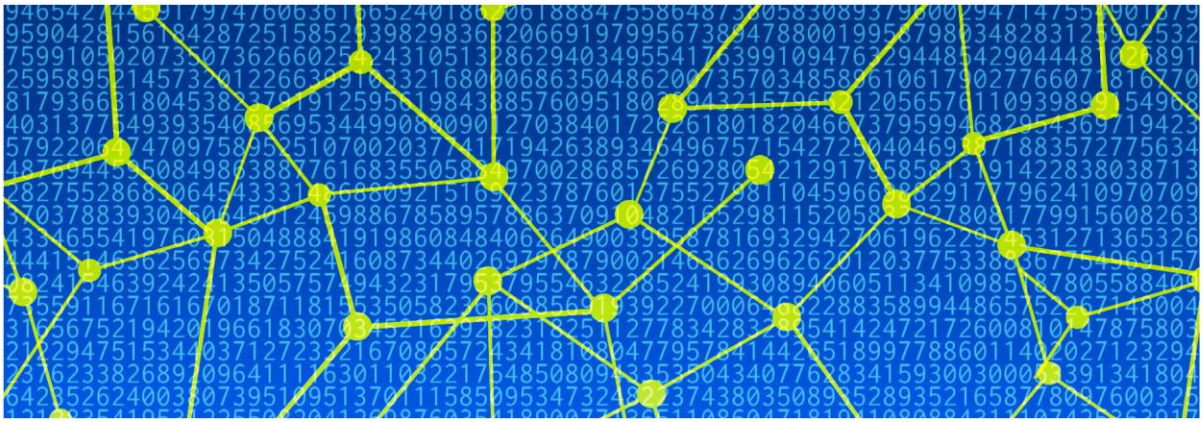

EUROPEAN DATA PROTECTION SUPERVISOR

Avis 4/2016

Avis concernant le «Bouclier vie privée UE-États-Unis» (Privacy Shield) Projet de décision d'adéquation

EDPS

Le 30 mai 2016

Le contrôleur européen de la protection des données (CEPD) est une institution indépendante de l'Union européenne (UE) chargée en vertu de l'article 41, paragraphe 2, du règlement nº 45/2001, «[e]n ce qui concerne le traitement de données à caractère personnel, [...] de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires», et «[...] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel». Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, la Commission a l'obligation, lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel, de consulter le CEPD.

Le CEPD et le contrôleur adjoint ont été nommés en décembre 2014 avec comme mission spécifique d'adopter une approche constructive et proactive. Le CEPD a publié en mars 2015 une stratégie quinquennale exposant la manière dont il entend mettre en œuvre ce mandat et en rendre compte.

Le présent avis se rapporte à la mission de conseil des institutions de l'UE sur les implications de leurs politiques en matière de protection des données et de promotion d'une élaboration responsable des politiques, conformément à l'action nº 9 de la stratégie du CEPD: «Faciliter l'élaboration responsable et éclairée de politiques».

Rapport de synthèse

Les flux de données sont mondiaux. L'UE est liée par les traités et la charte des droits fondamentaux de l'Union européenne, qui protège toutes les personnes sur son territoire. L'UE se doit de prendre toutes les mesures nécessaires pour garantir le respect des droits à la vie privée et à la protection des données à caractère personnel à tous les stades de traitement, y compris lors de transferts.

Depuis les révélations en 2013 d'activités de surveillance, l'UE et son partenaire stratégique, les États-Unis, ont souhaité définir un nouvel ensemble de normes reposant sur un système d'auto-certification, pour le transfert à des fins commerciales aux États-Unis de données à caractère personnel depuis l'UE. Comme les autorités nationales de protection des données de l'UE, le CEPD reconnaît la nécessité de créer, alors que les flux de données sont devenus mondiaux, instantanés et imprévisibles, un cadre juridique durable régissant les transferts commerciaux de données entre l'UE et les États-Unis, qui, ensemble, constituent le plus grand partenariat commercial au monde. Toutefois, ce cadre doit refléter pleinement nos valeurs communes fondées sur les droits démocratiques et individuels, établis en ce qui concerne l'UE par le traité de Lisbonne et la charte des droits fondamentaux, et en ce qui concerne les États-Unis, par la Constitution américaine.

Le projet de «Bouclier vie privée» peut constituer un pas dans la bonne direction mais tel qu'il est actuellement formulé, il ne comprend pas, à notre avis, l'ensemble des garanties nécessaires à la sauvegarde des droits de la personne au respect de la vie privée et à la protection des données de l'UE, ni en ce qui concerne les recours judiciaires. Des améliorations significatives sont nécessaires si la Commission européenne souhaite adopter une décision d'adéquation. En particulier, l'UE devrait obtenir des assurances supplémentaires en termes de nécessité et de proportionnalité au lieu de légitimer l'accès systématique aux données transférées par les autorités américaines sur la base de critères ayant une base juridique dans le pays bénéficiaire mais pas dans l'UE, au regard des traités et des décisions de l'UE et des traditions constitutionnelles communes aux États membres.

En outre, à l'ère de l'hyperconnectivité et de la répartition des réseaux, l'autorégulation par des organismes privés et les engagements pris par des agents publics peuvent jouer un rôle à court terme mais, sur le long terme, ces actions ne seront pas suffisantes pour préserver les droits et les intérêts des personnes et pleinement répondre à leurs besoins à l'heure du tout numérique et alors même que de nombreux pays se sont maintenant dotés de règles pour la protection des données.

Par conséquent, une solution à long terme dans le dialogue transatlantique serait bienvenue et permettrait également de transposer dans la loi fédérale applicable au moins les grands principes qui sous-tendent ces droits, et de les identifier clairement et précisément, comme cela est le cas avec d'autres pays non européens qui ont été «reconnus» (selon des critères stricts) comme assurant un niveau de protection adéquat; dans son arrêt Schrems, la CJUE a qualifié ces principes de«substantiellement équivalents» aux normes applicables en vertu du droit de l'Union, et le groupe de travail «Article 29» (G29) les désigne comme contenant «l'essentiel des principes fondamentaux» relatifs à la protection des données.

