d'une procédure de renvoi préjudiciel si elles considèrent que les moyens d'invalidité invoqués sont fondés[294]. C'est donc une approche prudente[295] qui a été choisie par la Cour, confirmant sa nécessaire saisine pour obtenir l'invalidation d'une décision d'adéquation.

149. Ce pouvoir reconnu aux autorités de contrôle est un atout pour la surveillance continue du respect du droit européen de la protection des données. Cependant, le risque d'opinions divergentes sur le niveau de protection assuré par un pays tiers soulève des inquiétudes quant à une trop grande fragmentation du paysage européen[296].

150. Cette appréhension peut toutefois être relativisée à trois égards. Premièrement, la Cour de l'Union reste l'ultime arbitre de ce qui constitue un niveau 'adéquat de protection'. Deuxièmement, les obligations de cohérence et de coordination[297] auxquelles sont soumises les autorités de contrôle impliquent de tendre vers une prise de décision commune à l'égard desdits transferts. Troisièmement, le 'guichet unique' suppose que l'autorité de contrôle compétente soit celle du pays dans lequel l'entreprise a son établissement principal[298]. C'est alors cette autorité-là qui se chargera d'examiner les plaintes et d'évaluer l'opportunité d'une suspension du flux des données en cause, en collaboration avec les autres autorités de contrôle concernées.

§3 – Le particularisme des autorités de contrôle

151. Plus qu'une bataille de pouvoir entre la Commission et les autorités de contrôle, cette question préjudicielle souligne l'importance du rôle accordé aux autorités de contrôle.

[293] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 63 ; Art. 28, §3, al. 1, 3ème tiret, de la directive 95/46, lu à la lumière de l'art. 8, § 3, de la Charte des droits fondamentaux de l'Union européenne.
[294] C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650, pt. 64 ; Art. 28, §3, al. 2, de la directive, lu en combinaison avec l'art. 47 de la Charte.
[295] A. CASSART, *op. cit*., p. 1234.
[296] C. Kuner, "Paper n°14/2016… », *op. cit.*, p. 12.
[297] Chapitre 7, du règlement. Ces obligations se manifestent dans le cadre des travaux du comité européen de la protection des données (ancien Groupe de travail Article 29) et ce, notamment dans le but de déterminer des positions communes quant-aux niveau adéquat de protection des données dans un pays tiers.
[298] Art. 56, §1, du règlement.

Qualifiées de 'gardiennes des droits et libertés fondamentaux'[299], ces autorités de contrôle témoignent de l'émergence de nouveaux acteurs dans le domaine de la protection des droits fondamentaux de l'Union européenne.

152. Non juridictionnelles, ces instances indépendantes fonctionnent sur la base d'une logique nouvelle. Alors que le mode de protection 'traditionnel' des droits fondamentaux se fonde sur l'existence de quatre éléments cumulatifs, le 'nouveau' mode se caractérise par l'absence d'au moins un de ces éléments. Ainsi, les mesures protectrices contraignantes peuvent n'être plus que dissuasives, persuasives ou informatives. Celles-ci n'interviennent plus nécessairement *a posteriori* mais parfois de manière préventive. Originellement initiées à la demande de la personne concernée, ces mesures peuvent désormais être prises d'office par les autorités de contrôle. Et enfin, dépassant les cas individuels, les mesures de protection des droits fondamentaux peuvent revêtir une dimension collective, visant à protéger une pluralité de citoyens à l'égard d'un ou plusieurs actes d'ingérence[300].

153. La mutation du mode de protection des droits fondamentaux, et plus particulièrement du droit à la protection des données, répond aux enjeux suscités par la nature même des ingérences. Le plus souvent imperceptibles et survenant à grande échelle, les actes de traitement des données personnelles ont fait naître le besoin d'une protection dynamique et proactive du droit fondamental à la protection des données[301].

154. Le 6 octobre 2015, les autorités de contrôle se sont ainsi vu reconnaître le pouvoir d'enquêter sur les réclamations qui leur sont soumises, en toute indépendance, « *dans l'intérêt supérieur de la protection des individus à l'égard du traitement des données à caractère personnel* »[302]. A l'heure où certains se demandent si l'Union européenne n'est pas avant tout un acteur économique cherchant une 'légitimité purement formelle' par l'entremise de la 'promotion externe des droits de l'Homme'[303], il semble heureux de voir les autorités de

[299] Voy. en ce sens, C.J.U.E., C-614/10 *Commission européenne c. République d'Autriche*, 16 octobre 2012, ECLI:EU:C:2012:631, pt. 52 et C.J.U.E., C-288/12 *Commission européenne c. Hongrie*, 8 avril 2014, ECLI:EU:C:2014:237, pt. 53.
[300] H. KRAEMER, « Les nouveaux acteurs dans le domaine des droits fondamentaux de l'Union européenne », *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence.* Sous la dir. de R. TINIÈRE et C. VIAL, Bruxelles, *Bruylant*, 1ère éd., avril 2015, pp. 321-322.
[301] H. KRAEMER, *ibidem*, p. 334.
[302] Av. gén. Y. BOT, *op. cit.*, pt. 73.
[303] C. MAUBERNARD, « Prendre la promotion externe des droits de l'Homme par l'Union européenne 'au sérieux' », *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence*, Sous la dir. de R. TINIÈRE et C. VIAL, Bruxelles, Bruylant, 1ère éd., avril 2015, p. 295.

contrôle indépendantes érigées - aux côtés de la Commission - au rang de garant du droit à la protection des données.

155. L'efficacité de ce contrôle par les autorités de contrôle dépendra cependant de deux éléments majeurs. D'une part, de la volonté de ces autorités à adopter des positions communes afin d'éviter une fragmentation dans l'application du droit européen de la protection des données. D'autre part, des pouvoirs et des ressources dont disposent lesdites autorités, ce que nous analyserons dans la section suivante.

Section 2 – Portrait des autorités de contrôle : statut et prérogatives

156. Afin de comprendre l'amplitude du rôle reconnu par la Cour de justice aux autorités de contrôle, il convient de s'attarder sur la dynamique rythmant leur fonctionnement. C'est par le biais d'une approche évolutive que nous analyserons les exigences imposées à ces dites autorités, en nous glissant dans les méandres de la jurisprudence européenne et du nouveau règlement général sur la protection des données. Dans un premier temps, nous examinerons les exigences d'indépendance auxquelles ces autorités sont soumises (§1) pour ensuite aborder l'étendue de leur compétence et de leurs pouvoirs (§2).

§1 – Le statut d'indépendance des autorités de contrôle

157. A l'heure actuelle fondé sur l'article 28, paragraphe 1, de la directive 95/46, le statut d'indépendance des autorités de contrôle vise à assurer la fiabilité et l'efficacité du contrôle du respect des règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ; la protection des individus concernés par les décisions des autorités de contrôle est également renforcée[304].

158. Afin de répondre aux impératifs d'objectivité et d'impartialité, lesdites autorités doivent être à l'abri de toute influence extérieure, directe ou indirecte, tant de l'Etat que d'entités infra-

[304] CJUE, C-518/07 *Commission européenne c. République fédérale d'Allemagne*, 9 mars 2010, ECLI:EU:C:2010:125, pt. 25. Dans cette affaire, la Cour a estimé que la République fédérale d'Allemagne avait agi en violation de l'article 28, §1, de la directive 95/46, en soumettant les autorités chargées du contrôle du traitement de données par le secteur non-public dans les différents Länder à une tutelle de l'Etat.

étatiques ou d'organismes contrôlés[305]. Cette garantie d'indépendance peut s'analyser à l'aune d'une double dimension.

159. Sous l'angle institutionnel, celle-ci vient faire obstacle à toute forme de tutelle étatique, qui permettrait à un organe politique de l'Etat d'influer, voire d'annuler ou de substituer les décisions prises par l'autorité de contrôle[306]. L'obligation pour les Etats de conférer le statut d'indépendance à ces autorités n'implique cependant pas la disparition de toute légitimité démocratique. D'une part, la nomination des 'personnes assumant la direction des autorités de contrôle' peut se faire par le Parlement ou par le Gouvernement. D'autre part, le législateur est libre de définir les compétences desdites autorités et de les obliger à rendre compte de leurs activités au Parlement[307].

160. Sous l'angle personnel, la garantie d'indépendance recouvre le respect des dispositions nationales relatives à la durée du mandat. Ainsi, si un Etat membre disposait du pouvoir de mettre anticipativement fin au mandat d'une autorité de contrôle, en violation des règles et garanties nationales préexistantes, *« la menace d'une telle cessation anticipée qui planerait sur l'autorité tout au long de l'exercice de son mandat pourrait conduire à une forme d'obéissance de celle-ci au pouvoir politique* »[308], incompatible avec l'exigence d'indépendance.

161. Sur cet impératif d'indépendance, le règlement[309] n'apporte que quelques clarifications. Après avoir précisé que les membres de l'autorité devaient agir libres de toute influence extérieure[310], la disposition poursuit en interdisant aux dits membres de poser des actes incompatibles avec leurs fonctions, pendant la durée de leur mandat[311].

162. Plus important encore, les Etats membres se voient désormais imposer de fournir aux autorités de contrôle les 'ressources humaines, techniques et financières ainsi que des locaux et

---

[305] CJUE, C-518/07 *Commission européenne c. République fédérale d'Allemagne*, 9 mars 2010, ECLI:EU:C:2010:125, pt. 25.
[306] CJUE, C-518/07 *Commission européenne c. République fédérale d'Allemagne*, 9 mars 2010, ECLI:EU:C:2010:125, pt. 31.
[307] CJUE, C-518/07 *Commission européenne c. République fédérale d'Allemagne*, 9 mars 2010, ECLI:EU:C:2010:125, pts. 44-45.
[308] C.J.U.E., C-614/10 *Commission européenne c. République d'Autriche*, 16 octobre 2012, ECLI:EU:C:2012:631, pt. 51 ; C.J.U.E., C-288/12 *Commission européenne c. Hongrie*, 8 avril 2014, ECLI:EU:C:2014:237, pt. 54.
[309] L'art. 52, du règlement s'inspire tant de l'arrêt de la Cour de justice du 9 mars 2010 que du Règlement (CE) 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *J.O.C.E.*, L 8 du 12 janvier 2001 : l'art. 44 prévoit les conditions d'indépendance du contrôleur européen chargé de la protection des données.
[310] Art. 52, §2, du règlement.
[311] Art. 52, §3, du règlement.

l'infrastructure nécessaires' afin d'assurer l'exercice effectif de leurs missions et de leurs pouvoirs[312]. Les négociateurs du règlement avaient été jusqu'à envisager la fixation de quotas de ressources – en fonction de la taille de la population et du nombre de traitements réalisés au sein de chaque Etat - mais les difficultés d'une telle entreprise ont eu raison d'eux[313]. Notons qu'une telle ingérence dans la gestion des budgets nationaux n'aurait probablement pas été appréciée par les vingt-huit Parlements. Sur le plan des principes, l'Etat membre pourrait se voir condamner en manquement par la Commission s'il ne fournissait pas les moyens suffisants[314] ; la détermination de ce seuil minimal serait cependant l'obstacle majeur au succès d'une telle action. Pour finir, l'article 52 du règlement réaffirme la liberté dont disposent les autorités de contrôle quant au choix de leurs agents, et soumis à leur autorité[315].

