GROUPE DE TRAVAIL «ARTICLE 29» SUR LA PROTECTION DES DONNÉES

16/FR
WP 238

Avis 01/2016 sur le projet de décision concernant le caractère adéquat du bouclier de protection des données UE-États-Unis

Adopté le 13 avril 2016

RESUME

Le 29 février 2016, la Commission européenne a publié une communication, un projet de décision d'adéquation ainsi que les textes en annexe constituant un nouveau cadre pour les échanges transatlantiques de données à caractère personnel à des fins commerciales: le bouclier de protection des données UE-États-Unis (ci-après «le bouclier de protection des données»), visant à remplacer le précédent régime de la sphère de sécurité des États-Unis, invalidé par la Cour de justice de l'Union européenne (ci-après «la CJUE») le 6 octobre 2015, dans l'affaire Schrems.

Conformément à l'article 30, paragraphe 1, de la directive 95/46/CE, le groupe de travail «Article 29» a évalué ces documents afin de donner son avis sur le projet de décision d'adéquation. Le groupe de travail «Article 29» a évalué à la fois les aspects commerciaux et les dérogations potentielles aux principes du bouclier de protection des données aux fins de l'application de la loi, de la sécurité nationale et de l'intérêt public.

Le groupe de travail «Article 29» a tenu compte du cadre juridique de l'UE applicable en matière de protection des données tel qu'établi par la directive 95/46/CE, ainsi que des droits fondamentaux au respect de la vie privée et à la protection des données consacrés par l'article 8 de la convention européenne des droits de l'homme et par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne. Il a également pris en considération le droit à un recours effectif et à un procès équitable établis à l'article 47 de la charte, ainsi que la jurisprudence relative aux différents droits fondamentaux.

Son analyse a également tenu compte du raisonnement suivi par la CJUE dans l'affaire Schrems en ce qui concerne la marge d'appréciation dont dispose la Commission pour évaluer l'adéquation. La vérification et les contrôles des exigences en matière d'adéquation doivent être rigoureusement effectués, en tenant compte des droits fondamentaux au respect de la vie privée et à la protection des données ainsi que du nombre de personnes potentiellement affectées par les transferts de données.

Le bouclier de protection des données doit être envisagé dans le contexte international actuel, caractérisé notamment par l'émergence des mégadonnées et des besoins de sécurité croissants. L'ampleur et la portée de la collecte et de l'utilisation de données à caractère personnel ont augmenté de manière vertigineuse depuis la publication, en 2000, de la première décision relative à la sphère de sécurité. Les autorités européennes de protection des données insistent fermement sur l'importance des principes qu'elles défendent.

Le groupe de travail «Article 29» salue tout d'abord les améliorations substantielles apportées par le bouclier de protection des données par rapport à la décision relative à la sphère de sécurité. Il note que bon nombre des lacunes de la sphère de sécurité qu'il avait soulignées dans sa lettre du 10 avril 2014 à la vice-présidente Reding ont été corrigées par les négociateurs.

Le fait que les principes et garanties établis par le bouclier de protection des données se retrouvent à la fois dans la décision d'adéquation et dans ses annexes rend les informations à la fois difficiles à trouver et, parfois, incohérentes. Cette dispersion contribue au manque général de clarté du nouveau cadre, et complique l'accès des personnes concernées, des organisations et des autorités de protection des données. De même, le langage utilisé manque de clarté. Le groupe de travail «Article 29» invite dès lors la Commission à rendre le bouclier de protection des données clair et compréhensible des deux côtés de l'Atlantique.

En ce qui concerne le droit applicable, le groupe de travail «Article 29» souligne que si la décision d'adéquation du bouclier de protection des données est adoptée sur la base de la directive 95/46/CE, elle doit être cohérente avec le cadre juridique de l'UE en matière de protection des données, tant sur le plan de sa portée que sur le plan de la terminologie utilisée. Selon le groupe de travail «Article 29», un contrôle devrait être réalisé peu après l'entrée en vigueur du règlement général sur la protection des données afin de s'assurer que le niveau accru de protection des données prévu par le règlement est bien respecté dans la décision d'adéquation et ses annexes.

Sur les aspects commerciaux du bouclier de protection des données

L'objectif premier du groupe de travail «Article 29» est de s'assurer qu'un niveau de protection des personnes fondamentalement équivalent est maintenu lors du traitement de données à caractère personnel sur la base des dispositions du bouclier de protection des données. Si le groupe de travail «Article 29» ne s'attend pas à ce que le bouclier de protection des données soit une simple copie, mot pour mot, du cadre juridique de l'UE, il estime qu'il devrait reprendre l'essentiel des principes fondamentaux et ainsi garantir un niveau de protection «fondamentalement équivalent».

Malgré les améliorations apportées par le bouclier de protection des données, le groupe de travail «Article 29» considère que certains principes clés de la protection des données établis en droit européen ne se retrouvent pas dans le projet de décision d'adéquation et les annexes, ou ont été remplacés de manière inappropriée par d'autres notions.

Par exemple, le principe de conservation des données n'est pas expressément mentionné et ne peut être clairement déduit du libellé actuel du principe «Intégrité des données et limitation des finalités». En outre, rien n'est dit sur la protection qui doit être accordée contre les décisions individuelles automatisées prises sur le seul fondement d'un traitement automatisé. L'application du principe de limitation des finalités aux opérations de traitement de données est également floue. Afin de clarifier l'utilisation de plusieurs notions importantes, le groupe de travail «Article 29» suggère que l'UE et les États-Unis se mettent d'accord sur des définitions claires qui figureront dans un glossaire de termes à inclure dans la FAQ du bouclier de protection des données.

Étant donné que le bouclier de protection des données sera également utilisé pour transférer des données en dehors des États-Unis, le groupe de travail «Article 29» insiste pour que les transferts ultérieurs d'une entité soumise au bouclier de protection des données à des

destinataires de pays tiers garantissent le même niveau de protection à tous les aspects du bouclier (y compris la sécurité nationale) et n'entraîne pas de diminution du respect des principes de protection des données de l'UE ou de contournement de ceux-ci. Dans le cas où un transfert ultérieur vers un pays tiers serait envisagé dans le cadre du bouclier de protection des données, chaque organisation participant au bouclier devrait être tenue d'évaluer les éventuelles exigences contraignantes de la législation nationale du pays tiers applicable à l'importateur des données préalablement au transfert de celles-ci. De manière générale, le groupe de travail «Article 29» conclut que les transferts ultérieurs de données à caractère personnel de l'UE ne sont pas suffisamment encadrés, surtout en ce qui concerne leur portée, la limitation de leurs finalités et les garanties applicables aux transferts à des mandataires.

Enfin, bien que le groupe de travail «Article 29» note que des recours supplémentaires sont offerts aux personnes afin qu'elles puissent exercer leurs droits, il craint que le nouveau mécanisme de recours s'avère concrètement trop complexe et trop difficile à utiliser pour les particuliers de l'UE et, dès lors, inefficace. Il est donc nécessaire de clarifier les différentes procédures de recours; en particulier, lorsqu'elles y sont disposées, les autorités de protection des données de l'UE pourraient être considérées comme des points de contact naturels pour les particuliers de l'UE dans le cadre des procédures, en ayant la possibilité d'agir en leur nom.

Dérogations pour les besoins de la sécurité nationale

S'agissant de l'accès aux données par les autorités publiques, tant dans l'UE que dans les pays tiers, le groupe de travail «Article 29» renvoie à son analyse des droits fondamentaux pertinents incluse dans le document de travail sur la justification des ingérences dans l'exercice des droits fondamentaux au respect de la vie privée et à la protection des données via des mesures de surveillance au moment du transfert de données à caractère personnel (garanties essentielles européennes) (WP237).

Le fait que le projet de décision d'adéquation tient désormais largement compte de la possibilité d'accéder aux données traitées au titre du bouclier de protection des données à des fins de sécurité nationale et d'application de la loi représente une avancée considérable par rapport à la décision relative à la sphère de sécurité. Le groupe de travail «Article 29» reconnaît qu'il s'agit d'un progrès important, de même que la transparence accrue offerte par l'administration américaine au sujet de la législation applicable à la collecte de renseignements (annexe VI).

Le groupe de travail «Article 29» note toutefois que les observations du bureau du directeur du renseignement national américain (ODNI) n'excluent pas la collecte massive et indifférenciée de données à caractère personnel provenant de l'UE. Le groupe de travail «Article 29» rappelle sa position de longue date selon laquelle la surveillance massive et indifférenciée des personnes ne saurait jamais être considérée comme proportionnée et strictement nécessaire dans une société démocratique, comme l'exige la protection offerte par les droits fondamentaux applicables. En outre, un contrôle approfondi de tous les programmes de surveillance est essentiel. Le groupe de travail «Article 29» constate qu'il y a une tendance

à collecter toujours plus de données sur une base massive et indifférenciée dans le cadre de la lutte contre le terrorisme. Étant donné les inquiétudes que cela soulève pour la protection des droits fondamentaux au respect de la vie privée et à la protection des données, le groupe de travail «Article 29» attend avec intérêt les prochains arrêts de la CJUE dans les affaires relatives à la collecte de données massive et indifférenciée.

S'agissant des recours, le groupe de travail «Article 29» se félicite de la création d'un poste de médiateur en vue d'offrir un nouveau mécanisme de recours. Cette décision pourrait apporter une amélioration considérable des droits des particuliers de l'UE en ce qui concerne les activités du renseignement américain. Toutefois, le groupe de travail «Article 29» craint que cette nouvelle institution ne soit pas suffisamment indépendante et ne dispose pas des pouvoirs nécessaires pour exercer efficacement sa mission et qu'elle ne représente pas un remède efficace en cas de désaccord.

Examen conjoint

Le mécanisme de réexamen annuel conjoint mentionné dans le projet de décision d'adéquation est capital pour la crédibilité globale du bouclier de protection des données et le groupe de travail «Article 29» est particulièrement satisfait que ce mécanisme permette de réexaminer la décision d'adéquation. Le groupe de travail «Article 29» croit comprendre à cet égard que ses représentants nationaux pourront participer pleinement au processus de réexamen; il demande néanmoins des précisions sur les dispositions exactes qui ont été prises. Les modalités (y compris le rapport final, sa publication et les conséquences éventuelles, ainsi que le financement) doivent être convenues suffisamment longtemps avant le premier réexamen.

Conclusion

Le groupe de travail «Article 29» prend note des améliorations substantielles apportées par le bouclier de protection des données par rapport à la décision relative à la sphère de sécurité invalidée. Compte tenu des préoccupations exprimées et des précisions demandées, le groupe de travail «Article 29» prie instamment la Commission de dissiper les préoccupations, d'apporter les solutions adéquates et de fournir les précisions demandées afin d'améliorer le projet de décision d'adéquation et de faire en sorte que la protection offerte par le bouclier de protection des données soit bien substantiellement équivalente à celle de l'UE.

TABLE DES MATIERES

1. INTRODUCTION

À la suite de l'arrêt rendu par la Cour de justice de l'Union européenne (ci-après «la CJUE») le 6 octobre 2015 dans l'affaire Schrems[1], le groupe de travail «Article 29» a appelé les États membres de l'Union européenne (ci-après «l'UE») et les autres institutions européennes à entamer des discussions avec les autorités des États-Unis en vue de trouver des solutions politiques, juridiques et techniques rendant possibles des transferts de données vers le territoire américain conformes aux droits fondamentaux.