Nous notons avec satisfaction la transparence accrue manifestée par les autorités américaines quant à l'utilisation de l'exception aux principes du Bouclier vie privée aux fins de l'application de la loi, de la sécurité nationale et de l'intérêt public.

Cependant, alors que la décision «Sphère de sécurité » (Safe Harbour) de 2000 considérait formellement que l'accès aux données pour des raisons de sécurité nationale devait être une exception, l'attention portée dans le projet de décision sur le Bouclier vie privée aux questions de l'accès, du filtrage et de l'analyse par les instances judiciaires et de renseignement des données à caractère personnel transférées à des fins commerciales indique que l'exception pourrait être devenue la règle. Le CEPD souligne en particulier qu'il ressort du projet de décision et de ses annexes que malgré la tendance récente à remplacer une surveillance générale par une surveillance plus ciblée et reposant sur une approche plus sélective, le nombre des renseignements d'origine électromagnétique (ROEM) et le volume des données transférées depuis l'UE et potentiellement recueillies et utilisées après leur transfert ainsi que pendant leur transit, peuvent demeurer élevés et donc contestables.

Même si ces pratiques peuvent également concerner les services de renseignement d'autres pays, et alors que nous nous félicitons de la transparence des autorités américaines sur cette nouvelle réalité, le projet de décision actuel pourrait légitimer cette tendance. Nous encourageons donc la Commission européenne à donner un signal fort: compte tenu des obligations qui incombent à l'UE dans le cadre du traité de Lisbonne, l'accès et l'utilisation par les pouvoirs publics de données transférées à des fins commerciales, y compris lorsque ces données sont en transit, ne devraient être possibles que dans des circonstances exceptionnelles et lorsque cela est indispensable à des fins d'intérêt public précises.

S'agissant des dispositions relatives aux transferts de données à des fins commerciales, les contrôleurs ne devraient pas avoir à changer constamment les modèles de conformité. Pourtant, le projet de décision est fondé sur le cadre juridique communautaire existant, qui sera remplacé par le règlement (UE) n° 2016/679 (règlement général sur la protection des données) en mai 2018, soit moins d'un an après la mise en œuvre complète du Bouclier vie privée par les contrôleurs. Le RGPD crée et renforce les obligations des contrôleurs, lesquelles se prolongent au-delà des neuf principes établis par le Bouclier vie privée. Même si le projet devait encore être modifié, nous recommandons à la Commission européenne d'évaluer l'ensemble des perspectives par rapport à son premier rapport, d'identifier en temps opportun les mesures pertinentes susceptibles de conduire à des solutions de remplacement à long terme du Bouclier vie privée, le cas échéant par un cadre juridique solide et durable qui permettra de renforcer les relations transatlantiques.

Par conséquent, le CEPD émet des recommandations spécifiques sur le Bouclier vie privée.

TABLE DES MATIÈRES

LE CONTRÔLEUR EUROPÉEN DE LA PROTECTION DES DONNÉES,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 16,

vu la charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8,

vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après «la directive»),

vu la décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale,

vu le règlement (CE) nº 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, et notamment son article 28, paragraphe 2, son article 41, paragraphe 2, et son article 46, point d),

ADOPTE L'AVIS SUIVANT:

I. INTRODUCTION

Le 6 octobre 2015, la Cour de justice de l'Union européenne (ci-après la CJUE) a invalidé [1]la décision sur l'adéquation de la Sphère de sécurité[2]. La Commission européenne a conclu un accord politique avec les États-Unis le 2 février 2016 concernant un nouveau cadre pour les transferts de données à caractère personnel dénommé le «Bouclier vie privée UE-États-Unis» (le Bouclier vie privée). Le 29 février, la Commission européenne a publié un projet de décision sur la pertinence de ce nouveau cadre (ci-après le «projet de décision»)[3] et ses sept annexes, ainsi que les principes de confidentialité du Bouclier vie privée et des observations et engagements écrits émanant des fonctionnaires et des autorités américaines. Le CEPD a reçu le projet de décision pour consultation le 18 mars de cette année.

Le CEPD a exprimé à plusieurs reprises sa position sur les transferts de données à caractère personnel entre l'UE et les États-Unis[4] et a contribué à la rédaction de l'avis du groupe de travail «Article 29» (ci-après «G29») relatif au projet de décision, en tant que membre de ce groupe[5]. Le G29 a exprimé des préoccupations sérieuses et a demandé à la Commission européenne d'identifier des solutions pour y remédier. Les membres du G29 attendent une réponse aux demandes d'explications exprimées dans l'avis[6]. Le 16 mars, 27 organisations à but non lucratif ont exprimé des critiques concernant le projet de décision dans une lettre adressée aux autorités de l'UE et aux autorités américaines[7]. Le 26 mai, le Parlement européen a adopté une résolution sur les flux de données transatlantiques[8] qui appelle la Commission à négocier avec l'administration américaine des améliorations supplémentaires des dispositions du Bouclier vie privée, afin de remédier à ses lacunes actuelles[9].

En tant que conseiller indépendant des législateurs de l'UE, conformément au règlement (CE) n° 45/2001, le CEPD publie maintenant des recommandations adressées aux parties impliquées dans le processus, en particulier la Commission. Le présent avis du CEPD se veut

à la fois fondé sur des principes et pragmatique, afin d'aider de manière proactive l'UE à atteindre ses objectifs par la mise en œuvre de mesures adéquates. Il complète et souligne certaines recommandations figurant dans l'avis du G29.

Le projet de décision met en évidence un certain nombre d'améliorations par rapport à la décision Sphère de sécurité, en particulier en ce qui concerne les principes relatifs au traitement de données à des fins commerciales. En ce qui concerne l'accès par les pouvoirs publics aux données transférées dans le cadre du Bouclier vie privée, nous nous félicitons également de la participation, pour la première fois, du ministère de la Justice, du Département d'État (affaires étrangères) et du Bureau du directeur des services nationaux de renseignement aux négociations. Cependant, les progrès accomplis au regard de la précédente décision Sphère de sécurité ne sont pas suffisants. La référence correcte ne doit pas être une décision précédemment invalidée car la décision d'adéquation doit reposer sur le cadre juridique actuel de l'UE (en particulier, la directive elle-même, l'article 16 du traité sur le fonctionnement de l'Union européenne et les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne, tels qu'interprétés par la CJUE). L'article 45 du règlement général de l'UE sur la protection des données (ci-après le RGPD)[10] fournira de nouvelles exigences pour les transferts de données, sur la base de la décision d'adéquation.