§2 – La compétence et les pouvoirs des autorités de contrôle

163. Après avoir circonscrit le domaine de compétence des autorités de contrôle (A.), nous évaluerons les pouvoirs dont ces dernières sont investies (B.).

A. Une juridiction circonscrite aux frontières de l'Union

164. En vertu de l'article 28 paragraphes 1 et 3 de la directive[316], l'autorité nationale est compétente, dans les limites des frontières de l'Etat membre dont elle relève, pour exercer les pouvoirs et les missions dont elle est investie.

165. Au grand avantage des entreprises, l'article 56 du règlement vient remédier à la problématique de l'autorité compétente lorsque le responsable du traitement est établi dans plusieurs Etats membres. Initialement tenues de se conformer à toutes les spécificités des législations nationales applicables, ces organisations seront désormais soulagées par l'instauration du 'guichet unique'[317].

[312] Art. 52, §4, du règlement.
[313] Annexe I du présent document, *op. cit.,* p. 75.
[314] Arts. 258, 259 et 260, du TFUE.
[315] Art. 52, §5, du règlement.
[316] Le domaine de compétence de l'autorité de contrôle est confirmé par l'art. 55, §1, du règlement.
[317] Art. 56, du règlement. Dans le contexte d'un traitement transnational, l'autorité dite 'chef de file' est déterminée en fonction de l'établissement principal du responsable ou de son lieu d'établissement unique. Cette autorité sera l'interlocuteur unique du responsable ou du sous-traitant pour le traitement considéré.

166. Favorisant une application cohérente de la législation européenne, ce mécanisme assure désormais une sécurité juridique renforcée et des charges administratives réduites dans le chef du responsable du traitement, ou de son sous-traitant. Cette autorité dite 'chef de file' sera donc seule compétente pour surveiller les activités de traitement transfrontaliers[318] de ces acteurs, et pour agir le cas échéant. La personne concernée par le traitement pourra, quant-à-elle, introduire une plainte devant son autorité nationale, elle-même soumise à une obligation de coordination avec l'autorité chef de file[319]. Ainsi, M. SCHREMS pourra désormais introduire sa plainte auprès de l'autorité autrichienne, qui se chargera d'en informer 'l'autorité chef de file' à Dublin. Gains de temps, d'argent et d'efficacité, cette innovation renforce l'accès des citoyens aux mécanismes de recours.

167. Sans nous appesantir davantage sur ce dispositif, il convient cependant de souligner deux difficultés probables. D'une part, la notion d'établissement principal comme critère d'identification de l'autorité de chef de file[320] semble sibylline, vu la complexité des règles d'identification et la définition proposée[321]. D'autre part, la procédure de coopération prévue entre les différentes autorités de contrôle en cas de plainte suppose un échange d'informations de grande ampleur, dont l'efficacité semble illusoire et la confusion probable dans l'esprit des différents intervenants[322].

B. Des attributions délimitées mais élargies

168. Actuellement, les pouvoirs reconnus aux autorités de contrôle sont doubles. L'un repose sur un pouvoir de conseil et d'avis au profit des autorités législatives et administratives, l'autre consiste en un pouvoir de contrôle, recouvrant les prérogatives d'enquête et d'intervention ainsi que le pouvoir d'ester en justice[323]. Une large marge de manœuvre est cependant accordée aux Etats membres, de sorte que la nature de tels pouvoirs varie largement d'un Etat à l'autre. Ainsi, certains pays, tels que la Suède ou l'Irlande, insistent sur le rôle préventif de l'agence alors que

[318] Pour une définition du 'traitement transfrontalier', voy. art. 4, §23, du règlement.
[319] L'art. 60, du règlement prévoit la procédure régissant les échanges d'information entre les différentes autorités de contrôle concernées par la plainte.
[320] L'art. 56, du règlement énonce les critères d'identification.
[321] Pour un affinement de la notion d'établissement : C.J.U.E, C-230/14 *Weltimmo s.r.o. c. Nemzeti Adatvedelmi es Informacioszabadsag Hatosag*, 1er octobre 2015, ECLI:EU:C:2015:639 et son commentaire : COTON (F.), *op. cit.*, p. 1215-1220.
[322] Voy. GDPR.expert, l'outil d'analyse du nouveau règlement européen, Cabinet Ulys, https://www.gdpr-expert.eu/article.html?id=60#difficultesprobables (consulté le 15 mars 2017).
[323] Art. 28, de la directive.

d'autres privilégient le contrôle *a posteriori* de l'autorité, comme c'est le cas de la Grèce ou de la Lettonie[324]. C'est précisément cette disparité que le règlement tend à estomper.

169. Pour ce faire, l'article 58 du règlement établit désormais un triptyque esquissant de façon détaillée trois types de pouvoirs, dont la lecture suffit à en comprendre la teneur. Outre les pouvoirs de conseil et d'enquête, les autorités de contrôle peuvent prendre des mesures correctrices, parmi lesquelles figure l'imposition d'amendes s'élevant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire annuel. Les entreprises respectueuses du droit de la protection des données jouiront ainsi d'un avantage concurrentiel[325] majeur sur l'échiquier économique mondial, vu l'importance croissante que revêt la question notamment dans l'esprit des consommateurs.

170. Ce nouveau pouvoir de sanction est d'autant plus novateur que la directive[326], elle, ne donnait pour seule indication que son caractère facultatif. A titre illustratif, la Belgique n'a pas fait le choix d'investir la Commission vie privée d'un tel pouvoir. Désormais, outre les hypothèses dans lesquelles ces amendes administratives peuvent être prononcées[327], le règlement prévoit onze facteurs[328] et un système graduel[329] afin d'en déterminer les montants. Celles-ci doivent être à la fois 'effectives, proportionnées et dissuasives'[330]. Nouveau bras armé des autorités de contrôle, ce pouvoir sanctionnateur permettra au droit européen de la protection des données de passer d'illusion à réalité. Le lobbying puissant initié à son encontre, essentiellement par les entreprises privées américaines, ne fait que témoigner de son importance.

171. Accueillie dans son principe, cette nouveauté suscite cependant quelques réticences. Alors que certains systèmes juridiques européens semblent étrangers à une telle pratique,

[324] Agence des droits fondamentaux de l'Union européenne, "Data Protection in The European Union: the role of National Data Protection Authorities", *Strenghtening the fundamental rights architecture in the EU II*, 2010, p. 20, pt. 4.1.3.
[325] Pour une analyse du nouveau règlement à l'aune du droit de la concurrence : 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 ; J.-P. GUÉDON, « Renforcement de la protection des données personnelles », *AJ Pénal*, 2016, p. 53.
[326] Art. 24, de la directive.
[327] Art. 83, §§ 4, 5 et 6, du règlement.
[328] Art. 83, §2, a) à k), du règlement. Les facteurs à prendre en compte sont notamment 'la nature, la gravité et la durée de la violation', le caractère délibéré ou négligent de la violation ou encore le degré de coopération établi avec l'autorité de contrôle.
[329] Art. 83, §§ 4, 5 et 6, du règlement. Le système graduel est établi en fonction de la gravité de l'infraction.
[330] Art. 83, §1, du règlement.

d'autres s'interrogent sur la nature des garanties procédurales à mettre en place[331]. Pour reprendre l'exemple belge, la reconnaissance d'un tel pouvoir à la commission vie privée[332] viendra modifier le rapport de celle-ci aux justiciables, glissant d'un modèle de conciliation vers un modèle de répression[333]. C'est le dépassement de la dimension consultative jadis prépondérante[334]. De plus, l'environnement politique entourant la mise en place d'un tel pouvoir sera déterminant. La méfiance des parlements nationaux à l'égard d'autorités indépendantes - libres de critiquer le pouvoir en place – pourrait jouer en faveur d'une limitation dudit pouvoir[335]. L'amateurisme invoqué de certaines agences pourrait également justifier l'octroi d'un pouvoir sanctionnateur réduit. Le contrôle devient stratégique.

172. A l'instar des autorités de concurrence, les autorités de contrôle fournissent un cadre de '*compliance*', requérant des entreprises une parfaite conformité avec les règles établies. C'est la naissance d'un véritable pouvoir de police[336] en matière de protection des données dont la condition d'existence est l'établissement d'un pouvoir sanctionnateur fort. Cette réforme impliquera néanmoins une recrudescence des moyens, tant humains que financiers, afin d'éviter que celle-ci ne reste lettre morte[337].

173. En d'autres termes, ce renforcement de pouvoir augure du renouveau des autorités de contrôle, dont le sérieux et l'importance institutionnelle seront réaffirmés sinon enfin reconnus.

---

[331] Voy. GDPR.expert, l'outil d'analyse du nouveau règlement européen, Cabinet Ulys, https://www.gdpr-expert.eu/article.html?id=83#difficultesprobables (consulté le 16 mars 2017).

[332] Sur la future réforme de la CVP : voy. Communiqué de Presse du 13 mai 2017, http://www.presscenter.be/fr/pressrelease/20160513/reforme-de-la-commission-pour-la-protection-de-la-vie-privee (consulté le 20 juillet 2017).

[333] Ce constat peut être nuancé par la liberté laissée aux Etats de n'octroyer à l'autorité qu'un pouvoir 'd'initier' l'amende, ultérieurement imposée par une juridiction. Ce pouvoir d'initiation devra lui-même être défini par chacun des Etats membres.

[334]Voy. GDPR.expert, l'outil d'analyse du nouveau règlement européen, Cabinet Ulys, https://www.gdpr-expert.eu/article.html?id=58#difficultesprobables (consulté le 16 mars 2017).

[335] A titre illustratif, notons les inquiétudes de l'Union concernant l'Etat de droit en Pologne. Voy. J. IWANIUK, « En Pologne, l'Etat de droit n'est plus que théorique », *Le Monde*, 9 février 2017, http://www.lemonde.fr/idees/article/2017/02/09/en-pologne-l-etat-de-droit-n-est-plus-que-theorique_5076989_3232.html (consulté le 20 juillet 2017).

[336]Voy. GDPR.expert, l'outil d'analyse du nouveau règlement européen, Cabinet Ulys, https://www.gdpr-expert.eu/article.html?id=58#difficultesprobables (consulté le 17 mars 2017).

[337] Voy. GDPR.expert, l'outil d'analyse du nouveau règlement européen, Cabinet Ulys, https://www.gdpr-expert.eu/article.html?id=58#difficultesprobables (consulté le 17 mars 2017).

Conclusion

174. La décision de la Cour de justice de l'Union européenne d'invalider *Safe Harbor* et de consolider les pouvoirs des autorités de contrôle était un préalable nécessaire à une refonte du système en place.

175. Certes, cette décision a parfois été qualifiée de protectionnisme, témoignant d'une jalousie européenne face au modèle de réussite américain[338]. L'ancien locataire de la Maison Blanche – Barack Obama - avait même été jusqu'à affirmer que si l'Europe s'en prenait à des géants comme Facebook et Google, ce n'était pas au nom de la défense de la vie privée, qui n'était qu'un prétexte ; selon lui, c'est pour des raisons commerciales que l'Union cherche à les bloquer[339]. A cet égard, nul ne peut ignorer que le débat sur la protection des données est pris en otage entre des intérêts commerciaux et politiques divergents. Il n'en reste pas moins que les Etats-Unis démontrent de façon croissante leur éloignement des normes de protection européennes. Il est donc légitime que l'Union tente de préserver son modèle de société et ses standards lorsque les données à caractère personnel de ses citoyens sont concernées.