Le 2 février 2016, après plus de deux ans de négociations, la Commission européenne et le ministère américain du commerce ont abouti à un accord politique relatif à un *nouveau cadre pour les échanges transatlantiques de données à caractère personnel à des fins commerciales: le bouclier de protection des données UE-États-Unis* (ci-après «le bouclier de protection des données»), visant à remplacer l'ancienne «sphère de sécurité» américaine.

Le 29 février 2016, la Commission a publié une communication[2], un projet de décision d'adéquation ainsi que les textes en annexe qui constitueront le bouclier de protection des données. Conformément à l'article 30, paragraphe 1, point c), de la directive 95/46/CE (ci-après «la directive»), le groupe de travail «Article 29» a examiné ces documents afin de rendre son avis actuel sur le projet de décision d'adéquation préparé par la Commission, y compris les documents du bouclier qui s'y rapportent. Dans le cadre de cet examen, le groupe de travail «Article 29» a scindé son travail en deux parties: une évaluation du volet commercial du bouclier de protection des données et une analyse des garanties mises en place au sujet des dérogations aux principes du bouclier à des fins de sécurité nationale, d'application de la loi et d'intérêt public.

À la suite de l'arrêt Schrems, le groupe de travail «Article 29» a organisé plusieurs réunions avec des délégations de l'administration américaine, des représentants d'organisations de la société civile européennes et américaines et des universitaires afin de préparer l'évaluation des conséquences de l'arrêt Schrems. Pendant l'examen du bouclier de protection des données, d'autres réunions se sont tenues avec la Commission européenne et des représentants de l'administration américaine. Lors de ces réunions, certaines précisions ont été données et celles-ci ont également été prises en compte dans le présent avis. Le groupe de travail «Article 29» souligne qu'à ce stade, ces précisions n'ont qu'un caractère informel et ne peuvent être considérées comme faisant partie intégrante du projet de décision d'adéquation, étant donné qu'elles n'ont pas encore été couchées par écrit.

Le groupe de travail «Article 29» se félicite néanmoins particulièrement de l'engagement pris par le ministère américain du commerce, pendant ces réunions, de coopérer avec les autorités de protection des données des États membres de l'UE au sujet de l'application du bouclier de protection des données et de leur fournir des instructions et une interprétation légale de l'application du bouclier pour publication sur leur site web.

[1] Arrêt du 6 octobre 2015, Maximillian Schrems/Data Protection Commissioner, C-362/14 (ci-après «l'arrêt Schrems»).
[2] COM(2016) 117 final du 29 février 2016.

1.1. Observations générales

1.1.1 Portée de l'examen du groupe de travail «Article 29»

Le groupe de travail «Article 29» a tout d'abord tenu compte du cadre applicable en matière de protection des données dans les États membres de l'Union européenne, notamment l'article 8 de la convention européenne des droits de l'homme (ci-après «la CEDH») qui protège le droit au respect de la vie privée et familiale, ainsi que les articles 7, 8 et 47 de la charte des droits fondamentaux de l'Union européenne (ci-après «la charte»), protégeant respectivement le droit au respect de la vie privée et familiale, le droit à la protection des données à caractère personnel et le droit à un recours effectif et à un procès équitable. Il a également pris en considération la jurisprudence pertinente, ainsi que les exigences de la directive.

L'exigence pour les pays tiers d'assurer un niveau de protection adéquat a été définie plus en détail par la CJUE dans l'arrêt Schrems. La Cour n'y a pas seulement expliqué que les dispositions de la directive devaient être interprétées «à la lumière des droits fondamentaux garantis par la Charte»[3], et notamment des articles 7 et 8, mais a également indiqué que le terme «niveau de protection adéquat» devait être compris 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 à celui garanti au sein de l'Union en vertu de la directive […], lue à la lumière de la Charte»[4]. Pour l'ancienne décision relative à la sphère de sécurité, cette analyse n'avait jamais été réalisée avec suffisamment de détail. Le groupe de travail «Article 29» a donc évalué le projet de décision d'adéquation à la lumière de l'obligation de contrôler que le niveau de protection des droits et libertés fondamentaux est *substantiellement équivalent* à celui garanti dans l'UE. Le groupe de travail «Article 29» souligne que le présent avis reprend ses principales préoccupations, mais que, compte tenu du peu de temps écoulé depuis la publication du projet de décision d'adéquation, d'autres problèmes pourraient être décelés à un stade ultérieur.

Le groupe de travail «Article 29» reconnaît qu'en définissant le terme «adéquat» utilisé à l'article 25, paragraphe 6, de la directive comme «substantiellement équivalent», la CJUE a apporté dans l'arrêt Schrems des précisions sur ce qu'était un caractère adéquat. La Cour a souligné que le terme «niveau de protection adéquat», s'il n'exige pas du pays tiers qu'il assure un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union, doit être compris 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* à celui garanti au sein de l'Union européenne en vertu de la directive lue à la lumière de la charte.

[3] Voir l'arrêt *Schrems*, point 38.
[4] Voir l'arrêt *Schrems*, point 73.

1.1.2 Examen du volet commercial du projet de décision d'adéquation

Le groupe de travail «Article 29» a déjà expliqué la manière dont il appliquait les grands principes de l'UE en matière de protection des données aux transferts de données à caractère personnel vers des pays tiers dans son document de travail nº 12 «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»[5]. Le groupe de travail «Article 29» a tenté de relever les garanties équivalentes assurant un niveau de protection équivalent aux principes garantis dans la directive, notamment en ce qui concerne la limitation des finalités, la qualité et la proportionnalité des données, la transparence, la sécurité, les droits d'accès, de rectification et d'opposition, la conservation des données et les restrictions relatives aux transferts ultérieurs. Une méthode similaire a été utilisée dans les avis rendus par le groupe de travail «Article 29» au moment de l'évaluation de la décision d'adéquation de la première décision relative à la sphère de sécurité[6], ainsi que dans les recommandations formulées par le groupe de travail dans sa lettre à l'ancienne vice-présidente et commissaire européenne pour la justice Viviane Reding, publiée le 10 avril 2014[7].

1.1.3 Examen des dérogations pour l'accès des autorités publiques et de leurs garanties

L'examen des dérogations relatives à l'accès des autorités publiques aux données à caractère personnel couvertes par le bouclier de protection des données est complexe, d'autant plus que, suite aux révélations d'Edward Snowden, les autorités de protection des données et le grand public sont davantage informés des programmes de surveillance américains. Le groupe de travail reconnaît et salue les efforts de l'administration américaine pour accroître la transparence de ses programmes de surveillance ainsi que sa volonté d'inclure des garanties supplémentaires dans le bouclier de protection des données. Parallèlement, le groupe de travail «Article 29» souligne que dans une société démocratique, toute ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel doit pouvoir se justifier. La CJUE a critiqué le fait que la décision relative à la sphère de sécurité ne contenait aucune constatation concernant l'existence, aux États-Unis, de règles adoptées par l'État en vue de limiter toute ingérence; en outre, elle ne fait pas état de l'existence d'une protection juridique efficace contre des ingérences de cette nature[8].

Le groupe de travail «Article 29» a par conséquent analysé le cadre juridique actuel des États-Unis et les pratiques des agences de renseignement américaines tels que décrits dans les annexes au projet de décision, ainsi que les conditions dans lesquelles ils autorisent une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel tels que protégés par le cadre juridique européen.

[5] Adoptée par le groupe de travail «Article 29» le 24 juillet 1998; voir notamment la page 6.
[6] Voir WP62, WP32, WP27, WP23, WP21, WP19, WP15 et WP7.
[7] http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20140410_wp29_to_ec_on_sh_recommendations.pdf
[8] Schrems, points 87 et 88.

Afin de déterminer si une ingérence pourrait se justifier dans une société démocratique, l'examen a été réalisé à la lumière de la jurisprudence européenne sur les droits fondamentaux, qui établit quatre garanties essentielles[9] pour les activités de renseignement:

A. le traitement doit être conforme à la loi et reposer sur des règles claires, précises et accessibles: autrement dit, toute personne raisonnablement informée devrait pouvoir prévoir ce qui risque d'arriver à ses données là où elles sont transférées;
B. la nécessité et la proportionnalité au regard des objectifs légitimes poursuivis doivent être démontrées: un équilibre doit être trouvé entre l'objectif pour lequel les données sont collectées et consultées et les droits de la personne;
C. un mécanisme de surveillance indépendant à la fois efficace et impartial doit avoir été mis en place: il peut s'agir soit d'un juge, soit d'un autre organe indépendant, à condition qu'il possède la capacité suffisante pour effectuer les contrôles nécessaires;
D. la personne concernée doit avoir à sa disposition des moyens de recours effectifs: toute personne devrait avoir le droit de défendre ses droits devant un organe indépendant.

1.2 Le projet de décision d'adéquation

Le groupe de travail «Article 29» se félicite tout d'abord qu'une nouvelle procédure d'adéquation puisse être lancée moins de six mois après la déclaration d'invalidité de la décision relative à la sphère de sécurité par la CJUE. Compte tenu du volume de transferts de données effectués au quotidien entre l'UE et les États Unis qui, comme le reconnaît le groupe de travail, constituent une partie essentielle de l'économie des deux côtés de l'Atlantique, une clarification juridique serait la bienvenue le plus tôt possible.

Le groupe de travail «Article 29» regrette néanmoins que le projet de décision d'adéquation publié par la Commission n'inclue pas d'évaluation exhaustive de la législation nationale et des engagements internationaux des États-Unis sous la forme d'un rapport d'adéquation, comme cela s'est fait par le passé dans des procédures similaires et conformément à l'article 25 de la directive. Cela a empêché le groupe de travail «Article 29» de réaliser une analyse complète du contexte juridique dans lequel le bouclier de protection des données sera mis en œuvre. Le groupe de travail note par exemple que l'actuel projet de décision d'adéquation n'inclut aucune observation sur la législation existant aux États-Unis en matière de protection de la vie privée et des données, tant au niveau fédéral qu'au niveau des États, y compris la législation sectorielle, ni sur la législation permettant certaines formes d'accès public hors du cadre de la surveillance. En outre, le lien entre les transferts de données au titre du bouclier de protection des données et les transferts au titre des autres mécanismes existants garantissant un niveau adéquat de protection des données, tels que l'accord UE-États-Unis sur les données des dossiers passagers (PNR) et l'accord relatif au programme de surveillance du financement du terrorisme (TFTP), n'est pas défini.

[9] Les garanties essentielles européennes sont basées sur la jurisprudence de la CJUE et la CEDH et spécifiées plus en détail dans le document de travail du groupe de travail «Article 29» WP237, publié le 13 avril 2016.