L'an dernier, la CJUE a affirmé que le seuil d'évaluation de l'adéquation est l'«équivalence substantielle», et elle a exigé une évaluation stricte, conforme à ce niveau d'exigence élevé[11]. Il n'est pas nécessaire pour obtenir l'adéquation d'adopter un cadre identique à celui qui existe déjà dans l'UE, mais conjointement, le Bouclier vie privée et la législation américaine devraient couvrir tous les éléments clés du cadre de protection des données de l'UE. Cela exige à la fois une évaluation globale de la législation et l'examen des éléments les plus importants du cadre de protection des données de l'UE[12]. Nous supposons que l'évaluation doit être effectuée de manière globale, tout en respectant l'essence de ces éléments. En outre, afin de respecter les dispositions du traité et de la charte, des éléments spécifiques, tels que le contrôle indépendant et les voies de recours, devront être pris en considération.

À cet égard, le CEPD est conscient que de nombreuses organisations des deux côtés de l'Atlantique attendent les conclusions relatives à cette décision d'adéquation. Cependant, les conséquences d'une nouvelle invalidation par la CJUE, résultant d'un constat d'insécurité juridique pour les personnes concernées et d'une charge trop élevée pour les PME, pourraient être graves. En outre, si le projet de décision est adopté puis invalidé par la CJUE, tout nouvel accord d'adéquation devra, cette fois, être négocié dans le cadre du RGPD. Nous recommandons donc une approche tournée vers l'avenir puisque le RGPD doit entrer en vigueur dans les deux années à venir.

Du point de vue des relations UE-États-Unis, soumises à des négociations sur le commerce et l'investissement, le projet de décision joue un rôle très important. En outre, un grand nombre des éléments pris en compte dans notre avis concernent indirectement le Bouclier vie privée et d'autres instruments de transfert, tels que les règles d'entreprise contraignantes (ci-après les «REC») et les clauses contractuelles standard (ci-après les «CCS»). Il revêt également une importance à l'échelle internationale étant donné que de nombreux pays tiers suivront l'affaire de près dans le contexte de l'adoption du nouveau cadre de protection des données de l'UE.

Par conséquent, nous accueillerions favorablement une solution générale pour les transferts de données UE-États-Unis, à condition que cette solution présente les garanties suffisantes en

terme d'exhaustivité et de pérennité. Pour cela, des améliorations importantes doivent être apportées au projet afin d'assurer le respect durable de nos droits et libertés fondamentaux. Si la décision est entérinée, la Commission européenne devra l'examiner rapidement afin d'identifier des mesures pertinentes permettant la mise en place de solutions à long terme de remplacement du Bouclier vie privée par un cadre juridique solide et durable, capable de renforcer les relations transatlantiques.

Le CEPD note également qu'il ressort du projet de décision et de ses annexes que malgré la tendance récente tendant à passer d'une surveillance massive et générale à des approches plus ciblées et sélectives, le volume des renseignements d'origine électromagnétique (ROEM) et des données transférées depuis l'UE pouvant être recueillis après le transfert et notamment pendant le transit, est susceptible d'être encore élevé et donc discutable.

Même si ces pratiques peuvent également concerner les services de renseignement d'autres pays, et alors que nous nous félicitons de la transparence des autorités américaines sur cette nouvelle réalité, le projet de décision actuel pourrait être interprété comme légitimant cette tendance. La question exige un contrôle démocratique public sérieux. Nous encourageons donc la Commission européenne à donner un signal fort: compte tenu des obligations qui incombent à l'UE dans le cadre du traité de Lisbonne, l'accès et l'utilisation par les pouvoirs publics de données transférées à des fins commerciales, y compris lorsque ces données sont en transit, ne devraient être possibles que dans des circonstances exceptionnelles et lorsque cela est indispensable pour servir un intérêt public précis.

De plus, nous notons que les garanties essentielles et pertinentes du respect de la vie privée des personnes dans l'UE semblent être élaborées de manière précise uniquement dans des documents internes des autorités américaines (tels que les déclarations concernant les activités de collecte de ROEM sur les câbles transatlantiques, le cas échéant)[13]. Même si nous ne remettons pas en question l'autorité des auteurs de ces documents et comprenons qu'une fois publiées au Journal officiel et dans le Registre fédéral, ces garanties seront considérées comme des «assurances écrites» sur la base desquelles l'UE pourra fonder son évaluation, nous notons également que, d'une manière générale, certaines garanties mériteraient que leur soit accordée une plus grande valeur juridique.

Outre des changements législatifs et des accords internationaux[14], d'autres solutions pratiques pourraient être explorées. Notre avis vise à fournir des conseils pragmatiques à cet égard.

II. PRINCIPALES RECOMMANDATIONS

1. Intégrer tous les principes importants en matière de protection des données

Le projet de décision indique que le Bouclier vie privée, dans son ensemble, assure un niveau de protection substantiellement équivalent à celui garanti par les principes de base de la directive[15]. Toutefois, le projet actuel omet des points essentiels de certains de ces principes, notamment en ce qui concerne la **conservation des données** et le **traitement automatisé des données**. D'autres éléments essentiels tels que le principe de **limitation des finalités**, devraient être mieux précisés. Les **dérogations** aux exigences du Bouclier vie privée doivent également être affinées. Le projet de décision n'explique pas complètement comment, même s'ils sont appliqués dans leur ensemble, le Bouclier vie privée et la législation américaine pourront combler ces lacunes. Ainsi qu'indiqué ci-dessus, le Bouclier vie privée devrait donc

être modifié pour mieux intégrer les principaux principes de protection des données de l'UE[16], ainsi que cela sera exposé plus en détail dans la section III.1 du présent Avis. En outre, les dispositions relatives aux **transferts ultérieurs**, au **droit d'accès** et au **droit de s'opposer** devraient être améliorées. Le CEPD souhaite souligner les recommandations du G29 à cet égard.