176. Bien que le nouvel accord constitue une avancée significative dans cette revendication identitaire européenne, il reste de trop nombreuses inquiétudes. Celles-ci touchent tant au cœur des principes adoptés qu'aux voies de recours et aux mécanismes de surveillance mis en place.

177. En ce qui concerne les principes consacrés par l'accord, ceux-ci sont souvent incomplets voir difficilement applicables. Les règles de conservation des données sont claires mais leur implémentation questionnée ; les traitements automatisés sont trop obscurs pour pouvoir prétendre les encadrer ; et le contrôle offert aux consommateurs sur leurs données semble illusoire vu la trop faible information dont ils disposent. Ces préoccupations ne sont cependant pas le signe d'une défaite de l'Union lors des négociations ; elles démontrent plutôt la difficile réglementation des technologies numériques dont la compréhension est parfois insuffisante. Outre le renforcement des principes et l'amélioration des connaissances techniques, il faudra surtout s'assurer de la volonté des entreprises de coopérer au succès du système. L'épée de Damoclès que représente le nouveau pouvoir de sanction des autorités de contrôle laisse présager une conformité accrue.

---

[338] A. CASSART, *op. cit.*, p. 1239.

[339] M. AHMED, « Obama attacks Europe over technology protectionism", *FT*, 16 février 2015, https://www.ft.com/content/41d968d6-b5d2-11e4-b58d-00144feab7de (consulté le 26 juillet 2017).

178. De plus, un *aggiornamento* de l'accord devra être assuré à l'occasion de son premier 'réexamen conjoint' au vu des nouvelles exigences posées par le règlement[340]. Pour ce faire, de nouveaux principes devront y être consacrés, tels que le principe de la 'protection des données dès la conception' ou celui du 'droit à la portabilité des données'. L'importance de cette mise à jour est inversement proportionnelle à sa mise en exergue dans l'accord. C'est en effet par le truchement de la note de bas de page n° 207[341] que la Commission s'arroge le droit, à partir du 25 mai 2018, de suspendre la décision 2016/1250 en cas de non-conformité avec le règlement. L'Europe a mis la barre très haut ; il reste à voir si la Commission osera faire usage d'un tel pouvoir.

179. Au demeurant, ce sont les voies de recours et les mécanismes de surveillance qui doivent être renforcés et simplifiés. Conçu en cascade, le système de recours est abscons et sa mise en œuvre amoindrie par la convergence majoritaire des procédures vers les Etats-Unis ; un rapatriement des plaintes vers l'Union européenne sera dès lors soumis au seul bon vouloir des entreprises. La supervision du système d'auto-certification est quant-à-elle existante mais en apparence stérile. En effet, les pouvoirs d'investigation des autorités américaines sont nébuleux, compromettant un contrôle efficace des pratiques des entreprises en cas de plainte notamment. Ces inquiétudes soulignent le besoin d'une protection des données répondant aux exigences du terrain. Sans détection ni sanction, la violation des principes deviendra la règle et la conformité l'exception. Il faut donner au système les moyens de son contrôle, faute de quoi l'accord ne sera que de façade.

180. La réaffirmation des pouvoirs des autorités de contrôle constitue cependant un heureux contrepoids à cette supervision principalement américaine. Outre le pouvoir d'enquêter sur une plainte visant à contester le caractère adéquat du niveau de protection existant dans un pays tiers, ces autorités sont compétentes pour suspendre les flux de données vers l'entreprise concernée. Le règlement concourt à cette dynamique en leur accordant des pouvoirs étendus et des ressources élargies. Ce 'nouveau printemps' des autorités de contrôle dépendra toutefois de la volonté des Etats de leur fournir les moyens de leur développement ; le rôle qui leur sera effectivement attribué dans le contexte des relations transatlantiques sera au même titre

[340] Un recours a d'ores et déjà été introduit près la Cour de justice de l'Union européenne dans l'affaire *Digital Rights Ireland* ; la demande consiste en l'examen de la validité de l'accord à l'aune des exigences nouvellement posées par le Règlement Général sur la Protection des données.

[341] « *À compter de la date d'entrée en application du règlement général sur la protection des données, la Commission fera usage des pouvoirs dont elle dispose pour adopter, en cas d'urgence impérieuse dûment justifiée, un acte d'exécution suspendant la présente décision, qui s'appliquera immédiatement, sans soumission préalable au comité de comitologie concerné, et qui restera en vigueur pour une période qui n'excède pas six mois* ».

déterminant. A cet égard, le nouvel accord ne leur réserve pas une place de choix ; l'autorité pourra - au mieux - transmettre la plainte d'un citoyen européen au ministère du commerce américain.

181. Les nombreuses craintes gravitant autour du nouvel accord transatlantique peuvent cependant trouver réconfort dans deux certitudes. D'une part, le réexamen imminent de l'accord permettra aux négociateurs de poursuivre leur travail et espérons-le, de corriger les faiblesses du 'Bouclier' et d'en combler les lacunes. D'autre part, le large champ d'application du règlement aura pour effet d'étendre la portée du droit européen à davantage d'entreprises étrangères, notamment américaines. Ces dernières seront directement soumises à l'ensemble des exigences du règlement et non plus aux seuls principes négociés dans l'accord.

182. Finalement, cette contribution est née sous l'impulsion d'une guerre de principes ; les négociations opposaient le modèle américain - piloté par la performance économique – à la position européenne - présidée par le souci de protection des droits fondamentaux. Ce sont deux visions dissidentes d'un besoin pourtant commun : encadrer la circulation des données dans un monde digital sans frontières.

183. Tout comme l'Union européenne et les Etats-Unis, toutes les autres puissances commerciales devront à l'avenir s'accorder sur les termes des échanges de données à caractère personnel. Pour l'heure, les pourparlers répondent à un bilatéralisme strict, marqué par le formalisme et le secret. Les faits dessinent quant-à-eux une courbe nouvelle, dévoilant l'amorçage d'un alignement naturel des législations étrangères sur les standards européens. La désynchronisation mondiale des standards de protection ne trouvera toutefois pas dans cet alignement un remède, mais plutôt un tremplin vers l'adoption d'un cadre international.

184. En tout état de cause, la vitesse adoptée par le développement des technologies numériques ne permet plus de recourir à ces formes historiques de négociation, lentes et ponctuelles. Il est temps de s'unir au sein d'une institution globale dont l'objet sera de faire évoluer, tous les jours, le droit de la protection des données.

Annexe I - Entretien avec Monsieur Ralf BENDRATH, Conseiller principal en matière de politiques auprès de Jan Philipp ALBRECHT (Député européen - Groupe Vert/Alliance libre européenne), réalisé à Bruxelles le 27 novembre 2016

First of all, principles are useless if Redress Mechanisms are too complex for European citizens; a big part of the process is in the hands of the Americans. Do you think we have obtained enough in the negotiations?

Actually, when we had a Committee hearing in March-April, Marc ROTENBERG, from the Electronic Privacy Information Center in Washington, made exactly the point that in the old Safe Harbor, the Redress Mechanism was four steps and now, it is even one step more. So it is more demanding and complex than before.

Then, one of the problem now is that when the companies self-certify, they can choose whether they want to depend from one of the European Data Protection authorities or from a self-certify body from the United-States. As far as I have seen, most of them are using the American bodies, like TRUSTe or Better Business Bureau And they are of course traditionally very friendly towards industries.

So there is no drastic change or improvement compared to the old Safe Harbor?

No, but it is a bit better because they were very expensive. In the Privacy Shield, there is now a fund so that the individuals do not have to pay themselves. But they get funding for complaints. Concerning the efficiency, we will have to wait for the evaluation, to get some experience. The Green Party was more concerned by the ongoing bulk collection and mass surveillance, but also the substance of the Privacy Shield principles. For example, you don't have an 'opt-in' like we have as default in Europe, but you have an opt-out and only in two cases: (i) if data is disclosed to a third party or (ii) processed further for incompatible purposes. It is much weaker than European standards.

What do you think about the self-certification system as whole? For the Court, it is not itself contrary to Article 25 of the Directive, but a proper supervision is then required. Is the Privacy Shield sufficiently answering the Court concerns?

If you would be very nice to the whole approach, you could say companies in Europe have the same situation. Nobody is really checking all of them when they process data so they have to make sure themselves they comply with the law. Chris CONNOLLY[342] has checked in his report how many companies listed in the Department of Commerce Safe Harbor List even have a Privacy Policy on their website, and many of them did not. That basic thing did not even work.

So, it will depend to a certain extent, on how individuals enforce their rights and go against such companies. But also on the Data Protection authorities. As far as I recall, the German authority just recently sent letters to 500 Privacy Shield certified companies and asked them a lot of things such as how they implemented the rules etc. They are trying to be proactive now.

The General Data Protection Regulation is expected to bring more harmonized practices among the national Data Protection authorities, are you convinced by their ability to all work on the same level?

For now, there are Data Protection authorities that are stricter and others are much less strict. In this context, the General Data Protection Regulation is relevant in at least three aspects.

First, you have the consistency mechanism and the one-stop-shop for companies but also for data subjects. So, poor Max SCHREMS does not have to go to Court in Ireland again. Under the new Regulation, he can go to Court in Vienna or to the Austrian Data Protection Authority. And they have to coordinate with their colleagues in Dublin. And if they do not agree, we have this 'binding vote mechanism', under Data Protection Board. Moreover, Max SCHREMS can also go to Court in Vienna, in its own language. It is also much cheaper that in Ireland, apparently.

[342] Consultant to the United Nation Conference on Trade and Development (UNCTAD); he has been the author of several reports on privacy and cyberlaws.

Secondly, you have the fines up to 4% of the worldwide turnover. So that is a lot of money and it is already clear that a lot of Information Technology (IT) players are now really trying to adapt to the new Regulation, much better than what they used to do so far for the old laws. With such a fine, the chief executive boards are rally now listening to their data protection officers (DPO). It also applies to companies that transfer data under the Privacy Shield and then do not comply.

Thirdly, a lot of companies won't need the Privacy Shield anymore, because they are directly in the scope of the new Regulation. Article 3 of the Regulation established the principle of market location. So wherever they are, even if they are just based in Silicon Valley and have their servers there, without being established in Europe, or they offer services on the European market and then process data back home, they have to comply with the full Regulation. Not just with the weak Privacy Shield principles.

It is a great improvement, but it does not solve the mass surveillance problem.

Well, companies are trying to solve that issue, by transferring their data centers to Europe. But you still have the problem of European mass surveillance.

The German Parliament recently adopted a new Foreign Intelligence law, which is crazy. And the investigatory powers in the United Kingdom are enormous. And they will never get an adequacy rating on this after Brexit. At least, the National Surveillance Agency (NSA) will have more difficulties to get hands on their data. What should be kept in mind is that national security is out of the European competence.

The question is who actually has the power to define what national security means. So on, the studies have defended the fact that in the European constitutional tradition, national security means the security of the rule of law, the security of fundamental rights and things like that. You cannot use that as a white card, to just do mass surveillance as much as you like. The question then is that, at some point, it should be clarified by the Court. The Commission should ask what the treaties actually mean and how to apply them. But it means that one would bring one of the Member States to Court and I recently heard that the Commission just started an

infringement procedure against the United Kingdom, in the context of PRISM[343] and TEMPORA[344]. But they stopped it, because of Brexit. It is more political.

Some are pleading for separating the commercial issues from the mass surveillance ones. Would that make sense in a context such as the Privacy Shield?