1.2.1 Champ d'application du cadre de l'UE en matière de protection des données et, en particulier, des principes de la directive 95/46/CE

Le groupe de travail «Article 29» rappelle qu'en vertu du cadre juridique de l'UE en matière de protection des données et notamment de la directive (article 4, paragraphe 1), la législation des États membres s'applique non seulement aux opérations de traitement effectuées par les responsables de traitement établis sur leur territoire, mais aussi lorsque les responsables de traitement (bien que non établis dans l'UE) recourent à des moyens situés sur le territoire de l'UE, notamment pour la collecte de données à caractère personnel. Par conséquent, la législation des États membres de l'UE s'applique à toute opération de traitement effectuée avant le transfert vers les États-Unis, soit dans le cadre des activités d'une organisation établie dans l'UE, soit en ayant recours à des moyens situés dans l'UE et utilisés par une organisation non établie dans l'UE. Le groupe de travail «Article 29» demande que cela soit explicitement formulé dans le projet de décision d'adéquation.

Il devrait être clair que les principes du bouclier de protection des données s'appliquent dès le moment du transfert des données. Le groupe de travail «Article 29» rappelle par ailleurs que les responsables de traitement établis dans l'UE qui transfèrent des données à un sous-traitant aux États-Unis demeurent soumis à la législation de l'UE en matière de protection des données.

1.2.2 Manque de clarté des documents du bouclier de protection des données

Le fait que les principes et garanties établis par le bouclier de protection des données se retrouvent à la fois dans la décision d'adéquation et dans ses annexes rend les informations à la fois difficiles à trouver et, parfois, incohérentes. Cela contribue à un manque général de clarté du nouveau cadre, ainsi qu'à compliquer l'accès des personnes concernées, des organisations et des autorités de protection des données. De même, le langage utilisé manque de clarté. Le groupe de travail «Article 29» invite dès lors la Commission à rendre le bouclier de protection des données clair et compréhensible des deux côtés de l'Atlantique.

Le groupe de travail «Article 29» propose d'inclure une annexe distincte définissant les termes clés utilisés dans les documents du bouclier de protection des données. Il est capital, pour le bon fonctionnement du bouclier de protection des données des deux côtés de l'Atlantique, que les obligations imposées par la décision d'adéquation soient comprises de manière homogène et sans équivoque: c'est pourquoi le groupe de travail «Article 29» craint qu'en raison des nombreuses références croisées et formulations non harmonisées, ainsi que de la complexité des documents-cadres, des difficultés soient rencontrées au niveau de la cohérence, de la compréhension et de la clarté de la mise en œuvre du bouclier.

Surtout, les documents du bouclier de protection des données utilisent une terminologie qui ne correspond pas au vocabulaire généralement utilisé dans l'UE pour traiter de la protection des données. Ce n'est pas nécessairement un problème, pour autant que la terminologie correspondante dans le droit de l'Union (et dans le droit américain) soit clairement indiquée. Or le groupe de travail «Article 29» regrette de constater que ce n'est pas le cas, y compris

dans le projet de décision d'adéquation. Par exemple, le terme «accès» est utilisé au chapitre 3 du projet de décision d'adéquation dans un sens qui implique la collecte de données à caractère personnel, au lieu du fait de permettre à quelqu'un de consulter des données déjà collectées. L'accès aux données par des entreprises et le droit d'accès des personnes sont deux notions distinctes qui ne doivent pas être confondues.

Le groupe de travail «Article 29» souligne que la terminologie doit également être utilisée de manière cohérente dans tous les documents, y compris le projet de décision d'adéquation. Ce n'est actuellement pas le cas, par exemple pour les notions de «traitement» et de «données à caractère personnel». Toutes deux sont en principe bien définies à l'annexe II, mais ne sont pas appliquées de manière cohérente tout au long des documents, ce qui crée des failles dans la protection[1011].

Le groupe de travail «Article 29» se félicite que les définitions de certains termes utilisés aient été incluses dans les documents constituant le bouclier de protection des données. Ce n'est toutefois pas le cas pour plusieurs autres termes essentiels, dont «mandataire» ou «sous-traitant», «données codées», «données rendues anonymes» et «particuliers de l'UE», qui, d'après le groupe de travail «Article 29», nécessitent une définition claire sur laquelle les États-Unis et l'Union européenne s'accordent, afin d'éviter toute confusion ultérieure pour les responsables de traitement et les sous-traitants faisant usage du bouclier de protection des données, les autorités de contrôle et le grand public. Une solution aisée serait d'ajouter un glossaire de termes à la FAQ du bouclier de protection des données.

Le groupe de travail «Article 29» attire également l'attention sur les raisons légitimes de traiter des données sensibles énumérées dans le principe complémentaire 1 (annexe II, section III.1), dans les cas où une organisation n'est pas tenue d'obtenir un accord explicite (consentement). Ce principe complémentaire 1 peut être interprété comme détaillant les raisons légitimes de collecter de données dans l'UE, cette liste étant similaire à l'article 8 de la directive. Le groupe de travail «Article 29» voudrait rappeler que toute opération de traitement (y compris la collecte et le transfert) de données sensibles soumises au droit de l'Union doit être effectuée sur la base de raisons légitimes au sens de l'article 8 de la

[10] Certaines des clauses ne font qu'énumérer certains types d'opérations de traitement de données au lieu d'utiliser le terme «traitement», d'où des failles dans la protection. Par exemple, selon le libellé de l'annexe II, section III.6.f, les principes du bouclier de protection des données ne devraient être applicables que lorsque l'organisation «stocke, utilise ou communique» les données reçues (et ne seraient donc pas applicables pour les autres opérations couvertes par le terme «traitement», comme la collecte, l'enregistrement, la modification, l'extraction, la consultation ou l'effacement). La sécurité des données ne serait imposée que pour la création, la gestion, l'utilisation ou la diffusion d'informations à caractère personnel (annexe II, section II.4). La définition des données à caractère personnel est également limitée aux données «reçues» et «enregistrées». Autre exemple, le principe «Notification» (annexe II, section II.1.a.iv) dispose que l'organisation certifiée doit informer les personnes des finalités pour lesquelles elles «collectent et utilisent» des données les concernant. L'annexe II, section III.9.a.11, mentionne exclusivement les données «transférées» ou «consultées». Même s'il semble que dans la plupart des cas, le but n'est pas de limiter la portée des principes, ni de créer des failles de protection, cette terminologie incohérente engendre un risque que de telles failles apparaissent. Le terme «traitement» étant défini dans les principes, il est essentiel de l'utiliser de manière cohérente, afin d'éviter les failles qui existent désormais, sinon ce serait laisser trop de place à une interprétation vraisemblablement non souhaitée, susceptible d'entraîner une interprétation erronée du texte de la décision.

[11] La définition du terme «données à caractère personnel» incluse à l'annexe II, section I.8.a, fait référence à «toute donnée ou information concernant une personne identifiée ou identifiable». Un principe complémentaire précise néanmoins que lorsqu'il s'agit de données relatives aux ressources humaines, les principes ne s'appliquent qu'en cas de «transfert ou d'accès à des dossiers individuels identifiés». Le groupe de travail «Article 29» pense que cela pourrait permettre des traitements de données à caractère personnel qui ne seraient conformes ni aux principes du droit de l'Union en matière de protection des données, ni à la définition générale des données à caractère personnel au titre du bouclier de protection des données.

directive. Le bouclier de protection des données ne saurait être interprété comme offrant d'autres raisons d'effectuer ce type de traitement. Par exemple, selon le groupe de travail «Article 29», il n'est pas possible pour une organisation américaine de collecter, en vertu du droit du travail américain, des données soumises au droit de l'Union (voir annexe II, section III.1.a.v.). Le groupe de travail «Article 29» souligne dès lors que toute interprétation du principe complémentaire 1 peut uniquement entraîner son application aux données sensibles déjà transférées après avoir été collectées dans l'UE sur la base de raisons légitimes figurant à l'article 8 de la directive.

Le groupe de travail «Article 29» observe enfin un manque de clarté quant à la question de savoir qui peut être considéré comme «un particulier de l'UE» et bénéficier à ce titre d'une protection en vertu du bouclier de protection des données: l'ensemble des citoyens de l'Union ou l'ensemble des personnes résidant dans l'Union. Cette question est particulièrement importante pour le droit à un recours, y compris l'accès au mécanisme de médiation. Par ailleurs, la décision d'adéquation doit déterminer la mesure dans laquelle le bouclier de protection des données s'appliquera également aux citoyens/résidents des pays de l'EEE et de la Suisse qui, par le passé, étaient également couverts par le mécanisme de la sphère de sécurité.

1.2.3 Réexamen conjoint et suspension

Le groupe de travail «Article 29» se félicite que la Commission européenne et l'administration américaine soient convenues de procéder à un réexamen régulier de l'application concrète du bouclier de protection des données. Ce mécanisme de réexamen conjoint est une pratique connue depuis quelques années dans la communauté européenne de la protection des données, surtout en ce qui concerne les accords relatifs aux échanges de données PNR avec des pays tiers et l'accord TFTP. Le groupe de travail «Article 29» salue également le fait qu'un nombre indéterminé de représentants des autorités de protection des données puissent prendre part à ces réexamens conjoints.

Compte tenu de son expérience des réexamens conjoints acquise ces dernières années, le groupe de travail «Article 29» insiste pour que le réexamen conjoint du bouclier de protection des données soit plus approfondi que ceux de l'accord PNR et du TFTP. Il est notamment souhaitable qu'il n'inclue pas seulement des réunions avec des représentants des agences, organisations et entreprises américaines, mais aussi des contrôles sur place de certains éléments du bouclier. Les représentants des APD qui participeront à ce réexamen devront pouvoir formuler des suggestions pour ces contrôles sur place.

Le groupe de travail «Article 29» estime qu'un réexamen conjoint nécessite une évaluation conjointe des conclusions. Jusqu'à présent, les résultats des réexamens conjoints ont été présentés dans un document de travail des services de la Commission, pour lequel l'approbation des membres de l'équipe du réexamen conjoint n'appartenant pas à la Commission n'est pas exigée. Pour le réexamen conjoint du bouclier de protection des données, le groupe de travail «Article 29» aimerait que le rapport des conclusions soit

véritablement un produit conjoint. Une autre solution envisageable pourrait être la publication d'un rapport de réexamen conjoint distinct pour les APD.

Enfin, s'agissant du réexamen conjoint, le groupe de travail «Article 29» rappelle la promesse de la Commission de rembourser les coûts supportés par les représentants du groupe de travail pendant les réexamens conjoints. Le groupe de travail suppose que cette promesse s'appliquera également pour le réexamen du bouclier de protection des données, au moins pour un nombre raisonnable de représentants des APD.

Le groupe de travail «Article 29» recommande qu'au plus tard trois mois avant le début du premier réexamen conjoint du bouclier de protection des données, les modalités relatives au réexamen soient arrêtées par la Commission, l'administration américaine et le groupe de travail et couchées par écrit.

1.2.4 Cadre juridique de l'UE en cours de révision

La décision d'adéquation du bouclier de protection des données constitue la première décision d'adéquation formulée à la suite de l'accord de principe sur le texte du règlement général sur la protection des données. Le groupe de travail «Article 29» a toutefois indiqué que le bouclier de protection des données ne reflétait pas encore la situation future. Par exemple, de nouvelles notions importantes, telles que le droit à la portabilité des données et les obligations supplémentaires pour les responsables de traitement, y compris la nécessité d'effectuer des analyses d'impact sur la protection des données et de respecter les principes de respect de la vie privée dès la conception et de respect de la vie privée par défaut, n'ont pas été incluses dans le bouclier. Le groupe de travail «Article 29» voudrait dès lors suggérer d'effectuer, comme pour toutes les décisions d'adéquation existantes, un réexamen du bouclier de protection des données peu après l'entrée en vigueur du RGPD. Une référence explicite à ce processus de réexamen dans la décision d'adéquation finale serait également bienvenue.