2. Limiter les dérogations

Conformément à l'annexe II.I.5 (a), les principes du Bouclier vie privée peuvent être limités dans la mesure nécessaire pour répondre aux exigences de sécurité nationale, d'application de la loi ou à toute autre exigence d'intérêt public. L'annexe II.I.5 (b) permet également de limiter ces principes si «des textes législatifs, des règlements administratifs ou des décisions jurisprudentielles créent des obligations contradictoires ou prévoient des autorisations explicites», sans aucune restriction quant aux fins d'un tel accès. **Les raisons justifiant les dérogations et l'exigence d'une base légale devraient être plus précis**[(points a) et b)]. Le CEPD souligne que l'une des raisons de l'invalidation de la décision Sphère de sécurité[17] était l'absence de conclusions concernant la limitation de l'ingérence des autorités américaines dans les droits des personnes concernées par un transfert de données depuis l'UE. La Cour a également demandé des règles claires et précises limitant la portée et l'application de toute ingérence dans les droits fondamentaux[18]. **Pour les mêmes raisons, l'annexe II.I.5 c) devrait préciser les finalités justifiant une dérogation ou être supprimée**.

Le CEPD accueille favorablement les efforts de transparence dans les informations fournies par le Bureau central du renseignement sur l'accès aux données par les autorités américaines[19]. Le CEPD note également des indications importantes dans la Directive de politique présidentielle 28 (ci-après: «DPP 28») contre la collecte massive. Cependant, la DPP 28 permet le traitement ultérieur de données recueillies «en masse» afin de «faciliter la collecte ciblée» et pour au moins six autres motifs. En outre, alors que le projet de décision indique que les ROEM peuvent être collectés exclusivement à des fins de renseignement ou de contre-espionnage étranger, le terme «renseignement étranger» est défini au sens large[20]. [21]De plus, cela semble indiquer que les conditions d'accès des autorités américaines aux données à caractère personnel «transférées»[22] sont différentes de celles qui régissent l'accès aux données à caractère personnel «susceptibles de transfert». Nous recommandons de nuancer le considérant 55 du projet de décision qui stipule que les restrictions sur l'accès et l'utilisation des données à caractère personnel transférées depuis l'UE vers les États-Unis à des fins de sécurité nationale sont «claires»[23].

Bien que la DPP 28 constitue une évolution positive, il reste à voir comment certaines **modifications politiques et législatives**, par exemple en ce qui concerne l'ordonnance de l'exécutif n° 12333, **pourraient permettre de satisfaire aux exigences d'adéquation**. L'examen en 2017 de l'article 702 de la FISA (Loi sur la surveillance et le renseignement étranger), qui ne semble pas actuellement exiger du gouvernement qu'il identifie des cibles particulières ou qu'il fournisse au Tribunal de surveillance du renseignement extérieur une justification pour le ciblage individuel[24], pourrait également constituer une opportunité à cet égard.

3. Améliorer les mécanismes de recours et de contrôle

Comme indiqué par le G29, il conviendrait, afin d'améliorer le mécanisme de recours proposé dans le domaine de la sécurité nationale, de renforcer également le rôle du **médiateur**, en lui permettant d'agir **de manière indépendante**, non seulement vis-à-vis de la communauté du renseignement mais également vis-à-vis de toute autre autorité[25]. En termes concrets, la possibilité que le médiateur soit en contact direct avec le Congrès pourrait être une option.

Nous recommandons que la Commission européenne obtienne des garanties plus **précises quant au respect et à la mise en œuvre effective des demandes d'information et de coopération du médiateur et de ses propres décisions et recommandations par tous les organismes et organes compétents**. Tout autre engagement des autorités américaines assurant une **coopération accrue entre les différentes instances de contrôle** serait également bienvenu. Les organes de contrôle appropriés, en particulier les inspecteurs généraux concernés, pourraient s'engager à accorder une priorité à la coordination avec le médiateur. Son analyse individuelle des plaintes permettrait de mieux prendre en compte l'évaluation permanente par le Privacy and Civil Liberties Oversight Board des bases juridiques américaines relatives au renseignement, et les recommandations de celui-ci.

Le CEPD note que ces organismes ont pour rôle de veiller au respect des lois, des règles et de la jurisprudence américaines, ce qui conduit à un niveau de protection différencié entre les ressortissants américains et les non ressortissants, et légitime le traitement de données par les autorités américaines; cela ne semble pas être «substantiellement équivalent» aux dérogations prévues par le cadre de l'UE en matière de protection des données[26]. Nous encourageons la Commission européenne à étudier la possibilité de **faire participer les représentants de l'UE a) à l'évaluation des résultats du système de contrôle** concernant le traitement par les autorités américaines de données à caractère personnel transférées depuis l'UE et **b) à la notification de certaines catégories des données à caractère personnel faisant l'objet d'un traitement** par les autorités américaines, en particulier lorsque ce traitement peut soulever des préoccupations relatives aux droits fondamentaux. Cette participation pourrait même prendre la forme d'un panel constitué de représentants externes de haut niveau et de confiance appartenant à une ou plusieurs commissions parlementaires de l'UE, à des organismes nationaux de contrôle du renseignement, à des hautes juridictions européennes ou nationales ou à des autorités chargées de la protection des données (ci-après «APD»).

Les solutions proposées par la Commission dans le cadre de l'accord UE-États-Unis sur le traitement et le transfert de données de messagerie financière (ci-après «le TFTP») ont créé un précédent, notamment en ce qui concerne la nécessité d'obtenir l'**autorisation d'une autorité judiciaire** pour répondre à certaines demandes des autorités américaines[27]. L'accord TFTP initial prévoyait également le **contrôle par un juge de l'UE** du traitement ultérieur de données[28]. Actuellement, **les APD** de l'UE participent également au contrôle du traitement réservé aux demandes américaines[29]. Des exemples utiles peuvent également être observés dans certains États membres de l'UE où les activités nationales de renseignement sont soumises à la compétence d'une APD[30]. À cet égard, la **notification des catégories de données à caractère personnel devant être traitées** par les autorités américaines à un panel incluant une autorité indépendante de l'UE, en particulier lorsque le traitement peut soulever des préoccupations au regard des normes de l'UE en la matière, pourrait aider à atténuer les préoccupations.