Well, in the context of the Privacy Shield, it makes sense to keep them together, if we look at the SCHREMS judgment of the Court. Within the European Union, it is maybe different because of the issue related to know where is the Union competence and where is the Member States competence. But there is growing cooperation among intelligence surveillance in Europe. And sometimes there is an interesting overlap on what they do on the national level and how they cooperate bilaterally or multilaterally.

We also have to look at what has done the Counter-terrorism group, established in The Hague. So it seems there is a growing structure for more formalized and institutionalized intelligence cooperation across or among Member States. The question is to know whether we should, at some point when the next Treaty changes, put that inside the European competence. But that is going to be a big step for Member States. And I am honestly not sure if that is a good idea. But we need that debate at some point, probably.

What about the idea of enacting brand new international standards and principles of data protection, agreed on by all countries?

There are already international agreements or some hard law, that go beyond the European context. That is the Council of Europe Convention 108 which includes for example Turkey and Russia. And they just revised it, based on our European reform. But the text is now hanging, because there are some issues with Russia. And an international treaty can only be changed unanimously. But there are also the Organization for Economic co-operation and Development (OECD) guidelines from 1980 which extends even further. Then, there is European Partners Again Corruption (EPAC) guidelines.

[343] Le programme de surveillance de masse mené par la 'National Security Agency' (NSA), aux Etats-Unis ; celui-ci fut révélé en 2013 par Edward SNOWDEN.
[344] Le programme de surveillance de masse mené par le 'Government Communication Headquarters (GCHQ) - le service de renseignements électroniques du Gouvernement du Royaume-Uni ; celui-ci fut révélé en 2013 par Edward SNOWDEN.

But to get to one fully harmonized worldwide international treaty on data protection, which also would be our European standards, it is probably very difficult. But, on the other hand, a lot of countries are adopting data protection laws that are modeled under the EU model, in order to get the adequacy decision.

Well, trying to elaborate those global standards might push other countries to adapt their data protection laws, such as China for instance.

The Parliament Research service made a study, on data protection in China, and they are indeed far from being good enough. But I know that Japanese ministry of Consumer Protection - or Justice - is looking into the new European rules, and seeing if they can adapt the Japanese data protection laws to get an adequacy rating. The European Union is already, *de facto*, the central standard. People try to get the adequacy rating and they follow us.

What are your thoughts on a centralized data protection authority for the European Union, which would replace the 28 national data protection authorities?

I don't think that would be necessary. I am from Germany, which is a Federal State, so we have sixteen authorities at the State level and then the Federal as well. And that works pretty well, because it is more distributed, more decentered, this is also closer to the action, so to speak. It is also easily reachable for the individuals and closer for companies. We find that in a lot of fields such as banking supervision, telecommunication regulations etc. We actually looked at all those existing models of regulatory, supervisory authorities and how they make sure that they have a coherent application of the law.

Consistent enforcement is the main point. And the model we came up for in the new Regulation is a bit unique, because it is the only policy field were the authorities are independent under European primary law. So that is why we have answered that they have to coordinate, they can even have binding decisions, which also bind the national authorities, but that still meet the criteria of independence because they are still independent from the government and from the Commission. But if that works well, then we are in the process of establishing a Board and the structure of the Secretariat. If that works, it is a good approach. And you don't need a centralized European authority for all these decisions, that only affect the data control somewhere in Germany.

So, here comes the benefit of the new Regulation which cures the discrepancies between the national authorities' practices; it provides for a harmonized and consistent enforcement of European law.

Yes, exactly. We wanted to make sure that the powers are close. Then, on top of that, you also have the European Supervisor, who is only competent for the supervision over EU institutions and bodies. But it still gives advices to the legislator here in Brussels.

In the context of complaints, do you think the Redress Mechanisms existing in the Privacy Shield, starting from a request to the company, will enable the individuals to get their rights fixed in cases of violation?

Well, indeed, you usually start with a request to the company. It responses. It can say 'yes we made a mistake and we have fixed it', and then everything is fine. But otherwise, you might want to get a fine because they did not comply. If the company does not follow up, such as Facebook saying to Max SCHREMS, "everything is fine here", then you can use the redress mechanism, the arbitration body either here or in Washington. But actually, it is thankfully clarified in the adequacy decision by the Commission, that European Data Protection authorities are always competent to suspend data flows, if they think something is not right. And so, no matter the arbitration body and the United States are saying. So that is always the last resort.

The recognition of that power by the Court is then a victory for the independence of Data Protection authorities.

Exactly, and that was a big question submitted to Luxembourg. The Irish Data Protection authority said that they were not competent to suspend data flows, because the Commission decision is binding on the Member States and national authorities. And the Court reaffirmed that the authorities were independent under primary law, and they always can stop data flows. And now, it is in the adequacy decision itself. Well, it will obviously depend on the national authorities and whether they are strong enough. But that will hopefully be so with the new consistency mechanism under the General Data Protection Regulation.

Moreover, the Member States have a specific obligation to appoint people who have experience in the field, that have knowledge and to give them resources. It includes legal and

technical expertise. So, when we negotiated it, there was some idea to even say all this should be based on the size of the population and the amount of data processing taking place in that Member State. But is very hard to assess. We did not get that far because somehow it is also the budget competence of national parliaments. Anyway, they need to be able do their job. And if not, the Commission should theoretically start infringement procedures.

Regarding the appointment of the members of the Data Protection authorities, there is a choice between involving the National Parliament or not. We know that Member States are quite reluctant to give too many powers to independent bodies, that are out of their control. Could that endanger the independence requirement of the authorities?

Yes, exactly. We can see that for example in Germany. The former Federal data protection commissioner was very good. He had experience in that field and had written books on data protection. He was very good and was even the chair of the Article 29 Working Party. When his term ended, the Grand Coalition in Berlin appointed a former member of the German Parliament, who had no experience in the data protection field, whatsoever. She turned out to be not so ambitious, to put it mightily. She made some good statements on mass surveillance for example, but she has not been as active as the previous one by far. It is a problem.

You see the same development if Courts become too influential, too activist. Then, Members States and governments tend to appoint judges that are nicer to them. That is a structural problem and I do not know how to solve that. We at least made sure, in the Regulation, that there are certain criteria for these appointees. They need to have experience in the data protection field; knowledge at least.

Knowing that The Privacy Shield will be annually reviewed, what are the most important aspects to work on in order to avoid another annulment by the Court?

We did not like the Privacy Shield to begin with. And we are currently negotiating a Parliament Resolution[345] on the final text of the Privacy Shield. The principles are just not good enough. That you only have opt-out in two cases and no opt-in. The redresses are terribly

[345] COMMISSION DES LIBERTÉS CIVILES, DE LA JUSTICE ET DES AFFAIRES INTÉRIEURES, "Draft Motion n°2016/3018 (RSP) for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-U.S. Privacy Shield", 7 décembre 2016.

complicated. And the Federal Trade Commission (FTC) does not have to follow up on each individual case, like a Data Protection authority would have to do.

But all that is tricky, because for a review, you do not normally criticize the fundamental underlying act as such but you just look at whether it is properly implemented. In that area, we will have to see whether people complained, and if so, if their complaint was successful and was easy for them to submit. What is important is that the German authority for example has already sent a couple of letters to companies, to know how they are dealing with it now.

Honestly, more relevant will be the Court cases that are coming up to kill the whole thing again. There are already two cases pending in front of the European Court of justice, Digital Rights Ireland and Lagfarter to the net. They went directly to the European Court and you can only do that if you can prove that you are directly affected by an European level decision. So that does not happen so often. So the Court might turn them down. But then, Max SCHREMS will go to national Courts and national Courts will submit the case to the Court of justice, that is easier. It is more relevant.

So you are quiet pessimistic about the benefits that an annual review is likely to bring, even though many issues are still to be discussed?

Yes. We have some experience with regard to these annual review provisions. For example, the EU-U.S. terrorism finance agreement, the so-called SWIFT[346] agreement, there was a review clause. But there you could already see, a couple of years ago, that it is not possible at all to talk about real problems. But we have to see, we are currently discussing in the Parliament about this Resolution.

We should insist on the fact that the Data Protection authorities, also involved in the review teams, should be able to issue an independent so-called 'minority opinion', so to speak, if they can't agree with the Commission on the final review assessment. But even there, the conservative here in the House are not willing to do that. Just close your eyes, and let the data flow.

[346] Society for Worldwide Interbank Financial Telecommunication.

With the exclusive power to decide about the adequate level of protection in a third country, the Commission detains a lot of power. Do you think it should remain like that?

Well, it is true, since 1995. But it is actually a bit better because, now in the Regulation, we have established criteria. And we also put the clarifications from the beginning that 'adequacy' means 'essentially equivalent'. So, on substance, it is a bit better. The Parliament actually wanted to have it as a Delegated act. Then, the Parliament would have had a veto power. But that was impossible to get agreed by the Members States in the negotiations.

Is the Privacy Shield strong enough to offset the weaknesses of American laws with regard to data protection? It seems already to be a satisfying first step, as we cannot compel the United States to change their laws.

Implementing the decision by the Commission or civil law contracts on standard contractual clauses or even consent from data subject does not change US laws. They would have indeed to change their laws, that is the big elephant in the room. They would have to change their laws in wo respects. First, to stop the indiscriminate mass surveillance. Second, to finally to come up with a proper and comprehensive data protection law. Obama tried last year, with the Privacy Bill of Right, but it was dead in the water the moment it was published. That is where the United States should go if they want to be a proper trading partner, in the matter of data.

So, instead of agreeing on this Privacy Shield quickly, and giving the Americans another opportunity to transfer in, actually, a privileged way as compared to other countries, the Commission could have been much stronger. By saying that the European Union has very strict criteria and cannot afford that the next adequacy decision is turned down again by the European Court of justice; it undermines the European overall credibility. They could have required from Washington to do something, on their side. They could have, at least, try but they did not. The general assumption that everything is fine in the United-States is just not possible anymore after Snowden I am afraid.

The NSA is mainly digging into the big companies, are there any reports concerning smaller companies? Are they safer?

Well, yes, there are Yahoo revelations, that apparently happened while they were negotiating on the Privacy Shield. Fool me once, shame on you, fool me twice, shame on me! Seriously, concerning smaller companies, a few self-certified under the Privacy Shield. But they could also wonder whether they have to transfer data to the United-States. They can also keep it in Europe and use European data processors, and then, they are safe. It gives job to Europe. Moreover, many companies, after the SCHREMS judgment, have moved to Standard Contractual Clauses and they do not need the Privacy Shield anymore. But Max SCHREMS has a case pending in Ireland, regarding those standards contractual clauses.

Annexe II - Entretien avec Monsieur Theodosios KOTTAS, stagiaire à l'Agence des droits fondamentaux de l'Union européenne, réalisé à Vienne le 27 juin 2017

First of all, is the General Data Protection Regulation a partial remedy against the weaknesses of the Privacy Shield agreement?

If you look at the agreement, in Article 45 of the adequacy decision, you can clearly see the existence of an annual review of the Privacy Shield. In any case, it must be compatible with the General Data Protection Regulation and if it is not at the moment, it will have to be compatible. That's already an issue.

If the companies want to operate outside the Privacy Shield, they will have to comply with the new Regulation. But it is much more difficult to send data from the European Union to the United-States just with applying the Regulation. There is no presumption of adequacy, so you will have to go through either the Binding Corporates Rules (BCR) - which for instance Facebook is using at the moment - or to have bilateral agreements between the companies, and then going to the Data Protection authorities.