2. EXAMEN DU VOLET COMMERCIAL DU PROJET DE DECISION D'ADEQUATION

2.1. Observations générales

2.1.1 Améliorations

Le groupe de travail «Article 29» se félicite des améliorations apportées par le bouclier de protection des données ainsi que de la volonté de ses négociateurs de tenter de combler les lacunes qu'il avait relevées au niveau de la sphère de sécurité. On peut notamment constater, par rapport à la sphère de sécurité, des améliorations au niveau des éléments suivants: insertion de définitions essentielles, telles que «données à caractère personnel», «traitement» et «responsable du traitement», la création de mécanismes destinés à assurer la surveillance de la liste du bouclier de protection des données et les contrôles internes ou externes de la conformité, désormais obligatoires. Des améliorations ont également été apportées au principe «Accès». Le groupe de travail «Article 29» constate par ailleurs que des droits de rectification et d'effacement sont à présent accordés en cas d'utilisation des données d'une manière jugée incompatible avec les principes du bouclier de protection des données. Par ailleurs, il est

désormais clairement indiqué que la personne doit à la fois se voir confirmer que ses données sont en cours de traitement et communiquer les données qui ont été traitées.

Enfin, le groupe de travail «Article 29» salue le renforcement des garanties légales établies en cas de transfert ultérieur des données ainsi que l'engagement pris par le ministère américain du commerce et la Commission fédérale du commerce (FTC) de mettre en œuvre les obligations établies par le bouclier de protection des données.

2.1.2 Application du bouclier de protection des données aux organisations faisant fonction de sous-traitants (mandataires)

La mesure dans laquelle les principes du bouclier de protection des données sont applicables aux organisations certifiées recevant des données à caractère personnel en provenance de l'UE à des seules fins de traitement (appelées «mandataires» ou «sous-traitants») reste malheureusement floue. Si les dispositions incluses à l'annexe II, section III.10.a., mentionnent effectivement des transferts de données vers des organisations certifiées à de telles fins (plus exactement, elles mentionnent l'obligation de conclure un contrat), elles ne contiennent aucune indication sur la manière dont les principes du bouclier de protection des données doivent s'appliquer aux sous-traitants (mandataires). Cela engendre une incertitude tant pour les organisations américaines certifiées qui reçoivent des données à des fins de traitement que pour les entreprises de l'Union qui effectuent des transferts de données vers des organisations certifiées agissant comme sous-traitants, ainsi que pour les personnes dont les données sont traitées. Il s'ensuit qu'il sera difficile de déterminer quelles sont les obligations qui s'appliquent effectivement aux organisations du bouclier qui traitent des données à caractère personnel en provenance de l'UE en tant que sous-traitants. Une clarification est donc manifestement nécessaire.

Il convient de tenir compte du fait que plusieurs des obligations figurant dans les principes ne sont pas applicables aux sous-traitants, vu que le responsable du traitement est toujours celui qui détermine les finalités et les moyens du traitement des données (voir la définition de «responsable de traitement» à l'annexe II, section I.8.c). C'est la raison pour laquelle certaines obligations incluses dans les principes peuvent, si elles sont appliquées à une organisation agissant en tant que sous-traitant, contredire le contrat de traitement de données exigé par le droit de l'UE (mentionné à l'annexe II, section III.10.a). Par exemple, le contrat de traitement de données n'autorise généralement pas le sous-traitant des données (mandataire) à effectuer un transfert ultérieur des données vers un responsable de traitement tiers, même dans les cas de figure visés à l'annexe II, section II.3.a. Les transferts ultérieurs vers des mandataires tiers ne doivent être autorisés qu'avec l'accord préalable du responsable du traitement. En outre, selon les dispositions du droit de l'Union, un sous-traitant (mandataire) n'est pas en mesure de fournir aux personnes une notification complète conformément au principe «Notification» (annexe II, section II.1), par exemple parce que cette organisation ne détermine pas elle-même les finalités du traitement.

Il est donc essentiel de préciser, dans les principes, que dans un tel cas de contradiction, les dispositions du contrat de traitement de données et, en particulier, les instructions de

l'organisation transférant les données depuis l'UE, prévalent. Sans cette précision, les principes pourraient être interprétés et appliqués d'une manière qui offrirait trop de capacités de contrôle au mandataire soumis au bouclier et l'exportateur de données de l'Union risquerait ainsi d'enfreindre ses obligations de responsable de traitement au titre de la législation européenne en matière de protection des données à laquelle il est soumis lorsqu'il transfère des données vers une organisation relevant du bouclier faisant office de mandataire. En outre, ce manque de clarté donne l'impression que le sous-traitant peut réutiliser les données comme il l'entend.

Par ailleurs, des règles spécifiques doivent être établies pour les cas où une organisation agit comme sous-traitant de données (mandataire), afin de veiller à ce que cette organisation respecte les instructions du responsable de traitement. Il doit être clairement indiqué que les organisations américaines recevant des données à de strictes fins de traitement ne peuvent décider de traiter les données en leur propre nom. En l'absence de règles spécifiques applicables aux organisations agissant en tant que sous-traitants, il est difficile de déterminer les règles qui permettraient aux sous-traitants (mandataires) de s'autocertifier.

2.1.3 Limitations de l'obligation de respecter les principes

L'annexe II, section I.5, prévoit notamment des exemptions aux principes lorsque des données couvertes par le bouclier de protection des données sont utilisées pour des raisons de sécurité nationale[12], d'intérêt public ou de respect des lois ou en vertu d'un texte législatif, d'un règlement administratif ou d'une décision jurisprudentielle créant des obligations contradictoires ou prévoyant des autorisations explicites. Sans connaître entièrement le droit américain au niveau fédéral et étatique, il est difficile pour le groupe de travail «Article 29» d'évaluer l'étendue de cette exemption et de déterminer si ces limitations peuvent se justifier dans une société démocratique. Il serait essentiel que la Commission européenne inclue également dans son projet de décision d'adéquation une analyse du niveau de protection accordé dans les cas où ces exemptions s'appliqueraient. Le groupe de travail «Article 29» appelle la Commission à faire en sorte que l'Union soit informée de tout texte législatif ou règlement du gouvernement susceptible d'affecter le respect des principes qui sont actuellement applicables ou qui le seront lorsque de nouveaux textes législatifs ou règlements entreront en vigueur aux États-Unis.

2.1.4 Absence d'un principe de limitation de la conservation des données

Le principe de limitation de la conservation des données [article 6, paragraphe 1, point e), de la directive] constitue un principe fondamental de la législation de l'Union en matière de protection des données; il exige que les données à caractère personnel ne soient conservées que pendant le temps nécessaire à la réalisation de l'objectif pour lequel elles ont été collectées ou ultérieurement traitées.

[12] Voir le chapitre 3 pour une analyse plus ample de l'utilisation des données à caractère personnel couvertes par le bouclier de protection des données à des fins de sécurité nationale et le chapitre 4 pour les fins relatives à l'application de la loi.

Toutefois, le groupe de travail «Article 29» ne trouve dans les documents constituant le bouclier de protection des données aucune référence à la nécessité que les responsables de traitement veillent à ce que les données soient effacées une fois que l'objectif pour lequel elles ont été collectées ou ultérieurement traitées est devenu obsolète. Il semble donc que les principes n'imposent pas aux organisations certifiées un délai limite de conservation des données comparable à celui imposé par le principe de limitation de la conservation des données en vertu du droit de l'Union.

Le libellé du principe «Intégrité des données et limitation des finalités» (annexe II, section II.5) ne saurait être considéré comme créant l'obligation, pour une organisation agissant en tant que responsable de traitement, d'effacer les données une fois qu'elles ne sont plus nécessaires à la réalisation des finalités pour lesquelles elles ont été collectées ou ultérieurement traitées ou, pour une organisation agissant en tant que sous-traitante, d'effacer les données une fois l'accord de service expiré.

Le groupe de travail souligne que l'absence de dispositions imposant une limite à la conservation des données au titre du bouclier de protection des données donne aux organisations la possibilité de conserver les données aussi longtemps qu'elles le souhaitent, même après avoir quitté le bouclier, ce qui n'est pas conforme au principe essentiel de limitation de la conservation des données.

2.1.5 Absence de garanties pour les décisions automatisées produisant des effets juridiques ou affectant de manière significative la personne

Le bouclier de protection des données n'apporte aucune garantie légale aux personnes soumises à des décisions produisant des effets juridiques à leur égard ou les affectant de manière significative, prises sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de leur personnalité, tels que leur rendement professionnel, leur crédit, leur fiabilité, leur comportement, etc.

La nécessité de fournir des garanties juridiques pour les décisions automatisées (produisant des effets juridiques ou affectant de manière significative la personne) afin de garantir un niveau de protection adéquat a déjà été soulignée par le groupe de travail «Article 29» dans son document de travail nº 12.

Cette nécessité est d'autant plus impérieuse que l'évolution constante des nouvelles technologies permet à davantage d'entreprises d'envisager la mise en place de systèmes de prise de décision automatisée, ce qui pourrait entraîner l'affaiblissement de la position des personnes laissées sans aucun recours contre ces décisions informatisées. Lorsque des décisions prises exclusivement par ces systèmes automatisés ont un impact sur la situation juridique de personnes ou affectent celles-ci de manière significative (par exemple en les plaçant sur une liste noire et en les privant ainsi de leurs droits), il est capital de fournir des garanties suffisantes, dont le droit de connaître la logique qui sous-tend le processus et de demander une nouvelle prise en charge sur une base non automatisée.

2.1.6 Période intermédiaire pour les relations commerciales existantes

Le bouclier de protection des données prévoit l'application immédiate des principes dès la certification. Toutefois, les organisations qui se certifient dans les deux premiers mois à compter de la date effective d'entrée en vigueur du cadre du bouclier de protection des données devront mettre le plus tôt possible leurs relations commerciales existantes avec des tierces parties en conformité avec le principe «Responsabilité en cas de transfert ultérieur», dans tous les cas dans les neuf mois suivant la date à laquelle elles certifient leur engagement à adhérer au bouclier de protection des données.

Cela signifie que les contrats existants doivent dans la mesure du possible être mis en conformité avec les principes dans les deux à neuf mois suivant la certification. Pendant cette période intermédiaire, il suffit de respecter les principes «Notification» et «Choix». Le groupe de travail «Article 29» insiste sur le fait que des transferts ne peuvent être effectués au titre du bouclier de protection des données qu'à partir du moment où l'organisation est en mesure de respecter pleinement toutes les exigences du bouclier. La possibilité d'envoyer des données pendant une période intermédiaire sans que le destinataire soit en mesure de respecter pleinement les principes du bouclier ne saurait être considérée comme respectant les conditions de transfert légal et n'est donc pas acceptable.