III. RECOMMANDATIONS COMPLÉMENTAIRES

1. Dispositions relatives aux transferts à des fins commerciales

Intégrer pleinement les principes de minimisation et de conservation des données

Le CEPD recommande de modifier l'annexe II afin d'interdire plus clairement **la conservation des données à caractère personnel sous une forme permettant l'identification des personnes concernées pendant plus longtemps que nécessaire** aux fins pour lesquelles les données ont été collectées ou traitées ultérieurement. Cette obligation, qui constitue un principe essentiel du droit de la protection des données en évitant un traitement plus long que nécessaire, appelle à l'établissement d'une politique de conservation des données par des organismes autorisés[31].

L'annexe II.II.5 du projet de décision précise que «les informations à caractère personnel doivent être limitées aux informations qui sont *pertinentes* aux fins du traitement». Le CEPD recommande, conformément au principe de minimisation des données, d'ajouter une exigence selon laquelle **les informations à caractère personnel doivent être *adéquates et proportionnelles*** ou ***limitées aux informations nécessaires* aux fins pour lesquelles elles sont collectées et/ou traitées ultérieurement**[32].

Nouvelles garanties concernant le traitement automatisé

Un principe devrait être ajouté à l'annexe II pour prévoir des mesures de sauvegarde des intérêts légitimes des individus faisant l'objet d'une décision produisant des effets juridiques qui les concernent ou les affectent significativement et qui est **basée uniquement sur un traitement automatisé de données** destiné à évaluer certains traits de leur personnalité tels que leur performance au travail, leur solvabilité, leur fiabilité, leur conduite, etc. Il serait envisageable d'inclure dans ces garanties la possibilité d'une intervention humaine du contrôleur, afin de permettre aux personnes concernées d'exprimer leur point de vue ou de contester la décision en question, et d'obtenir des informations sur la logique qui sous-tend le traitement. L'article 15 de l'accord-cadre pourrait également s'avérer utile[33].

Clarifier le principe de limitation des finalités

Ainsi que l'a souligné le G29, certains termes récurrent du projet de décision tels que «différentes finalités», «finalités sensiblement différentes» ou «utilisation non conforme», ne sont pas clairs et pourraient être source de malentendus[34]. Le CEPD recommande **de rationaliser les concepts afférents à la notion de «finalité»**. Le terme «finalité non conforme» devrait être privilégié dans l'ensemble du document. Il convient de préciser que dans tous les cas, les finalités «sensiblement différentes» justifiant le traitement ultérieur des données doivent être compatibles avec les finalités justifiant la collecte initiale des dites données.

En outre l'utilisation **à des fins de marketing** de données à caractère personnel initialement traitées à des fins de recherche médicale ou pharmaceutique ou dans le cadre des ressources humaines, ne doit en aucun cas être considérée comme étant compatible avec la finalité initiale. Par conséquent, les références à cette possibilité dans les principes supplémentaires 9 b) (i) et 14 b) (i) devraient être supprimées.

Exceptions à la limitation

En raison des nombreuses exceptions aux principes établis par le Bouclier vie privée[35], il peut être difficile pour les organisations, les personnes et les APD concernées de déterminer si certains types de traitement sont couverts. Cela est particulièrement important car les transferts commerciaux non couverts par le projet de décision devront être couverts par d'autres instruments (par exemple REC, CCS). La portée de ces exceptions devrait donc être clairement indiquée dans le projet de décision, afin de garantir la sécurité juridique. En outre, certaines de ces exceptions pourraient être problématiques si elles **contredisaient les principales exigences de la législation de l'UE en matière de protection des données**.

Cela vaut également pour le **«matériel journalistique»**»[36], qui est complètement exclu des exigences posées par les principes de confidentialité du Bouclier vie privée. Cependant, le droit à la liberté d'expression et les droits à la vie privée et à la protection des données doivent être conciliés conformément à la Charte et conformément à la Directive telle qu'interprétée par la CJUE, en particulier dans les[37]arrêts Google Espagne[38] et Satamedia[39]. Nous recommandons donc de ne remplacer cette exemption générale par des dérogations particulières à certaines exigences[40] que si ces dérogations sont nécessaires pour concilier les droits à la vie privée et à la protection des données avec les règles régissant la liberté d'expression, et sous réserve que le «matériel journalistique» soit effectivement utilisé à des fins journalistiques.

Améliorer les mécanismes de recours et de contrôle

En ce qui concerne le contrôle des transferts à des fins commerciales, en dépit de certains changements positifs, nous **recommandons que les autorités américaines continuent de vérifier de manière systématique et efficace le respect des principes de confidentialité du Bouclier vie privée**. Ainsi par exemple, le projet de décision pourrait être complété afin de mettre en évidence la façon dont les organismes auto-certifiés chargés du contrôle du respect des principes du Bouclier vie privée réalisent leurs visites ou leurs inspections des locaux[41]. S'agissant des «opérations des panels des APD»[42], le texte devrait être plus précis en ce qui concerne le fonctionnement à venir de ces panels par rapport à celui du panel établi dans le cadre de la Sphère de sécurité. Nous supposons que les éléments positifs des expériences antérieures pourront être conservés. À la lueur des développements récents en matière de mise en œuvre aux États-Unis, nous recommandons également de clarifier les rôles respectifs de la FCC et du FTC concernant les fournisseurs de services Internet à large bande.

Le projet de décision devrait également évaluer les moyens effectivement donnés aux personnes dont les données ont été transférées dans le cadre du Bouclier vie privée pour entamer des procédures devant les tribunaux américains. La volonté d'offrir des mécanismes de recours efficaces aux particuliers, démontrée par la diversité des voies de recours au niveau fédéral et au niveau de l'État, est néanmoins amoindrie par la complexité du système. Afin de faciliter la possibilité de présenter un recours indépendant, et en tenant compte de la complexité des mécanismes proposés, nous recommandons d'améliorer le système en encourageant la possibilité pour les organismes certifiés qui le souhaitent, dans la mesure où ils traitent les données transférées conformément aux dispositions du Bouclier vie privée, d'être **soumis au contrôle des APD,** ce qui leur permettrait de bénéficier de l'expertise de ces dernières en matière de traitement des données à caractère personnel. À cet égard, le G29 a également recommandé que les politiques de protection de la vie privée incluent la

possibilité pour les citoyens de l'UE d'intenter des poursuites en dommages et intérêts dans l'UE[43].