From a commercial point of view, I don't think it is cost-effective for the companies. It is the reason why the Shield creates that presumption. The companies now subscribe for the effect of the Shield in their transactions so you have easier transfer of data. So if the shield doesn't apply at all, you have commercial problems.

Is the first 'joint annual review' a genuine review or just the continuation of the negotiations? The question is real if we look at the number of topics which have been postponed to that first review, such as the automated decisions issue.

There is a famous footnote 158 [207] in the Privacy Shield. It says that, after the enactment of the Regulation, the Commission reserves the right to suspend immediately the Privacy Shield if they see that it will not comply with the Regulation after the review. They have set a very high standard. So the review is essential at this point.

When they were negotiating the Shield, they were at the same time negotiating the Regulation. They had in mind what would be the result of the European data protection reform

but at the same time, in the Council, there were a lot of fights about the effect of the Regulation. It is why they postponed the first annual review, as they did not know what would be the result of the negotiations.

With regard to the automated decisions, the problem is that nobody knows what it is. The creators of the algorithms don't even know how it works. The legislator is far behind the technology. Once you go through all the legislative procedures of the European Union, there is a question: do you legislate for a directive or a regulation. If you go for a directive in the automated decisions, for instance regarding artificial intelligence, big data or internet of things, you will end up with 28 different legislations. There is no result in the end. If you want a regulation, the countries will say they don't want it this way and that it is difficult to enforce.

As a result, you have a lot of countries that are opposing to the decision, as it is the case with the Regulation now. So there will be an advancement once the technology is a bit clearer. In the 2018 European Fundamental Rights Agency (FRA) report, there will be a specific Chapter on the algorithms and the automated decisions.

Would ethic be a solution?

The Ethic advisor board of the European Data Protection Supervisor is a good step forward. They try to promote, when you implement privacy by default, the implementation of ethics. But at the same time, if a company uses an algorithm, they don't know about that. It is a problem. For this matter, it is not necessary to notify the data protection authority. When you use an algorithm, you say that you process data but you are not obliged to disclose what is the algorithm.

The General Data Protection Regulation provides for a right to ask for a 'human intervention' in cases of automated decision-making, how is it going to work if the process itself is obscure?

There is a national example with the Netherlands. They use a lot of big data, automated decisions, for tax purposes for instance. It allows them to locate 99% of the fraud cases, through big data. But if the person contests the decision in Court, and asks how the decision was made, the answer will be "we don't know". It will be a problem with the Regulation. But you have the

processing of data for a 'legitimate interest'. The States and national authorities who use algorithm, they will rely on the legitimate interest. For commercial purposes, it will be difficult.

Do you have an example of a commercial processing of data for 'legitimate interest'? It seems tricky.

If, for instance, a commercial entity is hired by the State to do something for the latter, then it might exist, depending on the purpose of that public service. For instance, if it is a telecommunication provider, they use algorithms to locate people having habits to visit terrorist groups on Facebook. It can be 'legitimate interest'. The contract between the State and the telecommunication provider is purely for commercial purposes.

The definition of what constitutes a 'legitimate interest' will then be left to the public authorities?

Concerning the definition of public interest, if you look at the European Fundamental Rights Agency (FRA) annual report of this year, we talk about this. Now, it is for the member States to set appropriate fundamental safeguards. The Regulation cannot foresee all the situations that are going to arise. Obviously, it is the big problem when an individual asks for an information that neither the State nor the company can give, then it is for the Member States to resolve the issue between the companies and the State. At the moment, the Regulation cannot go too far regarding the disclosure of algorithms, because it is opposed to the business secrecy.

The Regulation is expected to bring more harmonized legislations and practices among the Member States, but the companies are not ready yet. Is the new Regulation asking too much, without distinguishing big companies from small and medium ones?

From all the conferences and missions that I have attended, we gathered that the big companies such as Facebook, Google or Microsoft they are ready to implement the decisions. Even though they disagree with more than 50% of the text, they can do this as they have the money. How is it going to be implemented by small and medium enterprises? It is difficult. So a solution coming from the big companies is that they provide all the systems necessary for implementing the Regulation and they sell them to the smaller companies.

With the directive, the problem was that the fundamental rights safeguards were all different depending on the Member States. They were exploiting loopholes of a Member State in order to transfer data. But now it is a good thing with the Regulation.

In the 2013 Report on the access to Data Protection remedies in EU Member States, the Agency underlined that the Data Protection authorities were both inefficient and inaccessible. Are you now satisfied with the changes brought by the new Regulation, increasing and harmonizing their powers throughout the Union?

The main issue is for the State to inform the public about the pathways towards the remedies. The remedies might be there but most of the people don't know they have the right to go to the Data Protection authorities. It is the main problem to tackle.

In my opinion, the Regulation reinforces a lot the remedies. But what do we mean by efficient and effective remedies? Do we mean that the people are using them or that if they use them, they work? That's a question. To know whether they use them is more a matter of policy and not a matter of law. But the public should be informed through Fundamental Rights Agency reports, Member States reports and events. The national authorities have also started organizing events in the Member States to inform the public. For instance, the 'Commission Nationale de l'Informatique et des Libertés' (CNIL) in France, the national authority in Belgium or the United Kingdom as well. They issue guidelines and try to come closer to the public.

Beside the knowledge of the available remedies, should the data subjects receive more information, on a regular basis, about the way their data are being used? More information might be necessary for the individuals to determine whether their data have been mishandled.

I believe for this issue, there are four things.

First, it concerns how the Data Protection authorities enforce and enhance Privacy by design and by default. It already creates a presumption, if correctly implemented, that Privacy is respected through the processing of data. The whole system will be designed with Privacy in mind.

The second is 'consent'. If the latter must be written and straightforward, it also ensures the individual is aware.

Third, there is the data protection impact assessment. Before you even put your system in force, you have those templates to fill in. The idea is to say that your system works sufficiently to comply with the Regulation. If they pass the Regulation impact assessment, then there is a rebuttable presumption that they will comply with both the privacy by design and by default and with the consent requirement.

Fourth, the Data Protection Officer (DPO) role is important in the case you submit a complaint to the company. He must examine the request and if he thinks things have not be done correctly, the Data Protection Officer will provide additional information to the individual concerned. If not, then you can file a complaint to the Data Protection authority. Then, the remedy is not to find out about your data but the Data Protection authority will tell whether there was a wrong processing or not. It might lead to the obligation for the company to amend their privacy policy. Or, even deeper, to change the whole system concerning the information of individuals on how they process their data while using the software.

If the individual whose data are processed, enters a system in which all those requirements are fulfilled, then they should be able to receive more information about the way their data are processed. All the Privacy Policies are written in very clear words. Of course, I am not sure if it will be done during the first years of implementation but ultimately, we will reach that point.

Concerning the Data Protection Officer, is he always working inside the company?

Yes, it depends on the type of data they are processing not on the size of the company anymore. If you are a telecommunication service provider, it is sure that you will need a Data Protection Officer. Because you process so many data, and most of them are sensitive. The Officer is not necessarily only the Officer, but it can be a technician. For instance, in the Fundamental Rights Agency, we have a Data Protection Officer who is also an 'Information and Technology' (IT) officer. So, whenever you have a data protection issue, you go to the Officer to discuss the matter. Possibly, the Officer is responsible for keeping under control the policy of the institution for data processing.

It does not seem that they are subject to any independence requirement in the Regulation. For instance, if a Data Protection Officer is also an internal worker of Facebook, how can we ensure they will handle the case with full independence and impartiality? Isn't there a conflict of interest?

In the Regulation, there is no independence requirement. The Data Protection Officer is not necessarily an inside worker but the duty can be outsourced. Facebook, for instance, outsource to consultancy companies. The issue is more related to the liability of the Officer. If the Officer is negligent, then there is an issue. At the moment, the Regulation is not clear concerning that liability. Under the directive, it was up for the Member States to decide. So it is for the company itself to put some sanctions on the Officers in case of negligence. But obviously, you cannot have 100% independent Data Protection Officers.

Data protection compliance has become a major competitive advantage for the companies which are correctly fulfilling their obligations. Are we going towards a form of auto-regulation, as there is too much to lose in cases of non-compliance?

At the moment, the big companies are rushing and advertise their compliance everywhere. At a recent conference that I attended, Google was there and they emphasized their compliance; for instance, with 'my Google account' were you can check your data and advertisements. Of course, it is a competitive advantage. As long as a customer feel safe, it will continue using the company services.

What do you think about the idea of coming back to an old system, where you would be able to pay the same amount Facebook earns while collecting your data, in exchange for no advertisement and better data protection?

Well, that's interesting. But we are not sure that even if you pay, you won't have any advertisement anymore. If you provide your consent for your data to be used and sold to third parties, then you accept the system. With Facebook, every time your login, this is your payment. In the Privacy Policy of Facebook, you can clearly see that every time you press login, this is your consent without reading anything.

Concerning Facebook-WhatsApp case, what do you think about the way it was handled by the Commission? Are we falling short of rules to tackle those increasingly complex issues?

There is a big difference between the United States and the European Union concerning privacy issues. In the United-States, a collection is not considered a collecting of data. In Europe, the processing starts with the collection. So in the United States, the problem is that using and sharing data with another company is just collection. This is a main difference. In the European Union, it is forbidden.

Now, the Regulation will make the rules easier to enforce. The Commission wants to fine the Facebook-WhatsApp case as a matter of competition law. They did not intervene in data protection. As now, enforcement of data protection law is more a matter for the Member States. But using competition law to sanction data protection issues is also a bit scary.

Competition law as a whole might need to be reshaped in order to face those new types of services, which are sold for data rather than for money. What do you think?

It is true. However, as we now have a regulation rather than a directive, you will have the new article Working Party Article 29. It will be coordinated between the Data Protection authorities. You also have the one-stop-shop, through which authorities can support and coordinate each other. It will be easier now. Coordination between the national authorities has even become an obligation under the Regulation.

I am not sure if competition law should work like this. In the United States, they only have Privacy and they don't have data protection law. It is a big difference because in the European Union, we have both. In the United States, for pure data protection issues, they say there is a contract between the consumer and the company so this is within the contract. As a State, they thus don't have any jurisdiction to intervene. That's why the competition law rules apply in the United States.

What is your opinion on the new move of Donald Trump, suppressing consumer consent for allowing telecommunication service providers to collect and sell their data?

Very recently, in the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament, there was a hearing on this matter. The Members of the European

Parliament expressed publicly their concerns about the amendment of the United States Privacy laws. This is going to be part of the annual review.

I don't want to be a prophet, but at the present moment, they should suspend the Shield. It is scary. But it would be very difficult for the companies, so the Commission will long be hesitating. The companies are struggling complying with the Regulation, so if you also stop the Shield, they will have a hard time.

What are your thoughts on the Digital Rights Ireland case? Is the Court going to wait until the entry into force of the General Data Protection Regulation?

A good step is to hear the opinion of the Advocate General but it did not fully take place yet. First, the hearings will take place and then one month later, the opinion of the advocate general will take place. But the workload is heavy for the European Court of Justice. You also have the national judgments to wait for.

The request by Digital Ireland is to check the validity of the Shield regarding the directive. But they changed it, as they want to compare it with the new Regulation. As the Court cannot yet use the Regulation, they will have to wait. They might start the hearings after the first annual review and then wait to render the judgment. The Regulation came after SCHREMS. It is then better to have an evaluation against the Regulation rather than against SCHREMS; the requirements of SCHREMS are still related to the Directive. Anyway, the Court won't be able to go very far. Analyzing the American situation was already very sensitive.