2.2. Observations spécifiques

2.2.1 Transparence

a) Remarques générales sur la notification

Le groupe de travail «Article 29» salue les exigences plus complètes et plus détaillées établies au titre du principe «Notification», en particulier le fait que la notification devra inclure un lien ou une adresse web vers la liste du bouclier de protection des données et mentionner le droit d'accès dont disposent les personnes ainsi que les mécanismes de règlement extrajudiciaire des litiges[13]. Le groupe de travail «Article 29» propose toutefois d'expliciter davantage les autres droits (de corriger ou d'effacer en cas de données inexactes ou traitées en violation des principes) couverts.

Les documents constituant le bouclier de protection des données suscitent un doute quant au moment où une organisation participant au bouclier de protection de la vie privée doit procéder à la notification d'une personne. L'annexe II, section II.1.b, dispose qu'une «notification doit être communiquée (…) lorsque [des personnes] sont invitées pour la première fois à fournir des informations à caractère personnel ou dès que possible après cette invitation et, en tout état de cause, avant que les données ne soient utilisées dans un but différent de celui pour lequel elles ont été initialement collectées ou traitées par l'organisation ayant effectué le transfert ou avant qu'elles ne soient diffusées pour la première fois à un tiers». Le groupe de travail «Article 29» considère que dans de nombreuses situations, les

[13] Annexe II, section II.1; le groupe de travail «Article 29» renvoie également à la deuxième recommandation de la Commission dans la communication COM(2103)847 ainsi qu'à la lettre du groupe de travail à la vice-présidente Reding du 10 avril 2014, en particulier le point 4 de la section «Transparence».

organisations américaines du bouclier ne collectent pas directement les données auprès de la personne concernée et que, par conséquent, la notification devrait être effectuée au moment où les données sont enregistrées par l'organisation.

Le groupe de travail «Article 29» note que la mise en œuvre effective des exigences relatives au principe «Notification» et à la politique de protection de la vie privée devrait être évaluée lors du premier examen annuel du bouclier.

b) Accessibilité du public à la politique de protection de la vie privée

Le groupe de travail «Article 29» se félicite de voir explicitement indiqué que le ministère américain du commerce vérifiera si les entreprises possédant un site web public ont bien publié leurs dispositions de protection de la vie privée sur ce site ou, si elles n'ont pas de site web public, le lieu où le texte de ces dispositions peut être consulté par le public[14].

c) Publication des conditions de protection de la vie privée figurant dans les contrats avec les sous-traitants

Le bouclier de protection des données prévoit, parmi les conditions dans lesquelles les organisations participant au bouclier de protection de la vie privée peuvent transférer des données à un sous-traitant (mandataire), l'obligation pour les organisations autocertifiées de «[faire] parvenir au ministère un résumé ou une copie représentative des dispositions de protection de la vie privée concernées figurant dans son contrat avec le mandataire» (voir l'annexe II, section II. 3.b.v). Le groupe de travail salue cette exigence de transparence vis-à-vis du ministère américain du commerce.

2.2.2 Choix

Le bouclier de protection des données prévoit le droit de s'opposer à la divulgation d'informations à caractère personnel à une tierce partie ou à l'utilisation d'informations personnelles dans un but matériellement différent[15] (annexe II, section III.2). En outre, les personnes bénéficient à tout moment d'un droit d'opposition à l'utilisation d'informations personnelles à des fins de marketing direct (annexe II, section III.12.a)[16].

Hormis en ce qui concerne les finalités de marketing direct, aucun détail n'est fourni au sujet de la manière et du moment où ce droit peut être exercé. Le groupe de travail «Article 29» considère que la seule référence à l'existence de ce droit dans la politique de protection de la vie privée n'est pas suffisante et qu'une possibilité *individualisée* d'exercer ce droit devrait être offerte *avant* la divulgation ou la réutilisation des informations à caractère personnel.

[14] Voir la première recommandation formulée par la Commission européenne dans sa communication COM(2013)847 ainsi que la lettre du groupe de travail «Article 29» à la vice-présidente Reding du 10 avril 2014, en particulier le point 3 de la section «Transparence».
[15] Le principe complémentaire 14.c.I prévoit le droit de se retirer d'un essai clinique, qui peut être considéré comme un droit d'opposition ou de retrait du consentement.
[16] Ce droit est identique à celui qui était accordé dans le cadre de la sphère de sécurité (FAQ 12) et aucun changement n'a été opéré à cet égard.

Le groupe de travail «Article 29» souligne par ailleurs qu'un droit général d'opposition (pour des motifs sérieux liés à la situation particulière de la personne concernée), interprété comme le droit, pour un individu, de réclamer l'interruption du traitement de ses données en présence de motifs sérieux et légitimes tenant à sa situation particulière, devrait être inclus dans le cadre du bouclier[17]. Le groupe de travail «Article 29» recommande fortement d'indiquer clairement dans le projet de décision d'adéquation que le droit d'opposition doit exister à tout moment et que cette opposition ne se limite pas à l'utilisation des données à des fins de marketing direct[18].

Le groupe de travail «Article 29» craint que l'absence d'une définition de ce qui doit être considéré comme un but «matériellement différent» ne génère confusion et insécurité juridique. Il convient de préciser que, quel que soit le cas de figure, le principe «Choix» ne peut jamais être utilisé pour contourner le principe de limitation des finalités[19]. Ce principe n'est applicable que lorsque la finalité est matériellement différente, mais tout de même compatible, le traitement pour une finalité incompatible était interdit (annexe II, section II.5.a). Il convient de préciser que le droit d'opposition ne saurait autoriser l'organisation à utiliser des données pour des finalités incompatibles. Le groupe de travail recommande par conséquent d'harmoniser les libellés concernés en utilisant une formulation unique et bien définie (p.ex. «finalité matériellement différente mais néanmoins compatible»).

Il serait utile de préciser à quel moment une décision prise afin de traiter des données pour une autre finalité ou pour divulguer des informations relève du droit de l'Union. Dans une telle situation, les conditions légales habituelles de l'Union concernant ce traitement (p.ex. l'interdiction du traitement pour une finalité incompatible, l'obligation de fournir un motif légitime pour le traitement et la nécessité d'informer la personne concernée) s'appliquent directement, y compris à l'organisation américaine soumise au droit de l'Union. Concrètement, cela signifie qu'il appartiendra à l'exportateur de l'Union prenant une telle décision de garantir la transparence et la licéité du traitement conformément au droit de l'Union. Le principe du choix ne s'appliquera donc que lorsque la décision est prise exclusivement par l'organisation américaine participant au bouclier non soumise au droit de l'Union.

2.2.3 Transferts ultérieurs

a) Champ d'application

Le groupe de travail «Article 29» est préoccupé par le cas où des transferts ultérieurs de données à caractère personnel seraient effectués d'une organisation certifiée participant au bouclier et située aux États-Unis vers un destinataire d'un pays tiers.

Le bouclier ne doit pas être uniquement considéré comme un outil permettant de transférer des données européennes de l'UE vers les États-Unis, mais aussi comme un outil qui servira à

[18] Voir la lettre du groupe de travail «Article 29» à la vice-présidente Reding, section «Choix».
[19] Un exemple concret de traitement ultérieur incompatible autorisé au titre du principe «Choix» est fourni par le principe complémentaire 9.b.i (voir le commentaire du groupe de travail «Article 29» à ce sujet au point consacré aux «données RH»).

transférer des données des États-Unis vers des pays tiers. Les dispositions relatives aux transferts ultérieurs constituent donc un élément important du bouclier; elles doivent apporter suffisamment de garanties ainsi qu'un niveau adéquat de protection pour les transferts ultérieurs de données en dehors des États-Unis. Un problème particulier concerne la sécurité nationale et les autorités chargées de l'application de la loi.

Le principe «Responsabilité en cas de transfert ultérieur» du bouclier de protection des données ne se limite pas aux responsables de traitement, sous-traitants ou agents destinataires de données qui sont établis aux États-Unis. Des transferts ultérieurs vers des pays tiers peuvent donc être effectués sur la base du bouclier même si le pays tiers en question possède des lois prévoyant l'accès du public aux données à caractère personnel, par exemple aux fins de la surveillance. Les données européennes sont ainsi exposées à un risque d'atteintes injustifiées à la protection des droits fondamentaux.

En cas de transfert ultérieur vers un pays tiers, chaque organisation participant au bouclier devrait être tenue d'évaluer les éventuelles exigences contraignantes de la législation nationale du pays tiers applicable à l'importateur des données préalablement au transfert de celles-ci. Lorsqu'un risque important pour les garanties, les obligations et le niveau de protection prévus par le bouclier de protection des données est détecté, l'organisation américaine participant au bouclier agissant en tant que sous-traitante (mandataire) avertit sans tarder le responsable de traitement de l'UE avant de procéder au moindre transfert ultérieur. Dans ce cas de figure, l'exportateur des données est autorisé à suspendre le transfert des données et/ou à résilier le contrat. En présence d'un tel risque d'incidence négative importante, l'organisation participant au bouclier agissant comme responsable du traitement ne doit pas être autorisée à procéder au transfert ultérieur des données, puisque cela reviendrait à enfreindre son obligation de garantir un niveau de protection égal à celui requis par les principes en cas de transfert ultérieur (voir l'annexe II, section II.3.a).

De même, en cas de modification de la législation du pays tiers susceptible d'affecter de manière substantielle les garanties, les obligations et le niveau de protection prévus par le bouclier de protection des données, l'organisation américaine participant au bouclier agissant en tant que sous-traitante (mandataire) doit être tenue - au titre du bouclier - de notifier cette modification à l'exportateur des données dès qu'elle en a connaissance; l'exportateur des données dispose alors du droit de suspendre le transfert des données et/ou de résilier le contrat. Dès lors, dans ce cas, l'organisation participant au bouclier agissant comme responsable du traitement ne doit pas être autorisée à procéder au transfert ultérieur des données, puisqu'elle a l'obligation de garantir un niveau de protection égal à celui requis par les principes (voir l'annexe II, section II.3.a).

Le groupe de travail «Article 29» rappelle sa position selon laquelle, lorsqu'un responsable de traitement européen prend connaissance d'un transfert ultérieur vers une tierce partie en dehors des États-Unis avant même que le transfert vers les États-Unis n'ait lieu, ou lorsque le responsable de traitement européen est conjointement responsable de la décision d'autoriser les transferts ultérieurs, le transfert doit être considéré comme un transfert direct de l'UE vers

le pays tiers situé en dehors des États-Unis. Ce sont alors les articles 25 et 26 de la directive qui sont applicables au transfert, et non le principe de transfert ultérieur du bouclier.

b) Transferts d'une organisation participant au bouclier vers un responsable de traitement d'un pays tiers

Le groupe de travail «Article 29» se félicite de l'obligation de conclure des contrats (annexe II, section II.3.a) afin d'assurer que les responsables de traitement de pays tiers garantiront un niveau de protection au moins égal à celui requis par les principes du bouclier de protection des données. Le but est de garantir le maintien de la protection adéquate des données à caractère personnel même après leur transfert ultérieur. Le groupe de travail «Article 29» a néanmoins quelques remarques à formuler au sujet des conditions proposées.