2. Recommandations concernant l'accès des autorités américaines

Le projet de décision indique que dans l'ensemble, les mécanismes de contrôle et de recours prévoient des moyens légaux permettant aux personnes concernées d'avoir accès à leurs données à caractère personnel et d'en demander la rectification ou la suppression[44]. Toutefois, le projet de décision n'évalue pas pleinement les possibilités offertes aux individus d'exercer leurs **droits d'accès, de rectification et de suppression** des données recueillies ou consultées par les pouvoirs publics **à des fins autres que la sécurité nationale** (par exemple dans le cadre de l'application de la loi ou à d'autres fins d'«intérêt public»[45]. Ce point de la décision doit donc être clarifié. À cet égard, le CEPD note que la loi Judicial Redress Act récemment adoptée s'applique[46] uniquement aux «enregistrements» directement transférés par des entités publiques ou privées des pays couverts (de l'UE) aux autorité publiques américaines[47]. En sont donc exclues les données à caractère personnel transférées par des entités privées soumises au Bouclier vie privée et ensuite demandées ou consultées par les autorités américaines.

Le CEPD note que même si plusieurs niveaux de contrôle et de recours sont disponibles aux États-Unis, pris dans leur ensemble, ces mécanismes ne semblent pas couvrir de manière adéquate tous les cas où le gouvernement peut accéder à des données à caractère personnel. En outre, en vertu de la Constitution, des lois et des règlements en vigueur aux États-Unis, les personnes qui ne sont pas de nationalité américaine ne bénéficient pas toujours des mêmes droits que les personnes de nationalité américaine. La pertinence réelle de ces mécanismes de contrôle et de recours pour le Bouclier vie privée est donc limitée. Des**garanties supplémentaires pour un contrôle et des recours indépendants** sont donc nécessaires en cas d'accès aux données à des fins d'application de la loi et à d'autres fins d'intérêt public.

3. Évaluation de l'impact des autres lois et règlements pertinents

Toutes les règles applicables aux données transférées de l'UE vers les États-Unis dans le cadre du projet de décision devraient être évaluées à la lueur des nombreuses exceptions à l'application des principes du Bouclier vie privée concernant le traitement de données à des fins commerciales, ou lorsque d'autres règles peuvent interférer avec ces principes. Cette évaluation devrait inclure les **lois américaines fédérales et centrales** régissant**l'accès aux données à des fins d'intérêt public** autres que la sécurité nationale et l'application de la loi, ainsi que les autres lois et règlements ayant une incidence sur la protection des données à caractère personnel[48]. L'évaluation devrait aussi tenir compte des **engagements internationaux** pertinents à cet égard, notamment les engagements qui autorisent les pouvoirs publics à accéder aux données à caractère personnel initialement traitées à des fins commerciales, ou le transfert de telles données

4. Un examen sérieux

Comme l'exige le G29, l'examen conjoint de l'application du Bouclier vie privée ne doit pas seulement reposer sur des réunions avec des entités publiques et privées, mais aussi sur des **contrôle sur site**. L'examen ne devrait pas être limité à la partie commerciale du projet de décision, mais devrait également couvrir **l'accès des autorités américaines aux données**

transférées dans le cadre du Bouclier vie privée. Ceci devrait être précisé dans le projet de décision. Le projet de décision devrait également mentionner que les **conclusions et les résultats, à tout le moins celles des ADP de l'UE, doivent figurer dans le rapport** de l'examen conjoint.

5. Interactions avec le RGPD

Comme cela est indiqué précédemment, toute solution durable concernant les transferts de données entre l'UE et les États-Unis doit prendre en compte le nouveau cadre de la protection des données de l'UE. Cela est essentiel pour assurer un niveau suffisant de protection et de sécurité juridique des grands principes du cadre de protection des données de l'UE , non seulement à court terme mais aussi à moyen et à long terme. En particulier, le projet de décision devrait prendre en considération les nouveaux éléments du RGPD qui ne sont pas présents dans la directive tels que les principes de **vie privée dès la conception, vie privée par défaut, portabilité des données.** Le CEPD note que le RGPD fournit également des critères plus clairs et plus détaillés en ce qui concerne les décisions d'adéquation, y compris l'existence et le fonctionnement efficace **d'autorités de contrôle indépendantes** dans le pays tiers en question[49].

Enfin, le RGPD modifie le champ d'application du cadre de protection des données de l'UE. Les contrôleurs ou les sous-traitants qui ne sont pas établis dans l'UE seront soumis aux règles de l'UE aussi longtemps que leurs activités de traitement seront liées à la vente de produits ou de services à des particuliers dans l'UE, ou à l'étude du comportement de ces 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'UE dès lors que ces organismes entrent dans le champ d'application modifié du cadre. Dans ce cas, le cadre juridique de l'UE prévaudra sur les principes du Bouclier vie privée et les organismes concernés seront tenus de se conformer précisément au RGPD.

IV. CONCLUSION

Le CEPD salue les efforts accomplis par les parties pour apporter une solution aux problèmes relatifs aux transferts de données à caractère personnel à des fins commerciales de l'UE vers les États-Unis dans le cadre d'un système d'auto-certification. Cependant, des améliorations importantes sont nécessaires pour parvenir à un cadre solide et fiable sur le long terme.