When the Shield was negotiated, a very symbolic picture has been released. Obama was signing the new laws in the presence of the Ambassador of the European Union. This is already something than we have never seen before: Europe making the United States to change their laws to secure a decision. The European Union is not a State so the presence of the European Ambassador is a big step. Before the directive in the 90s, we would never have imagined that. The Shield is then already a good step.

What do you think about the extended scope of application of the new Regulation?

This is for the benefit of European citizens. It is not that they just want to apply European law for commercial entities that are in a third country. They want to ensure that whenever data

of European citizens are involved, they are 100% protected. How else would you communicate to the European citizens than their data are processed in a legal manner, if it is not the laws of the European Union.

Of course, extraterritorial application of European law is a bit tricky because again, the Union is not a State. And even when a State applies its laws in another country, there is a problem. But at the same time, it is voluntary. They don't say European law will apply to them, they say if you want to continue commercial relations with the European Union, you have to comply with our standards. It is the same thing with the single market. The product specifications have to comply with the internal market regulations, otherwise you cannot export something within the Union. As you said before, there is no exchange of money but data, then we need a 'digital single market' as Juncker says. We need this to be applied globally.

International data transfers are becoming complex as far as the applicable legal framework is concerned. Does the requirement of a 'substantially equivalent level' of protection, as laid down by the Court, amount to an extraterritorial application of EU law?

My opinion is that the requirement of adequate level of personal data protection does not amount to extra-territorial application of European law. It is in the absolute discretion of the State in question to choose the means by which personal data are protected; it is however, the level of protection that should be essentially equivalent to the one guaranteed in the EU legal order.

In addition, the Court of Justice does not assume jurisdiction on the legality of the concerned State's legislation. The jurisdiction arises only on the basis of the Commission's Adequacy Decision which is part of the European Union's legal order. If the Court adjudicates on a State's level of protection of personal data, it is only based on the assessment conducted previously by the Commission; the European Court essentially confirms or annuls the Commission's assessment. The Court of Justice will never oblige a third country to change its legislation.

In that regard, are Data Protection authorities sufficiently powerful to ensure the respect of European law, knowing that they have no jurisdiction outside the European borders?

First, after SCHREMS, the Data Protection authorities have now jurisdiction to check how European data are used. They can suspend the commercial activity of a company in the Union if the processing of the data does not respect the Regulation.

To ensure some consistency within the Union, the Working Party Article 29 is under an obligation to ensure coordination, and the one-stop-shop will be helpful. The latter principle implies that the competent national authority is the one of the country where the company has the biggest presence. That authority will handle all the requests. As an individual, you go to your national authority, which is not necessarily the one which is going to decide on the issue. If you are part of a bigger problem, one authority will coordinate the whole thing and the decision will be uniform. Now, the Regulation harmonized the way national Data Protection authorities should work. But we don't know yet if it is really going to be the case.

An infringement procedure could be started if, for instance, the State does not provide enough resources to its Data Protection authority. Would that be realistic, looking at the political sensitiveness of the issue?

Yes, normally it is possible. But I am not sure if it is really going to happen. How do you assess the money and resources to be provided by a State to an independent authority? You have to look at the Data Protection authorities' workload, which depends on the number of companies which are present in the country. For instance, the national authority in Greece has less work than in the UK, Germany or France.

Ralf BENDRATH, Senior Policy Advisor to MEP Jan Philipp ALBRECHT, told me that when negotiating the new Regulation, they went as far as discussing the possibility of imposing 'resources quotas' to the Member States. Could that have been a solution?

Well, yes, but it would never pass in the Council. Of course, it is a matter of priorities at the moment. It depends on how the Data Protection authorities are willing to implement the law.

What we have heard in the context of contact we have had with national authorities is that, for now, they are very busy in still implementing the directive. They do not have the time to analyze the new legislation. The 25th of May will come soon, but they are not ready yet. It is a problem. Again, it might be an issue of resources, as they could need to hire more staff and legal counsels to analyze the new Regulation. But, again, it depends on the Member States.

They did not have sufficient time. And I don't think it was a problem of the period let by the legislator, which was two years, it is a lot to prepare. The authorities had so many complaints, and they are still initiating the investigations that they were filing years go. They say they do not have time to adapt. It led again to a comparison between the big companies and the Data Protection authorities. The former was saying, we have the power to implement the General Data Protection authorities now because we have the money, we have staffs. The Data Protection authorities are very limited, sometimes not going to more than 50 people there.

The national authorities do not seem to be ready to deal with a large number of claims, which is however highly expected under the General Data Protection Regulation.

I really hope they will able be able to do so. Otherwise, the Regulation was just a painful negotiation. Especially in the Council. If in the end, it does not work out, then this will be a shame. It was a massive step forward, even though not everybody agrees.

Even if it is admittedly difficult to implement, the benefits resulting even from 70% of implementation would be good. Looking at all the laws the companies have to comply with, obviously, they don't comply with 100% of all of them. You can't reach 100% compliance when you have daily transactions. But at least the effort to start complying with the main principle will lead to large benefits for the citizens and for the companies themselves, as they will gain trust for the consumers. It is going to be very beneficial. If the companies are more ready to comply, then, it will be easier for the Data Protection authorities to do their job as they won't face too much work.

As we are now waiting for the first annual review of the Privacy Shield agreement, what is the main clash to be expected? Still the Prism reminiscence?

Yes, it will be the access of the United States public authorities to the data of European citizens. This thing has not changed. It is the National Security Agency (NSA), the Central

Intelligence Agency (CIA), the intelligence services, I don't think they are prevented from accessing the data. They try to implement sort of remedies, but still you don't have any right of notification if you are under surveillance and the bulk collection of the data is not clear yet.

When your data are transferred for commercial purposes, and then used for security purposes, there is an issue. If the collection if for 'legitimate interest', then let's have appropriate safeguards and have access to all the data. But without those safeguards, appropriate oversight or authorization, it cannot work. The United States Foreign Intelligence Surveillance Court (FISA) authorizes easily the access.

What about the refusal by WhatsApp and Apple to create a 'backdoor' for the public authorities? Is it a step forward or just an illusion of protection against that bulk collection?

For WhatsApp, it is related to the content, as the content is encrypted. But who is communicating with whom, what time and when, this is all available. When Apple is saying, 'you don't touch the IPhone', you still have the telecommunication provider collecting data thanks to the SIM Card.

All the data contained in the SIM card such as the location - coming from the satellite - who you contact and when, all this is already a lot of information. You can't see the photos that are stored but if you use the cloud, it is different. Metadata are equally important. You can collect all the information and then get the broader picture. So, it is the main issue. A lot of things can be pushed, but when you are dealing with security issues, then I don't know how far the European Union can push.

Bibliographie

❖ LÉGISLATION

CONSEIL DE L'EUROPE

- Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955.
- Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *STE 108*, Strasbourg, 28 janvier 1981.

UNION EUROPÉENNE

- Charte des droits fondamentaux de l'Union européenne, *J.O.U.E.*, C 364 du 18 décembre 2000.
- Traité sur le fonctionnement de l'Union européenne, *J.O.U.E.*, C 326 du 26 octobre 2012.
- 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 du 23 novembre 1995.
- Règlement (CE) n°45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, *J.O.C.E.*, L 8 du 12 janvier 2001.
- 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 95/46/CE (règlement général sur la protection des données), *J.O.U.E.*, L 119 du 4 mai 2016.

❖ **DÉCISIONS, RÉSOLUTIONS, COMMUNICATIONS, AVIS ET RECOMMANDATIONS**

PARLEMENT EUROPÉEN ET COMMISSIONS PARLEMENTAIRES

- 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.

- COMMISSION DES LIBERTÉS CIVILES, DE LA JUSTICE ET DES AFFAIRES INTÉRIEURES (LIBE), « 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.

- 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.

- DIRECTION GÉNÉRALE DES POLITIQUES EXTERNES DU PARLEMENT EUROPÉEN, « Transatlantic Digital Economy and Data Protection : State-of-Play and Future implications for the EU's External policies », *ISBN:978-92-823-8660-6,* 1er juillet 2016.

- COMMISSION DES LIBERTÉS CIVILES, DE LA JUSTICE ET DES AFFAIRES INTÉRIEURES (LIBE), "Draft Motion n°2016/3018 (RSP) for a Resolution to wind up the debate on the statement by the Commission pursuant to Rule 123(2) of the Rules of Procedure on the adequacy of the protection afforded by the EU-U.S. Privacy Shield", 7 décembre 2016.

COMMISSION EUROPÉENNE

- Décision (CE) 2000/518/CE de la Commission du 26 juillet 2000 constatant, conformément à la directive 95/46/EC du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel en Suisse, *J.O.C.E.*, L 215/1 du 25 août 2000.

- Décision (CE) 2000/520 de la Commission du 26 juillet 2000 conformément à la directive 95/46/EC du Parlement européen et du Conseil relative à la pertinence de 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 du 25 août 2000.

- Décision (CE) 2002/2/CE de la Commission du 20 décembre 2001 constatant, conformément à la directive 95/46/EC du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi canadienne sur la protection des renseignements personnels et les documents électroniques, *J.O.C.E.*, L 2/13 du 4 janvier 2002.

- Décision (UE) 2003/490/CE de la Commission du 30 juin 2003 constatant, conformément à la directive 95/46/EC du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par l'Argentine, *J.O.U.E.*, L 168/19 du 5 juillet 2003.

- Décision (UE) 2003/821/CE de la Commission du 21 novembre 2003, constatant le niveau de protection adéquat des données à caractère personnel à Guernesey, *J.O.U.E.*, L 308/27 du 25 novembre 2003.

- Décision (UE) 2004/411/CE de la Commission du 28 avril 2004 constatant, conformément à la directive 95/46/EC du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel dans l'Ile de Man, *J.O.U.E.*, L 151/51 du 30 avril 2004.

- 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.

- Décision (UE) 2008/393/CE de la Commission du 8 mai 2008 constatant, conformément à la directive 95/46/EC du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré à Jersey, *J.O.U.E.*, L 138/21 du 28 août 2008.

- Décision (UE) 2010/411/CE de la Commission du 5 mars 2010 constatant, conformément à la directive 95/46/EC du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la loi des Iles Féroé relative au traitement des données à caractère personnel, *J.O.U.E.*, L 58 du 9 mars 2010.

- Décision (UE) 2010/625/UE de la Commission du 19 octobre 2010 constatant, conformément à la directive 95/46/EC du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré en Andorre, *J.O.U.E.*, L 277/27 du 21 octobre 2010.

- Décision (UE) 2011/61/UE de la Commission du 31 janvier 2011, constatant, conformément à la directive 95/46/EC du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par l'Etat d'Israël concernant le traitement automatisé des données à caractère personnel, *J.O.U.E.*, L 27/39 du 1 février 2011.

- Décision d'exécution (UE) 2013/65/UE de la Commission du 19 décembre 2012 constatant, conformément à la directive 95/46/EC du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la Nouvelle-Zélande, *J.O.U.E.,* L 28/12 du 30 janvier 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.

- 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.

- 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.

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

- 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.

- Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/EC 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 du 1er août 2016.