Absence de référence au principe de limitation des finalités

Le groupe de travail «Article 29» recommande d'insérer également une référence claire au principe de limitation des finalités (annexe II, section II.5) dans les conditions relatives aux transferts ultérieurs vers un responsable de traitement de pays tiers (annexe II, section II.3.a). Il serait ainsi clairement établi qu'aucun transfert ultérieur ne peut avoir lieu lorsque le responsable de traitement du pays tiers entend poursuivre une finalité incompatible.

Exemption à l'obligation de contrat pour les transferts intragroupe entre responsables de traitement

Une exemption à l'obligation de contrat est prévue pour les transferts intragroupes entre responsables de traitement. Dans ce cas de figure, les principes disposent que la continuité de la protection pourrait être garantie par des règles d'entreprise contraignantes (REC) ou par «d'autres instruments intragroupe (par ex. les programmes de conformité et de contrôle)» (annexe II, section III.10.b). Le groupe de travail «Article 29» considère que la référence à «d'autres instruments intragroupe» ne garantit pas que les autres membres du groupe prendront des engagements juridiquement contraignants. Le groupe de travail «Article 29» et la législation de l'Union[20] étant globalement favorables à des engagements contraignants qui encadreraient les transferts intragroupes, il est important d'éviter que le bouclier de protection des données soit utilisé dans le but de contourner cette obligation. Le groupe de travail «Article 29» rappelle qu'en tout état de cause, les transferts ultérieurs des États-Unis vers des pays tiers prévus avant même le transfert des données vers les États-Unis ou soumis à une responsabilité conjointe avec le responsable de traitement de l'Union[21] doivent être considérés comme des transferts directs de l'UE vers le pays tiers extérieur aux États-Unis. Les articles 25 et 26 de la directive leur sont donc applicables.

c) Transferts d'une organisation participant au bouclier vers un sous-traitant (mandataire) d'un pays tiers

[20] La nécessité d'engagements contraignants et exécutoires est également soulignée dans le RGPD, quel que soit l'instrument utilisé (REC, clauses contractuelles, codes de conduite ou certification).
[21] Par exemple pour les données RH.

Le groupe de travail «Article 29» salue le fait qu'un contrat pour les transferts ultérieurs soit désormais obligatoire pour les entités destinataires agissant en tant que sous-traitantes (mandataires), peu importe qu'elles participent au bouclier de protection des données ou qu'elles bénéficient d'une autre solution au titre d'une décision d'adéquation. Le groupe de travail «Article 29» accueille également favorablement les garanties supplémentaires encadrant ces transferts ultérieurs (annexe II, sections II.3.a.i, II.3.a.iii, II.3.a.iv, II.3.a.v et II.7.d). Le dernier point (annexe II, section II.7.d) porte sur l'obligation de rester responsable lorsque des données sont divulguées à un mandataire. Il semble néanmoins que cette garantie ne s'applique pas lorsqu'une organisation choisit de coopérer avec une APD (voir l'annexe II, section III.5.a in fine). Le groupe de travail «Article 29» ne voit pas la raison d'une telle exemption et considère que la responsabilité devrait également s'appliquer dans ce cas.

Absence de référence au principe de limitation des finalités

Le groupe de travail «Article 29» note que si le principe «Responsabilité en cas de transfert ultérieur» (annexe II, section II.3) explique que les données à caractère personnel peuvent uniquement être transférées à une tierce partie agissant comme mandataire à des fins limitées et spécifiques, il n'indique pas explicitement que celles-ci doivent être compatibles avec les fins initiales pour lesquelles les données ont été collectées ainsi qu'avec les instructions du responsable du traitement. Une plus grande clarté est nécessaire sur ce point. Le groupe de travail «Article 29» propose dès lors de faire en sorte que la décision d'adéquation apporte plus de détails, en y insérant par exemple une référence claire au principe de limitation des finalités (annexe II, section II.5), interdisant le traitement (y compris la divulgation) de données pour une finalité incompatible avec le principe de transfert ultérieur (en plus du principe d'opposition).

Nécessité d'obligations supplémentaires pour les organisations participant au bouclier agissant en tant que sous-traitantes (mandataires) de données transférées à un autre sous-traitant (mandataire)

L'absence de règles claires applicables aux cas où l'organisation participant au bouclier agit en tant que sous-traitante (c'est-à-dire pour le compte d'un responsable de traitement de l'Union) entraîne une faille risquant d'empêcher le responsable de traitement de l'Union de garder le contrôle. Les organisations participant au bouclier qui reçoivent des données en tant que mandataires d'un responsable de traitement de l'Union sont tenues de respecter les instructions de ce dernier. Cette obligation devrait être expressément mentionnée dans les principes afin de s'assurer que tout manquement à ces instructions entraînera non seulement une infraction au contrat (annexe II, section III.10.a.ii), mais aussi une violation des principes du bouclier de protection des données.

La possibilité offerte à une organisation du bouclier agissant en tant que mandataire de transférer ultérieurement des données à un mandataire tiers doit être clairement indiquée au responsable du traitement et être soumise à son accord préalable. Il convient donc de mentionner clairement que c'est le contrat conclu par le mandataire avec le responsable de

traitement de l'Union (appelé «contrat au titre de l'article 17» dans la FAQ nº 10) qui détermine si un transfert ultérieur est autorisé[22].

Les conditions actuellement applicables aux transferts ultérieurs à un mandataire reposent sur l'hypothèse que l'organisation participant au bouclier agit en tant que responsable du traitement et peut donc décider elle-même de l'éventuelle intervention d'un mandataire tiers. Cela ne devrait toutefois pas être possible lorsque l'organisation participant au bouclier agit en tant que mandataire, car le responsable du traitement serait alors privé de ses capacités de contrôle.

Les dispositions de protection de la vie privée figurant dans le contrat conclu avec le mandataire tiers doivent au moins être mises à la disposition du responsable du traitement et doivent également offrir un niveau de protection au moins égal à celui offert par le contrat conclu avec le responsable du traitement.

2.2.4 Intégrité des données et limitation des finalités

a) Proportionnalité

Sur un plan secondaire, le groupe de travail «Article 29» renvoie à sa lettre adressée à la vice-présidente Reding, dans laquelle il indiquait qu'il était «possible que même en respectant à la lettre les principes "Notification" et "Choix", un traitement de données à caractère personnel ne soit pas proportionné au regard des droits et des libertés de la personne concernée ou de la société. Le principe de la proportionnalité ou du caractère raisonnable doit être respecté à tous les stades du traitement et être appliqué en plus des principes "Notification" et "Choix"»[23].

Le bouclier de protection des données (annexe II, section II.5.a) dispose que les informations doivent se limiter à ce qui est pertinent aux fins du traitement. Le groupe de travail «Article 29» préférerait que ce libellé soit modifié dans la décision d'adéquation finale: en effet, le seul fait que les données soient pertinentes aux fins du traitement ne suffit pas à rendre le traitement proportionné. Afin de respecter le principe de proportionnalité, le traitement devrait être limité aux données qui lui sont nécessaires.

b) Exactitude

Le principe «Intégrité des données et limitation des finalités» (annexe II, section II.5) dispose également ce qui suit: «Toute organisation doit prendre les mesures qui s'imposent, dans la limite de ces objectifs, pour assurer la fiabilité des données à caractère personnel par rapport à l'utilisation prévue ainsi que leur exactitude, leur exhaustivité et leur actualité». Le groupe de travail «Article 29» note qu'il s'agit mot pour mot du même libellé que celui utilisé dans les arrangements relatifs à la sphère de sécurité. Il doute que l'expression «dans la limite nécessaire à la réalisation de ces objectifs» doive être incluse, puisque selon lui, l'exactitude

[22] Voir la lettre du groupe de travail «Article 29» à la vice-présidente Reding du 10 avril 2014, point 4, section «Transfert ultérieur».
[23] Voir la lettre du groupe de travail «Article 29» à la vice-présidente Reding du 10 avril 2014, p. 8.

des données ne dépend pas des objectifs du traitement. Le groupe de travail «Article 29» préférerait que ce lien ne soit pas fait dans la décision d'adéquation finale.

c) Limitation de la finalité

Lorsque des données à caractère personnel sont transférées à une organisation américaine par un responsable de traitement établi dans l'UE, l'exportateur des données doit explicitement informer l'organisation américaine des finalités pour lesquelles les données ont été initialement collectées. En effet, cette information est nécessaire pour pouvoir déterminer si un changement de finalité est intervenu après le transfert, déclenchant ainsi l'application des principes «Notification» et «Choix», et permettre d'attribuer les risques et responsabilités.

Le principe «Intégrité des données et limitation des finalités» (annexe II, section II.5) dispose qu'une organisation ne peut pas traiter des données à caractère personnel d'une manière qui est incompatible avec les objectifs pour lesquels elles ont été collectées ou avec les objectifs approuvés ultérieurement par la personne concernée. Le principe «Choix» (annexe II, section II.2) prévoit néanmoins un consentement à l'«utilisation» d'informations sensibles (données concernant le dossier médical ou l'état de santé d'une personne, son origine raciale ou ethnique, ses opinions politiques, ses croyances religieuses ou ses convictions philosophiques, son affiliation à un syndicat ou sa sexualité, ainsi que les données relatives à son casier judiciaire) 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 la personne concernée. Ce consentement n'est pas exigé dans les situations mentionnées au principe complémentaire 1.a (annexe II, section III.1.a). S'agissant des informations à caractère personnel non sensibles, un système d'opposition est prévu.

Le groupe de travail «Article 29» note que la portée du principe de limitation des finalités est différente selon qu'il s'agit du principe «Notification», «Choix» ou «Intégrité des données et limitation des finalités». Les termes «finalité incompatible» et «but matériellement différent» sont d'ailleurs utilisés dans le même texte sans qu'aucun de ces deux concepts ne soit clairement défini[24].

Le groupe de travail «Article 29» craint sérieusement que cette incohérence ne pose d'énormes difficultés au moment de concilier le principe «Intégrité des données et limitation des finalités» (annexe II, section II.5) et le principe «Choix» (annexe II, section II.2): en effet, l'un indique que les données ne peuvent être traitées d'une manière qui serait incompatible avec les finalités pour lesquelles elles ont été collectées tandis que l'autre prévoit un mécanisme d'opposition en cas de traitement des données dans un but matériellement différent de l'objectif initial.

[24] Le groupe de travail «Article 29» a noté l'utilisation d'autres expressions: «utilisation non conforme» (annexe II, section III.14.b.ii), «utilisation à d'autres fins» (annexe II, section III. 9.B.i), «utilisation dans un but différent de celui pour lequel elles ont été initialement collectées» (annexe II, section II.1.b). Ce manque de clarté pourrait avoir comme conséquence des garanties insuffisantes en ce qui concerne le principe de limitation des finalités.

On pourrait donc en déduire que le principe «Choix» autorise un traitement ultérieur incompatible[25]. Selon le groupe de travail «Article 29», il est nécessaire d'indiquer explicitement qu'une organisation n'est pas autorisée à traiter des données dans un but matériellement différent lorsque ce but est incompatible en vertu du principe «Limitation des finalités». En d'autres termes, il doit être clairement précisé que le principe «Choix» n'est pas une exemption au principe de limitation des finalités.