Bruxelles, le 30 mai 2016

(signature)

Giovanni BUTTARELLI

Contrôleur européen de la protection des données

[1] Arrêt C-362/14, Maximillian Schrems / Data Protection Commissioner, 6 octobre 2015 (ci-après «*arrêt Schrems*»).
[2] Décision 2000/520/CE de la Commission du 26 juillet 2000 conforme à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique [notifiée sous le numéro C(2000) 2441] (JO 2000 L 215, p. 7).
[3] Décision d'exécution de la Commission du XXX, conforme à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes du Bouclier vie privée UE-États-Unis, disponible ici: http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf.
[4] Voir l'avis du Contrôleur européen de la protection des données sur la communication de la Commission au Parlement européen et au Conseil relative au «rétablissement de la confiance dans les flux de données entre l'Union européenne et les États-Unis» et sur la 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 européenne et des entreprises établies sur son territoire», du 20 février 2014, et le discours du CEPD lors de son audition devant la CJUE dans l'affaire *Schrems* disponible ici: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2015/15-03-24_EDPS_Pleading_Schrems_vs_Data_Commissioner_EN.pdf).
[5] Avis 01/2016 du G29 relatif à l'adéquation de la décision relative au Bouclier vie privée UE-États-Unis (WP 238), disponible ici: http://ec.europa.eu/jus.tice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf.
[6] Voir l'exposé liminaire du commissaire britannique à l'information, Christopher Graham, lors de la conférence IAPP, Europe Data Protection Intensive 2016 de Londres. Discours disponible (en vidéo) ici: https://iapp.org/news/video/iapp-europe-data-protection-intensive-2016-christopher-graham-keynote/.
[7] Lettre signée par Access Now et 26 autres ONG adressée au G29 et à d'autres institutions.
[8] Résolution du Parlement européen du 26 mai 2016 sur les flux de données transatlantiques [2016/2727(RSP)].
[9] *Idem*, paragraphe 14.
[10] Règlement (UE) 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 - «RGPD»).
[11] Arrêt *Schrems*, points 71, 73, 74 et 96.
[12] Cette approche a déjà été prise en considération dans l'un des premiers articles du G29 sur les transferts de données (GWP12: «Document de travail concernant les transferts de données à caractère personnel vers des pays tiers: application des articles 25 et 26 de la directive de l'UE relative à la protection des données», 24 juillet 1998).
[13] Voir, par exemple, les précisions figurant à l'annexe VI.1. a) que la directive de politique présidentielle 28 (PPD28) prévoit d'appliquer aux données collectées à partir des câbles transatlantiques par la communauté du renseignement américain.
[14] Lors d'une audience devant la CJUE, qui s'est tenue dans le cadre de l'affaire *Schrems*, le CEPD a déclaré que «*La seule solution efficace serait de négocier un accord international prévoyant une protection adéquate contre la surveillance non ciblée, et des obligations en matière de contrôle, de transparence, de recours et de protection des données*». Discours du CEPD lors de l'audience du 24 mars 2015 devant la Cour de justice dans l'affaire Schrems/Data Protection Commissioner (C-362/14).
[15] Projet de décision, considérant 49.
[16] Dans l'arrêt *Schrems*, la Cour a considéré que l'article 1 de la décision de la Commission relative à la sphère de sécurité n'est pas conforme aux exigences de la Directive et qu'il n'est donc pas valable (voir le point 98). Elle n'a par conséquent pas examiné le contenu des principes de la sphère de sécurité. Elle a toutefois déclaré que la Directive vise à assurer non seulement une protection efficace et complète des droits et des libertés fondamentaux mais également un niveau élevé de protection de ces droits et libertés. L'objectif de l'article 25, paragraphe 6, de la Directive, est d'assurer la continuité de ce niveau de protection élevé pour les transferts de données à caractère personnel vers des pays tiers (point 72). L'expression «niveau de protection adéquat» doit être comprise comme exigeant un niveau de protection «substantiellement équivalent» à celui garanti au sein de l'Union en vertu de la directive 95/46 lue à la lumière de la Charte. À défaut d'une telle exigence, l'objectif mentionné au point précédent serait méconnu et le niveau élevé de protection garanti par la Directive pourrait facilement être contourné par des transferts de données à caractère personnel depuis l'Union vers des pays tiers (point 73). Même si les moyens utilisés par un pays tiers peuvent être différents de ceux utilisés dans l'UE [par exemple, un système d'auto-certification (point 80), ils doivent être efficaces pour garantir cette protection substantiellement équivalente (point 74). En conséquence, il convient de procéder à un contrôle strict tenant compte, d'une part, du rôle important que joue la protection des données à caractère personnel pour la protection

du droit fondamental au respect de la vie privée et, d'autre part, du nombre important de personnes dont les droits fondamentaux sont susceptibles d'être violés (point 78). Ainsi, ce sont tous les éléments essentiels de la Directive qui doivent être pris en considération.

[17] Arrêt *Schrems*, points 88.

[18] Dans l'arrêt *Schrems*, la CJUE a demandé que soient établies des règles claires et précises régissant la portée et l'application de toute ingérence dans les droits fondamentaux des personnes dont les données à caractère personnel sont ou pourraient être transférées depuis l'Union vers les États-Unis (point 81). Ces règles, qui devraient également comprendre des garanties contre les abus, sont d'autant plus importantes lorsque les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données (point 91). Voir également l'arrêt Digital Rights Ireland Ltd./Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, et Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl et al., CJUE, 8 avril 2014, affaires jointes C-293/12 et C-594/12, points 54-55). En outre, cette réglementation doit être fondée sur des critères objectifs permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence (*arrêt Schrems*, point 93).

[19] Projet de décision, Annexe VI.

[20] L'annexe VI du projet de décision comprend non seulement «des informations relatives aux moyens, aux intentions et aux activités des gouvernements étrangers ou d'éléments de ceux-ci » et relatives aux « terroristes internationaux », mais aussi des informations relatives à des «organisations étrangères» et des «personnes étrangères» (DPP 28: Activités ROEM (DPP-28, 17 janvier 2014, note de bas de page 2).

[21] Projet de décision, considérant 67.

[22] Projet de décision, considérant 65.

[23] Projet de décision, considérant 55.

[24] Rapport du Privacy and Civil Liberties Oversight Board (Conseil de surveillance de la vie privée et des libertés civiles) sur le programme de surveillance conduit conformément à l'article 702 de la FISA, 2 juillet 2014, p. 106.

[25] Projet de décision, considérants 53 et 104.

[26] Selon la Commission, la portée des programmes américains de renseignement, combinée avec le traitement différencié des citoyens de l'UE, remet en question le niveau de protection assuré par la Sphère de sécurité (*Communication de la Commission au Parlement européen et au Conseil: rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique* [COM(2013) 846 final], p. 4). En ce qui concerne les différences significatives entre les garanties applicables aux ressortissants américains par rapport à garanties applicables aux non ressortissants, voir également le *Rapport sur les conclusions des co-présidents du groupe de travail ad-hoc UE-États-Unis sur la protection des données* du 27 novembre 2013, p. 17

[27] Voir le communiqué de presse de la Commission européenne sur l'adoption d'un projet de mandat pour entamer, avec le gouvernement des États-Unis, des négociations sur les transferts de données bancaires, dans le cadre du programme de surveillance du financement du terrorisme, du 24 mars 2010. Dans le texte final de l'accord, l'autorisation judiciaire a été remplacée par une autorisation d'Europol, conformément à l'article 4 de l'accord Union européenne-États-Unis sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (JO L. 195/5).