- Décision d'exécution (UE) 2016/2295 de la Commission du 16 décembre 2016 modifiant les décisions 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE et 2011/61/UE, et les décisions d'exécution 2012/484/UE et 2013/65/UE constatant, conformément à l'article 25, paragraphe 6, de la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par certains pays, *J. O.U.E.*, L 344/83 du 17 décembre 2016.

- COMMISSION EUROPÉENNE, « Concentrations : la Commission affirme que Facebook a communiqué des informations trompeuses sur le rachat de WhatsApp », *Communiqué de Presse, IP-16-4473*, 20 décembre 2016.

- COMMISSION EUROPÉENNE, *Guide to the EU-U.S. Privacy Shield*, Belgique, 2016.

- COMMISSION EUROPÉENNE, « Mergers : Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover », *Communiqué de Presse, IP/17/1369*, 18 mai 2017.

NATIONS UNIES

- Résolution 45/95 de l'Assemblée Générale des Nations Unies relatives aux principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel », adoptée le 14 décembre 1990.

GROUPE DE TRAVAIL ARTICLE 29 (G29)

- G29, « Premières orientations relatives aux transferts de données personnelles vers des pays tiers – Méthodes possibles d'évaluation du critère adéquat de protection », *WP4*, 26 juin 1997.

- G29, « Transfert des données personnelles vers des pays tiers : Application des articles 25 et 26 de la directive relative à la protection des données », *WP12*, 24 juillet 1998.

- G29, « Avis n°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 », *WP15*, 26 janvier 1999.

- G29, « Avis n°4/2000 sur le niveau de protection assuré par 'les principes de la sphère de sécurité' », *WP32*, 16 mai 2000.

- G29, " Document de travail n°5035/01 : Application internationale du droit de l'UE en matière de protection des données au traitement des données à caractère personnel sur Internet par des sites web établis en dehors de l'UE", *WP56*, 30 mai 2002.

- G29, « Document de travail : Transferts de données personnelles vers des pays tiers : Application de l'article 26(2) de la directive UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données », *WP74*, 3 juin 2003.

- G29, « Document de travail relatif à une interprétation commune des dispositions de l'article 26, paragraphe 1, de la directive 95/46/EC du 24 octobre 1995 », *WP114*, 25 novembre 2005.

- G29, "Letter from I. FALQUE-PIERROTIN, President of the WP29, to Vice-President REDING", Bruxelles, 10 avril 2014, *Ares(2014)1139376*, http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf

- G29, « Déclaration commune des autorités européennes de protection des données réunies au sein du groupe de l'article 29, *WP227*, 26 novembre 2014.

- G29, « Statement of the Article 29 Working Party on the consequences of the Schrems judgment », *Communiqué de Presse,* 3 février 2016.

- G29, "Opinion n°01/2016 on the EU-U.S. Privacy Shield draft adequacy decision", *WP238,* 13 avril 2016.

- G29, "Lettre ouverte à WhatsApp", 27 octobre 2016, https://www.cnil.fr/sites/default/files/atoms/files/20161027_letter_of_the_chair_of_the_art_29_wp_whatsapp.pdf (consulté le 20 avril 2017)

- G29, "Guidelines on the right to data portability", *WP242*, adoptées le 13 décembre 2016 et révisées le 5 avril 2017.

- G29, "Annex II to the Guidelines on the Right to Data Portability - Frequently asked Questions", *WP242,* 13 décembre 2016.

CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES (CEPD)

- CEPD, "Position Paper - The transfer of personal data to third countries and international organizations by EU institutions and bodies", Bruxelles, 14 juillet 2014.

- CEPD, « Avis n°7/2015 - Relever les défis des données massives : un appel à la transparence, au contrôle par l'utilisateur, à la protection des données dès la conception et à la reddition des comptes », 19 novembre 2015.

- Décision 2016 C 33/01 du contrôleur européen de la protection des données du 3 décembre 2015 instituant un groupe consultatif externe sur les dimensions éthiques de la protection des données (groupe consultatif sur l'éthique), *J.O.U.E.*, C 33/1 du 28 janvier 2016.

- CEPD, « Avis n°4/2016 concernant le 'Bouclier vie privée UE-Etats-Unis (Privacy Shield) Projet d'adéquation », 30 mai 2016.

AUTORITÉS NATIONALES DE PROTECTION DES DONNÉES

- SCHAAR (P.), Federal Commissioner of Data Protection and Freedom of Information (BfDI), « Privacy by design », Berlin, Allemagne, 19 mars 2010, https://link.springer.com/content/pdf/10.1007/s12394-010-0055-x.pdf

- CNIL, « Mesures pour traiter les risques sur les libertés et la vie privée », juin 2012, https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-BonnesPratiques.pdf

- CAVOUKIAN (A.), Information and Privacy Commissioner, « Operationalizing Privacy by Design: a guide to implementing strong privacy practices", Ontario, Canada, décembre 2012, http://www.cil.cnrs.fr/CIL/IMG/pdf/operationalizing-pbd-guide.pdf

- CNDP, « Privacy by Design : le respect de la vie privée dès la conception », Grand-Duché du Luxembourg, 18 mai 2015, https://cnpd.public.lu/fr/dossiers-thematiques/nouvelles-tech-communication/privacy-by-design/ (consulté le 11 juillet 2017).

- BFDI, « Press Release – Administrative order against the mass synchronization of data between Facebook and WhatsApp", Allemagne, 27 septembre 2016, https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Press_Release_2016-09-27_Adminstrative_Order_Facebook_WhatsApp.pdf

- COMMISSION VIE PRIVÉE BELGE, « Réforme de la commission pour la protection de la vie privée », *Communiqué de Presse*, Bruxelles, 13 mai 2017, http://www.presscenter.be/fr/pressrelease/20160513/reforme-de-la-commission-pour-la-protection-de-la-vie-privee (consulté le 20 juillet 2017).

AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE

- AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE, "Data Protection in The European Union: the role of National Data Protection Authorities", *Strenghtening the fundamental rights architecture in the EU II*, 2010.

- AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE, *Report on the access to data protection remedies in EU Member States*, 2013.

- AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE, *Handbook on European data protection law*, 2014.

- AGENCE DES DROITS FONDAMENTAUX DE L'UNION EUROPÉENNE, *Handbook on European law realting to access to justice*, 2016.

❖ JURISPRUDENCE

UNION EUROPÉENNE

- C.J.C.E., C-314/85 *Foto-Frost c. Hauptzollamt Lübeck-Ost*, 22 octobre 1987, ECLI:EU:C:1987:452.
- C.J.C.E., C-101/01 *Bodil Lindqvist*, 6 novembre 2003, ECLI:EU:C:2003:596.
- C.J.C.E., C-344/04 *International Air Transport Association et European Low Fares Airline Association c. Department for transport*, 10 janvier 2006, ECLI:EU:C:2006/10.
- CJUE, C-518/07 *Commission européenne c. République fédérale d'Allemagne*, 9 mars 2010, ECLI:EU:C:2010:125.
- C.J.U.E., C-614/10 *Commission européenne c. République d'Autriche*, 16 octobre 2012, ECLI:EU:C:2012:631.
- C.J.U.E., C-288/12 *Commission européenne c. Hongrie*, 8 avril 2014, ECLI:EU:C:2014:237.
- C.J.U.E, C-293/12 et C-594/12 *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e.a.*, 8 avril 2014, ECLI:EU:C:2014.
- C.J.U.E., C-131/12 *Google Spain SL et Google Inc. C. Agencia Espanola de Proteccion de Datos (AEPD) et Mario Costeja Gonzales*, 13 mai 2014, ECLI:EU:C:2014:317.
- C.J.U.E, C-230/14 *Weltimmo s.r.o. c. Nemzeti Adatvedelmi es Informacioszabadsag Hatosag*, 1er octobre 2015, ECLI:EU:C:2015:639.
- C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 6 octobre 2015, ECLI:EU:C:2015:650.

JURIDICTIONS NATIONALES

- UNITED STATES SUPREME COURT, n°78-5374 *Smith c. Maryland*, 442 U.S. 735, 20 juin 1979.

- HIGH COURT OF IRELAND, n°013/765/JR, *Maximilian Schrems c. Data Protection Commissioner*, 16 juillet 2014.

❖ ***DOCTRINE***

- ALBRECHT (J.-P.), *The EU's Data Protection Reform*, Göttingen, AktivDruck, décembre 2015.
- ALBRECHT (J.-P.), "Privacy Shield – Press Breakfast by MEP Jan Albrecht", Parlement européen, Bruxelles, 12 juillet 2016, p. 2, http://europe-v-facebook.org/PA_PS.pdf
- Av. gén. BOT (Y.), concl. préc. C.J.U.E., C-2015/650 *Maximilian Schrems c. Data Protection Commissioner*, 23 septembre 2015, C-362/14, ECLI:EU:C:2015:650.
- BUTTARELLI (G.), « La vie privée et l'émergence des nouvelles technologies – Le point de vue de l'Union européenne », La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux. Actes du colloque du 17 octobre 2016, Sénat de Belgique, Bruxelles, 2016, pp. 22-26.
- CASSART (A.), « Les données personnelles expédiées aux U.S.A. arriveront-elles un jour à bon port ? », *J.L.M.B.*, n°2017/26, p. 1230-1240.
- CAUCHOIS (R.), « La protection des données personnelles en Europe et la compétitivité des entreprises européennes », *Quelle protection des données personnelles en Europe*, Bruxelles, Larcier, 2015, pp. 155-168.
- COTON (F.), « L''établissement' du responsable de traitement de données, une notion clé », *J.L.M.B.*, 2017/26, p. 1215-1220.
- DEBET (A.), MASSOT (J.) et METALLINOS (N.), *Informatique et libertés – La protection des données à caractère personnel en droit français et européen*, Issy-les-Moulineaux, Lextenso, 2015.
- DEFRAIGNE (C.), « Mot de bienvenue », La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux. Actes du colloque du 17 octobre 2016, Sénat de Belgique, Bruxelles, 2016, pp. 9-12.

- DE HERT (P.) et PAPAKONSTANTINOU (V.), « Three scenarios for international governance of data privacy: towards an international data privacy organization, preferably a UN agency?", *I/S: a journal of Law and Policy for the Information Society*, vol. 9, éd. 2, 2013, pp. 271-324.

- DESFORGES (A.), « Les stratégies européennes dans le cyberespace », *Droits et souveraineté numérique en Europe*, Bruxelles, Bruylant, 2016, pp. 81-90.

- GIRARD (F.), « La notion de vie privée aux Etats-Unis », *Le droit à l'oubli numérique*, Bruxelles, Larcier, 2015, pp. 200-227.

- GROSJEAN (A.), « 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, pp. 197-215.

- GUÉDON (J.-P.), « Renforcement de la protection des données personnelles », *AJ Pénal*, 2016, p. 53.

- GUERGUINOV (O.) et LÉONARD (T.), « GDPR. Droit à la portabilité des données : analyse des lignes directrices du G29 », 28 décembre 2016, https://www.droit-technologie.org/actualites/gdpr-droit-a-portabilite-donnees-analyse-lignes-directrices-g29/ (consulté le 18 juillet 2017).

- HAVELANGE (B.) et LACOSTE (A.-C.), « Les flux transfrontaliers de données à caractère personnel en droit européen », *J.D.E.*, 2001, pp. 241-248.

- HUSTINX (P.), « Introduction. The role of data protection authorities », *Défis du droit à la protection de la vie privée*, sous la coordination de PÉREZ ASINARI (M.-V.) et PALAZZI (P.), Bruylant, 2008, pp. 561-568.