Par ailleurs, quoi qu'il en soit, si le traitement ultérieur peut être considéré comme compatible, les principes «Notification» et «Choix» doivent également s'appliquer.

2.2.5 Exceptions journalistiques

Les exceptions journalistiques au traitement de données à caractère personnel sont couvertes par le principe complémentaire 2 (annexe II, section III.2). Ces dispositions sont censées refléter la protection de la liberté d'expression consacrée dans la Constitution des États-Unis. Les documents du bouclier de protection des données indiquent par conséquent que «les informations à caractère personnel qui ont été publiées antérieurement, puis archivées ne sont pas soumises aux principes du bouclier de protection des données» (annexe II, section III.2.b). Cette exemption semble inclure tout traitement ultérieur par un responsable de traitement ou un sous-traitant; autrement dit, elle ne se limite pas au traitement ultérieur à des fins journalistiques. Comme déjà indiqué dans la lettre à la vice-présidente Reding du 10 avril 2014, le groupe de travail «Article 29» aurait préféré une approche plus limitée des exceptions journalistiques, plus conforme au principe tel qu'appliqué dans l'Union, ainsi que le droit à la suppression de la liste des résultats conformément à l'arrêt Google Spain[26].

2.2.5 Droit d'accès, de rectification et d'effacement pour les personnes concernées

En vertu du bouclier de protection des données, les personnes ont le droit d'obtenir la *confirmation* que leurs données sont traitées par l'organisation et de *se faire communiquer* ces données (annexe II, section III.8.a.i). Toutefois, l'obligation, pour les organisations, de répondre aux questions de personnes concernées portant sur les finalités du traitement, les catégories de données à caractère personnel sur lesquelles il porte et les destinataires ou les catégories de destinataires auxquels les données à caractère personnel sont communiquées est relativement faible. D'après le groupe de travail «Article 29», les détails qui doivent être fournis à la personne concernée doivent être indiqués dans le corps de texte, et non pas uniquement dans une note de bas de page, et leur inclusion doit clairement constituer une obligation (en rapport avec l'annexe II, section III.8.a.i.1).

Selon le principe complémentaire 8, «[l]'accès ne doit être fourni que dans la mesure où l'organisation stocke les informations à caractère personnel» (annexe II, section III.8.d.ii). Cette règle ne doit pas être interprétée de manière restrictive: l'accès doit en principe

[25] Voir également le commentaire relatif au principe «Choix». D'après le groupe de travail «Article 29», le fait que les règles relatives au transfert ultérieur (annexe II, section II.3) ne fassent référence qu'au principe «Choix» et pas au principe «Limitation des finalités» accroît le risque d'une telle interprétation.

[26] Arrêt du 13 mai 2014, Google Spain/Agencia Española de Protección de Datos et Mario Costeja González, C-131/12.

concerner toutes les données traitées par une organisation, quel que soit le mode de traitement, et non pas seulement les données stockées. Dès lors, afin de garantir l'efficacité du droit d'accès, il est important de spécifier clairement que «stocker» signifie «traiter» au sens de la définition incluse à l'annexe II, section I.8.b. L'application de cette règle devrait faire l'objet d'une attention particulière lors du réexamen conjoint du bouclier de protection des données.

Des inquiétudes subsistent en ce qui concerne la liste d'exceptions incluse à l'annexe II, section III.8.e.(i), similaire à celle fournie à la FAQ nº 8 de la sphère de sécurité et qui a tendance à faire pencher la balance en faveur des intérêts des organisations. Dans ce cadre, les personnes n'obtiendront pas l'accès à leurs propres données personnelles pour les raisons suivantes: «le non-respect d'une obligation ou d'un privilège professionnel» (annexe II, section III.8.e.3), «une entrave aux enquêtes sur la sécurité des employés et aux procédures d'arbitrage, ou lors de l'organisation des remplacements et des restructurations» (annexe II, section III.8.e.4), et «le fait de porter atteinte à la confidentialité nécessaire au contrôle, à l'inspection ou aux fonctions réglementaires en rapport avec une gestion saine, ou dans le cadre de négociations futures ou en cours impliquant l'organisation» (annexe II, section III.8.e.5). À ces raisons doit venir s'ajouter l'exemption générale relative aux informations commerciales confidentielles incluse à l'annexe II, section III.8.c. Dès lors, une personne ne pourra jamais accéder à ses données dans l'une des situations mentionnées ci-dessus et aucune mise en balance des droits et intérêts de cette personne d'une part, et de l'organisation d'autre part, ne sera effectuée pour trouver une solution à la demande d'accès.

Le groupe de travail «Article 29» rappelle que le droit d'accéder à ses propres données est accordé aux personnes par l'article 8, paragraphe 2, de la charte. S'il ne s'agit pas d'un droit absolu, il est néanmoins essentiel pour le droit à la protection des données à caractère personnel, car il facilite l'exercice des autres droits de la personne concernée, tels que les droits à la rectification et à l'effacement.

S'agissant de ces derniers, le groupe de travail «Article 29» note avec satisfaction que les principes du bouclier de protection des données apportent une amélioration par rapport à ceux de la sphère de sécurité, pour autant que ces droits soient accordés non seulement lorsque les données sont inexactes, mais aussi lorsqu'elles ont été traitées en violation des principes (annexe II, section II.6).

2.2.6 Voies de recours, application et responsabilité (mécanismes de recours)

a) Exercice effectif des droits de recours des particuliers de l'UE

Le groupe de travail «Article 29» prend note des engagements des autorités américaines en ce qui concerne les différents niveaux du mécanisme de recours. Toutefois, compte tenu de la complexité et du manque de clarté de l'architecture globale du mécanisme, le groupe de travail craint que dans les faits, l'exercice effectif du droit de la personne concernée soit entravé. Le groupe de travail «Article 29» souligne que la qualité du mécanisme de recours devrait prévaloir sur la quantité de mécanismes à disposition des particuliers de l'UE. Il craint

également que la plupart, voire la totalité, des mécanismes de recours ne prévoient une procédure aux États-Unis, ce qui compliquerait le contrôle de la procédure par les ADP de l'Union.

Le mécanisme de recours prévu par le bouclier de protection des données se concentre d'ailleurs en premier lieu sur la possibilité pour les personnes concernées de «faire valoir leurs droits et d'introduire une réclamation en cas de non-conformité avec les principes de protection de la vie privée en prenant directement contact avec l'entreprise américaine autocertifiée»[27]. En outre, les organisations doivent désigner un organisme indépendant d'instruction des litiges pour l'instruction et la résolution des différentes plaintes. Le groupe de travail «Article 29» note avec satisfaction que cela sera organisé sans aucun frais pour la personne.

À titre subsidiaire, les réclamations pourront être directement introduites auprès de la Commission fédérale du commerce, même si celle-ci n'a aucune obligation de les traiter. Les APD pourront également introduire une réclamation et le ministère américain du commerce s'est engagé à examiner les réclamations et à faire tout ce qui est en son pouvoir pour favoriser la résolution des plaintes (annexe I) auxquelles la Commission fédérale du commerce (FTC) a donné la priorité (annexe II, section III.7.e). Toutefois, le fait qu'une réclamation soit considérée comme prioritaire par la FTC ne donne aucune assurance à la personne concernée que sa plainte soit traitée.

En dernier recours, les particuliers auront la possibilité de faire appel à un arbitrage contraignant. Le panel d'arbitrage sera basé aux États-Unis et soumis au contrôle des tribunaux américains.

Le bouclier de protection des données offre également à l'organisation la possibilité d'opter pour une coopération avec les APD de l'Union (annexe II, section III.5.a). Cette coopération est même obligatoire pour les données relatives aux ressources humaines collectées dans le cadre d'une relation de travail (annexe II, section III.9.d.ii). Dans ce cas de figure, le règlement extrajudiciaire des litiges ne sera pas applicable (annexe II, section III.5.a). Le bouclier de protection des données n'indique pas clairement comment la coopération avec les APD de l'Union sera concrètement organisée. Il est notamment difficile de savoir si un même panel traitera de tous les cas ou si chaque cas sera traité par un panel différent.

Le groupe de travail «Article 29» considère que la décision d'adéquation devrait inclure davantage d'informations au sujet de la compétence des APD pour traiter les réclamations. Celle-ci semble dépendre de la qualification de l'organisation, mais il est difficile de déterminer exactement de quelle manière.

Quoi qu'il en soit, lorsque l'organisation agit en tant que mandataire pour le compte d'un responsable de traitement de l'UE, les personnes auront la possibilité d'introduire une réclamation auprès de l'APD de l'UE compétente. La situation sera la même pour les

[27] Commission européenne, projet de décision d'adéquation, point 30.

traitements de données relatives aux ressources humaines et pour les traitements de données commerciales.

Lorsque l'organisation participant au bouclier agit en tant que responsable de traitement, la compétence d'une APD pour traiter la réclamation est limitée aux opérations de traitement soumises au droit de l'Union (traitements sous l'autorité du responsable du traitement - y compris les traitements soumis à une responsabilité conjointe avec l'organisation américaine - ou pour lesquels l'organisation membre du bouclier est directement soumise au droit de l'Union, par exemple parce qu'elle utilise du matériel dans l'UE). Toutefois, pour les traitements de données effectués uniquement au titre du droit américain, les seuls mécanismes applicables seront ceux du bouclier de protection des données. Afin de surmonter la barrière de la langue et le manque de connaissance du système juridique américain, il serait utile que les APD de l'UE aient le droit d'agir en tant qu'intermédiaires dans la réclamation du particulier ou d'assister celui-ci dans ses procédures de règlement extrajudiciaire avec les organisations américaines ou dans le cadre de ses contacts avec les autorités américaines, si l'APD l'estime pertinent.

Le groupe de travail «Article 29» souligne que le mécanisme expliqué dans le bouclier de protection des données ne suit pas la recommandation antérieure selon laquelle les particuliers de l'UE devraient «pouvoir demander une compensation dans l'Union européenne» et se voir «accorder le droit d'introduire une réclamation auprès d'une juridiction nationale compétente de l'UE»[28]. Il serait bienvenu que les organisations participant au bouclier incluent une telle possibilité dans leur politique de protection de la vie privée.

Afin d'assurer l'efficacité du système, le groupe de travail «Article 29» recommande que celui-ci permette aux APD de l'UE de représenter la personne concernée et d'agir pour son compte ou en tant qu'intermédiaire. À titre subsidiaire, le système devrait inclure des clauses de compétence spécifiques permettant aux personnes concernées d'exercer leurs droits en Europe.

b) Arbitrage

Les procédures finales d'arbitrage ne sont pas encore finalisées, ce qui complique leur évaluation par le groupe de travail «Article 29». Puisqu'il semble que le système d'arbitrage sera mis en œuvre au titre du droit américain et que la seule langue de procédure sera l'anglais, les APD de l'Union pourraient vouloir être autorisées à prêter assistance aux personnes concernées.

Par ailleurs, la procédure d'arbitrage a été mise en place parce qu'il n'y avait aucune assurance que les réclamations soient traitées, puisque la FTC n'a pas l'obligation de traiter chacune d'entre elles. Si un particulier de l'UE estime avoir besoin de se faire assister par un avocat, le groupe de travail «Article 29» observe que cette personne devra prendre elle-même en charge les honoraires, ce qui pourrait la dissuader de soumettre sa réclamation à la procédure d'arbitrage.