[28] Voir les «engagements TFTP» sur le traitement par le département du Trésor des États-Unis, aux fins de la lutte contre le terrorisme, de données à caractère personnel provenant de l'UE (SWIFT - JO 2007, C 166/09), qui ont permis à l'UE de désigner une «personnalité européenne éminente» chargée de vérifier si les États-Unis respectent leurs engagements. En 2008, la Commission européenne a désigné le juge Bruguière «personnalité éminente » (communiqué de presse de la Commission européenne: *Examen par l'UE du «Programme de surveillance du financement du terrorisme» des États-Unis* , PI/08/400, du 7 Mars 2008).

[29] Conformément à sa mission de supervision, l'autorité de contrôle commune d'Europol, composée de représentants de chaque autorité nationale de protection des données de l'UE, suit les réponses d'Europol aux demandes de données à caractère personnel émanant des États-Unis dans le cadre de l'accord TFTP. En outre, les autorités nationales de protection des données de l'UE participent à l'examen conjoint de l'accord, conformément à l'article 13 de l'accord entre l'Union européenne et les États-Unis sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme (JO L. 195/5).

[30] Voir les garanties de protection des données à caractère personnel, «Résumé des principales activités de l'APD italienne en 2013», point 1.1, disponible ici: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3205017 (en anglais) et le communiqué de presse (en italien), «Sicurezza dati personali: Protocollo d'intenti tra l'Autorità Garante e il Direttore Generale del Dis», 11 novembre 2013,

disponible ici: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/2746204. Voir également le document de l'Agence des droits fondamentaux de l'Union européenne intitulé «Surveillance par les services de renseignement: protection des droits fondamentaux et voies de recours dans l'Union européenne – Panorama du droit des États membres en 2015», disponible ici: http://fra.europa.eu/sites/default/files/fra_uploads/fra-2015-surveillance-intelligence-services_en.pdf.

[31] Même si l'annexe VI prévoit une période de conservation de cinq ans à des fins de renseignement, elle précise également que les informations peuvent être conservées pendant plus de cinq ans «si cette conservation continue de présenter un intérêt national pour les États-Unis». En outre, ce principe ne couvre pas les données transférées et utilisées à des fins purement commerciales.

[32] Voir l'article 6, paragraphe 1, point c), de la Directive.

[33] Accord entre les États-Unis d'Amérique et l'Union européenne concernant la protection des informations à caractère personnel afin de prévenir et de détecter les infractions pénales et de procéder aux enquêtes et poursuites en la matière. Le projet de mise en œuvre disponible ici: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf. Voir également l'Avis 1/2016 du CEPD, du 12 février 2016 concernant l'accord-cadre, point 44.

[34] Avis 01/2016 du G29 concernant la décision d'adéquation relative au Bouclier vie privée UE-États-Unis (WP 238), p. 20.

[35] Ainsi par exemple, le principe complémentaire 3 prévoit une exemption de responsabilité pour les fournisseurs de services Internet, les opérateurs de télécommunications et d'«autres organisations» quand ils transmettent, acheminent, échangent ou enregistrent des informations pour le compte d'une autre organisation dans le cadre du Bouclier vie privée. Le considérant 47 de la directive 95/46 n'exclut pas que ces entités puissent être des sous-traitants et qu'ils puissent être soumis à la Directive. En outre, le traitement des données par ces entités est déjà couvert par la directive Vie privée et communications électroniques. Enfin, le régime dérogatoire de responsabilité de la directive 2000/31 «e-commerce» ne concerne pas le droit de la protection des données [(article 1, paragraphe 5, point b)]. Étant donné que les entreprises de télécommunications semblent être exclues du champ d'application du Bouclier vie privée, leur inclusion dans ce principe crée une confusion.

[36] Annexe II, III, 2 b) du projet de décision.

[37] Arrêt C-73/0716, Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy et Satamedia Oy, 16 décembre 2008.

[38] Arrêt C-131/12 – Google Espagne/Agencia Española de Protección de Datos et Mario Costeja González, 13 mai 2014.

39 Voir également la jurisprudence de la Cour européenne des droits de l'homme, en particulier l'arrêt Von Hannover c. Allemagne, n° 59320/00, Von Hannover c. Allemagne (n° 2) [GC] n° 40660/08 et 60641/08, et l'arrêt Axel Springer AG c. Allemagne [GC] n° 39954/08.

[40] Voir également l'article 9 de la Directive.

[41] Au point 81 de l'arrêt *Schrems*, la CJUE déclare, concernant le système d'auto-certification que «*la fiabilité d'un tel système [...] 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 droits fondamentaux, notamment du droit au respect de la vie privée ainsi que du droit à la protection des données à caractère personnel*».

[42] Voir les principes complémentaires, annexe II.III.5 c) du Bouclier vie privée.

[43] Avis 01/2016 du G29 relatif à la décision d'adéquation sur le Bouclier vie privée vie privée UE-États-Unis (WP 238), p. 27, et lettre à la vice-Présidente Reding du 10 avril 2014, p. 5, disponible ici: http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf.

[44] Projet de décision, paragraphes 50-51.

[45] Projet de décision, p. 29.

[46] Judicial Redress Act, 2015, Pub. L. 114-126, R.H. 1428.

[47] Section 2 H 4a) de la Judicial Redress Act.

[48] tels que la loi américaine de 1996 sur la sécurité sociale (Health Insurance Portability and Accountability Act), Pub. L., 110 Stat. 1936 (HIPAA) ou la loi de 1998 sur la protection de la vie privée des enfants sur internet (Children's Online Privacy Protection Act), Pub. L. 105-277, 112 Stat. 2681-728 (COPPA).

[49] Voir article 45, paragraphe 2, point b), du RGPD.