- KINDT (E.), « Vie privée et vie publique en Belgique », La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux. Actes du colloque du 17 octobre 2016, Sénat de Belgique, Bruxelles, 2016, pp. 43-49.

- KRAEMER (H.), « Les nouveaux acteurs dans le domaine des droits fondamentaux de l'Union européenne », *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence.* Sous la dir. de TINIÈRE (R.) et VIAL (C.), Bruxelles, *Bruylant*, 1ère éd., avril 2015, pp. 321-355.

- KROLL (J.), HUEY (J.), BAROCAS (S.), FELTEN (E.), REIDENBERG (J.), ROBINSON (D.) et YU (H.), "Accountable algorithms", *University of Pennsylvania Law Review*, vol. 165, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2765268 (consulté le 7 juillet 2017).

- KUNER (C.), "An international Legal Framework for Data Protection: Issues and Prospects", *Computer Law & Security Review*, vol. 25, 2009.

- KUNER (C.), « The European Commission's proposed data protection regulation: a Copernican revolution in European data protection law", *Bloomberg BNA Privacy and Security Law Report*, 6 février 2012.

- KUNER (C.), "Paper n°48/2015 - The European Union and the Search for an International Data Protection Framework", *Groningen Journal of International Law*, vol. 2, éd. 1: Privacy in international law, août 2015, pp. 55-71.

- KUNER (C.), "Paper n°49/2015 - Extraterritoriality and International Data transfers in EU Data Protection Law", *Legal studies - Research Paper studies*, Cambridge University Press, août 2015.

- KUNER (C.), « Paper n°14/2016 - Reality and illusion in EU Data Transfer Regulation Post Schrems", *Legal studies - Research Paper studies*, Cambridge University Press, mars 2016.

- KUNER (C.), SVANTESSON (B.), CATE (F.), LYNSKEY (O.) et MILLARD (C.), « Machine learning with personal data: is data protection law smart enough to meet the challenge », *International Data Privacy Law*, vol. 7, n° 1, Oxford University Press, 2017.

- LE BAIL (F.), « Protection de la vie privée et des données personnelles : l'Europe à l'avant-garde », *New frontiers of antitrust – 2013*, Bruxelles Bruylant, 2013, pp. 101-109.

- MANNY (C.), « Incomplete privacy : how federal law misses problems connected to the U.S. consumer data base industry », *Défis du droit à la protection de la vie privée – perspectives du droit européen et nord-américain, Cahiers du Centre de Recherches Informatique et Droit*, vol. 31, Bruxelles, Bruylant, 2008, pp. 172-187.

- MAUBERNARD (C.), « Prendre la promotion externe des droits de l'Homme par l'Union européenne 'au sérieux' », *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence*, Sous la dir. de TINIÈRE (R.) et VIAL (C.), Bruxelles, Bruylant, 1ère éd., avril 2015, pp. 295-319.

- MOINY (J.-P.), « Facebook au regard des règles européennes concernant la protection des données », *R.E.D.C.*, 2010/2, p. 235-271.

- NIKOLTCHEV (S.), « Les données à caractère personnel sont-elles vraiment privées ? », *Observatoire européen de l'audiovisuel*, IRIS *plus*, Strasbourg, 2013.

- NIMMER (R.), « Internationally interactive law : perspectives on trans-border data control from the U.S. », *Défis du droit à la protection de la vie privée – Perspectives du droit européen et nord-américain, Cahiers du Centre de Recherches Informatique et Droit*, vol. 31, Bruxelles, Bruylant, 2008, pp. 415-437.

- PEYROU (S.), « La Cour de justice de l'Union européenne, à l'avant-garde de la défense des droits numériques », *J.D.E.*, 2015, pp. 395-398.

- PEYROU (S.), « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la C.J.U.E », *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence*, sous la direction de TINIÈRE (R.) et VIAL (C.), Bruxelles, *Bruylant*, 1ère éd., avril 2015, pp. 213-231.

- POULLET (Y.), « Internet et vie privée : entre risques et espoirs », *J.T.*, 2001, pp. 155-164.

- POULLET (Y.), "Transborder Data Flows and Extraterritoriality: the European Position", *Journal of International Commercial Law and Technology*, 2007, vol. 2, issue n°3, pp. 141-153.

- POULLET (Y.), « Le point de vue de la société sur le sentiment de traçabilité », La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux. Actes du colloque du 17 octobre 2016, Sénat de Belgique, Bruxelles, 2016, pp. 58-66.

- RAAB (C.) et SZEKELY (I.), « Data protection authorities and information technology », *Computer Law & Security Review: The International Journal of Technology Law and Practice*, n° 33, 2017, pp. 1-13.

- RAPAILLE (G.), « La protection de la vie privée dans le domaine de la sécurité et de la vie publique – Terrain et sécurité », La vie privée des citoyens et la protection des données face aux nouvelles technologies : les enjeux. Actes du colloque du 17 octobre 2016, Sénat de Belgique, Bruxelles, 2016, pp. 34-38.

- ROSIER (K.), "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, pp. 61-119.

- ROUVROY (A.) et BERNS (T.), « Gouvernementalité algorithmique et perspectives d'émancipation : le disparate comme condition d'individuation par la relation ? », *Politique des algorithmes. Les métriques du web*, Réseaux, vol. 31, n°177, 2013, pp. 163-196.

- SVANTESSON (B.), "A 'layered approach' to the extraterritoriality of data privacy laws", *International Data Privacy Law*, vol. 3, n° 4, Oxford University Press, octobre 2013, pp. 278-286.

- VAN DER AUWERMEULEN (B.), « How to attribute the right to data portability in Europe: A comparative analysis of legislations", *Computer Law & Security Review: The International Journal of Technology Law and Practice*, n° 33, 2017, pp. 57-72.

- VAN GYSEGHEM (J.-M.), DE TERWAGNE (C.), HERVEG (J.) et GAYREL (C.), « La protection des données à caractère personnel en droit européen », *Journal européen des droits de l'homme*, 2014/1, pp. 55 et s.

- WOLF (C.), "White Paper - Overextended: jurisdiction and applicable law under the EU General Data Protection Regulation", *Future of Privacy Forum*, janvier 2013, https://docslide.net/documents/overextended-jurisdiction-and-applicable-law-under-the-eu-general-data-protection.html (consulté le 23 février 2017).

❖ ***ARTICLES DE PRESSE, LIVRES, ÉTUDES ET INTERVIEWS***

ARTICLES DE PRESSE

- AHMED (M.), « Obama attacks Europe over technology protectionism", *FT*, 16 février 2015, https://www.ft.com/content/41d968d6-b5d2-11e4-b58d-00144feab7de (consulté le 26 juillet 2017).

- BRAHMBHATT (K.), « Privacy by design – is there such a thing as too much?", Londres, 12 avril 2016, http://aodigitalhub.com/2016/04/12/privacy-design-thing-much/ (consulté le 15 juillet 2017).

- TURNER (M.), « This is the future of investing, and you probably can't afford it », 11 novembre 2015, http://www.businessinsider.com/hedge-funds-are-analysing-data-to-get-an-edge-2015-8 (consulté le 20 avril 2017).

- RIBEIRO (J.), "Google, Facebook et Microsoft prêts à soutenir Apple face au FBI », *LeMondeInformatique.fr*, 26 février 2016.

- TUAL (M.), « Facebook cesse d'exploiter les données des utilisateurs européens de WhatsApp », *Le Monde*, 18 novembre 2016, http://www.lemonde.fr/pixels/article/2016/11/17/facebook-cesse-d-exploiter-les-donnees-des-utilisateurs-europeens-de-whatsapp_5032943_4408996.html (consulté le 22 avril 2017).

- THORNHILL (J.), « Data capitalism is cashing in our privacy – for now », *FT*, jeudi 10 janvier 2017, p. 9.

- IWANIUK (J.), « En Pologne, l'Etat de droit n'est plus que théorique », *Le Monde*, 9 février 2017, http://www.lemonde.fr/idees/article/2017/02/09/en-pologne-l-etat-de-droit-n-est-plus-que-theorique_5076989_3232.html (consulté le 20 juillet 2017).

- MURGIA (M.) et CHAZAN (G.), "Germany bans Facebook-WhatsApp sharing", *FT*, mercredi 28 septembre 2016, p. 13.

- MURGIA (M.), « WhatsApp sends clear message over demands for decryption », *FT*, 28 mars 2017, p. 15.

- MURGIA (M.) et TOPLENSKY (R.), « Facebook fined over WhatsApp deal », *FT*, jeudi 18 mai 2017, p. 11.

- MOROZOV (E.), « Trump rouvre le marché des données personnelles », *Le Monde diplomatique*, 31 mars 2017, https://blog.mondediplo.net/2017-03-31-Trump-rouvre-le-marche-des-donnees-personnelles (consulté le 15 avril 2017).

- « Digital privacy is more than just opting in or out », *FT*, samedi 1er avril 2017, p. 8.

- TOPLENSKY (R.), ROBINSON (D.) et MURGIA (M.), "Facebook faces more hurdles after Europe fine", *FT*, 22 mai 2017, p. 9.

- WIGGLESWORTH (R.), « 'Alternative data' sellers fail to remove personal information, say hedge funds », *FT*, lundi 12 décembre 2016, p. 1.

LIVRES

- CHACE (C.), *Surviving AI. The Promise and peril of artificial intelligence, Three Cs Publishing*, 2015.
- GUGAIN (M.) et LABBÉ (C.), *L'Homme Nu. La dictature invisible du numérique*, Robert Laffont, Paris, 2016.
- O'NEIL (C.), "Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy", *Allen Lane*, 2016.

ETUDES

- CONSEIL D'ETAT FRANÇAIS, Etude annuelle 2014 – Le numérique et les droits fondamentaux, France, *EDCE*, n°65, 2014.

INTERVIEWS

- Entretien avec Monsieur Ralf BENDRATH, Conseiller principal en matière de politiques auprès de Jan Philipp Albrecht (Député européen - Groupe Vert/Alliance libre européenne), réalisé au Parlement européen à Bruxelles le 27 novembre 2016 (Annexe I).
- Entretien avec Monsieur Theodosios KOTTAS, stagiaire à l'Agence des droits fondamentaux de l'Union européenne, réalisé à Vienne le 27 juin 2017 (Annexe II).

Table des matières

Plagiat et erreur méthodologique grave

Le plagiat entraîne l'application des articles 87 à 90 du règlement général des études et des examens de l'UCL.

Il y a lieu d'entendre par « plagiat », l'utilisation des idées et énonciations d'un tiers, fussent-elles paraphrasées et quelle qu'en soit l'ampleur, sans que leur source ne soit mentionnée explicitement et distinctement à l'endroit exact de l'utilisation.

La reproduction littérale du passage d'une œuvre, même non soumise à droit d'auteur, requiert que l'extrait soit placé entre guillemets et que la citation soit immédiatement suivie de la référence exacte à la source consultée.*.

En outre, la reproduction littérale de passages d'une œuvre sans les placer entre guillemets, quand bien même l'auteur et la source de cette œuvre seraient mentionnés, constitue une erreur méthodologique grave pouvant entraîner l'échec.

* A ce sujet, voy. notamment **http://www.uclouvain.be/plagiat**.

Place Montesquieu, 2 bte L2.07.01, 1348 Louvain-la-Neuve, Belgique **www.uclouvain.be/drt**