[28] Voir la lettre du groupe de travail «Article 29» à la vice-présidente Reding du 10 avril 2014.

c) Surveillance, application et efficacité des mécanismes de recours

Conditions d'adhésion au bouclier

Selon la CJUE, «la fiabilité d'un système d'autocertification […] 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 […]»[29].

Le groupe de travail «Article 29» note que le rôle dévolu par le bouclier au ministère américain du commerce dans le processus de certification semble se borner à vérifier que les documents sont complets. Si le groupe de travail reconnaît que l'autocertification n'implique pas systématiquement un contrôle a priori de la mise en œuvre des politiques de protection de la vie privée, le ministère du commerce devrait au minimum s'engager à vérifier systématiquement que les politiques de protection de la vie privée incluent tous les principes du bouclier. Cet engagement est mentionné dans le projet de décision d'adéquation mais n'est pas clairement identifiable dans la lettre d'observations du ministère américain du commerce[30].

Une violation des principes du bouclier de protection des données pourrait passer inaperçue pendant longtemps et n'être détectée qu'une fois qu'un grave préjudice, peut-être même irréparable, aura été porté aux droits fondamentaux de la personne concernée. Cette approche pourrait par conséquent être contraire au principe de précaution appliqué par l'Union.

Transparence assurée grâce à la liste du bouclier de protection des données et au registre des organisations radiées de la liste

D'importantes améliorations ont été apportées en ce qui concerne la transparence vis-à-vis de la personne concernée. En plus de l'ensemble des organisations américaines qui se sont autocertifiées auprès du ministère américain du commerce, la nouvelle liste du bouclier de protection des données inclura également un registre de toutes les organisations radiées de la liste, indiquant également la raison de la radiation[31]. Le site web du bouclier de protection des données publié par le ministère américain du commerce se focalisera davantage sur les publics cibles de manière à faciliter la vérification des types d'informations couverts par l'autocertification d'une organisation ainsi que la politique de protection de la vie privée applicable aux informations couvertes et la méthode utilisée par l'organisation pour contrôler son respect des principes[32]. Le groupe de travail «Article 29» se félicite de voir explicitement indiqué que le ministère américain du commerce vérifiera si les entreprises possédant un site web public ont bien publié leurs dispositions de protection de la vie privée sur ce site ou, si elles n'ont pas de site web public, le lieu où le texte de ces dispositions peut être consulté par

[29] CJUE, Schrems, point 81.
[30] Commission européenne, projet de décision d'adéquation, point 34.
[31] Annexe I, p. 5, et annexe II, section II.1; le groupe de travail «Article 29» renvoie également à la quatrième recommandation de la Commission dans la communication COM(2103)847 ainsi qu'à la lettre du groupe de travail à la vice-présidente Reding du 10 avril 2014, en particulier le point 5 de la section «Transparence».
[32] Annexe I, p. 8; le groupe de travail «Article 29» renvoie également à sa lettre à la vice-présidente Reding, en particulier le point 2 de la section «Transparence».

le public[33]. Les documents contiennent également plus d'informations sur le contenu de la politique de protection de la vie privée[34].

D'après le groupe de travail «Article 29», un problème pourrait se poser si une organisation déjà incluse dans la liste du bouclier élargit par la suite sa certification à d'autres catégories de données. La liste ne refléterait alors pas les différentes périodes d'applicabilité des principes aux différentes catégories de données et les particuliers et entreprises de l'UE risqueraient de ne pas pouvoir déterminer avec certitude si un ensemble de données spécifique est soumis aux principes du bouclier et, si oui, depuis quand. Pour éviter ce problème, le groupe de travail recommande d'ajouter, pour chaque organisation de la liste du bouclier de protection des données, une fiche spécifiant séparément pour chaque catégorie de données à caractère personnel la date d'entrée en vigueur de l'autocertification.

Le groupe de travail «Article 29» se félicite que le ministère américain du commerce tienne un registre des organisations radiées de la liste du bouclier de protection des données et que ce registre inclue une explication précisant que ces organisations ne bénéficient plus des avantages du bouclier de protection des données, mais qu'elles n'en doivent pas moins continuer d'appliquer les principes aux données à caractère personnel qu'elles ont reçues pendant la période durant laquelle elles ont été des organisations certifiées du bouclier, et ce aussi longtemps qu'elles conserveront ces informations (annexe I, p. 3). Toutefois, étant donné que certaines organisations radiées de la liste du bouclier de protection des données peuvent décider de restituer ou de supprimer les données reçues dans le cadre du bouclier, tandis que d'autres choisiront au contraire de conserver ces données, il est important de faire preuve de plus de transparence à ce sujet vis-à-vis des personnes concernées. C'est pourquoi le registre d'entreprises tenu par le ministère du commerce devrait préciser si l'organisation conserve toujours des données à caractère personnel reçues au titre du bouclier ou si elle les a restituées ou supprimées. Si l'organisation les a conservées, le registre doit alors indiquer expressément qu'elle doit continuer d'appliquer à leur égard les principes du bouclier.

En outre, le registre tenu par le ministère américain du commerce devrait mentionner que ces organisations ne bénéficient plus des avantages du bouclier de protection des données, ce qui veut dire qu'elles n'ont plus le droit de recevoir des données à caractère personnel en provenance de l'UE au titre des principes du bouclier.

Procédures de vérification

Afin de s'assurer que leur autocertification est bien effective en pratique, les organisations peuvent effectuer une autoévaluation ou un contrôle extérieur de la conformité. Le groupe de travail «Article 29» déplore que la formation des employés ne soit exigée que lorsque l'organisation opte pour une vérification via des autoévaluations (annexe II, section III.7.c). Il semblerait également que l'obligation de s'assurer que les politiques sont appropriées,

[33] Annexe I, pp. 3 et 4; le groupe de travail «Article 29» renvoie également à la première recommandation de la Commission dans la communication COM(2103)847 ainsi qu'à la lettre du groupe de travail à la vice-présidente Reding du 10 avril 2014, en particulier le point 3 de la section «Transparence».
[34] Annexe I, p. 5 et 6, et annexe II, section III.6.

complètes, affichées de façon bien visible, mises en œuvre et accessibles ne concerne que les organisations qui choisissent une évaluation interne (autoévaluation) et que le contrôle par un mécanisme externe se limite au contrôle du respect de la politique de protection de la vie privée de l'organisation.

A posteriori

Le groupe de travail «Article 29» se félicite que la FTC et le ministère américain du commerce soient investis de pouvoirs d'enquête en cas de réclamation. Le groupe de travail «Article 29» note par ailleurs que le ministère américain du commerce aura la possibilité d'effectuer des vérifications d'office, notamment en envoyant des questionnaires. Le groupe de travail «Article 29» voudrait néanmoins s'assurer que cette approche est suffisante pour satisfaire l'exigence de mise en place de mécanismes efficaces de détection et de contrôle des infractions établie par la CJUE. Le groupe de travail «Article 29» a d'ailleurs toujours des questions sur les pouvoirs exacts conférés aux autorités américaines d'application de la loi pour effectuer des contrôles sur place dans les locaux des organisations autocertifiées afin d'enquêter sur les violations du bouclier, sur la marche à suivre pour obtenir l'exequatur d'une décision d'une autorité de l'UE sur le territoire américain et sur le caractère véritablement dissuasif des sanctions prévues par le bouclier.

2.2.7 Traitements de données sur les ressources humaines

Champ d'application

Le principe complémentaire 9 (annexe II, section III.9) s'applique aux informations à caractère personnel relatives à un salarié (actuel ou ancien) rassemblées dans le cadre d'une relation de travail. D'après le texte du principe complémentaire 9.a.ii, les principes du bouclier de protection de la vie privée ne s'appliquent qu'en cas de «transfert ou d'accès à des dossiers individuels identifiés». Ce terme «dossier identifié» ne correspond pas à la définition de «données à caractère personnel» figurant à l'annexe II, section I.8.a, qui inclut «toute donnée ou information concernant une personne identifiée ou identifiable» et n'est donc pas conforme à la définition utilisée dans la directive[35].

Le principe complémentaire 9.a.ii dispose que «[l]es rapports statistiques fondés sur les données agrégées en matière d'emploi et qui ne contiennent pas de données à caractère personnel ou qui utilisent des données rendues anonymes ne présentent pas de risques pour la vie privée». Cette déclaration contredit plusieurs avis rendus par le groupe de travail «Article 29». Le groupe de travail «Article 29» voudrait souligner que les données agrégées peuvent toujours être identifiées à nouveau et qu'elles doivent donc être considérées comme des données à caractère personnel[36].

[35] Comme déjà souligné, la limitation aux dossiers ayant fait l'objet d'un «transfert» ou d'un «accès» n'est pas non plus conforme au terme «traitement» (annexe II, section I.8.b).
[36] Voir l'avis 4/2007 sur la notion de données à caractère personnel ainsi que l'avis 05/2014 sur les techniques d'anonymisation.

Notification, choix et limitation des finalités

Le principe complémentaire 9.b.i fournit un exemple d'application des principes «Notification» et «Choix» lorsque des données RH sont utilisées dans un but différent. Cet exemple concerne une organisation américaine voulant «utiliser les données à caractère personnel rassemblées dans le cadre d'une relation de travail dans un but qui n'est pas lié à cette relation de travail — par exemple l'envoi de messages de marketing». Dans ce scénario, la modification de la finalité est autorisée à condition de respecter les principes «Notification» et «Choix». Selon le groupe de travail «Article 29», le traitement ultérieur de données relatives aux ressources humaines à des fins de marketing direct doit la plupart du temps être considéré comme une finalité incompatible et donc contraire au principe de limitation des finalités (annexe II, section II.5.a). En outre, le groupe de travail «Article 29» considère que le principe «Choix» ne saurait constituer une base appropriée pour que l'employé «consente» (opposition) à un changement de finalité, dans un contexte d'emploi où ce consentement n'est pas forcément entièrement libre.

Le groupe de travail «Article 29» doute fortement que la priorité donnée par le bouclier au principe «Choix» en tant que condition d'utilisation ultérieure de données dans un but différent soit conforme aux lignes directrices de l'OCDE sur la protection de la vie privée, vu qu'il n'y a aucune garantie suffisante permettant d'empêcher que ce mécanisme d'opposition ne soit également utilisé pour des traitements ultérieurs incompatibles. Le principe complémentaire 9.b.iv prévoit une exemption large et explicite aux principes «Notification» et «Choix» «dans la mesure nécessaire et pour aussi longtemps que nécessaire, pour éviter de limiter les capacités de l'organisation dans le cadre de promotions, d'engagements ou d'autres décisions similaires relatives à l'emploi». Premièrement, l'utilisation de données relatives aux ressources humaines à ces fins devrait déjà être explicitement déclarée lors de la collecte des données. En outre, l'expression «autres décisions similaires relatives à l'emploi» est trop large et trop vague. La conséquence sera que les données relatives aux ressources humaines seront totalement exemptées des principes «Notification» et «Choix» lorsqu'elles seront traitées dans le cadre de la relation de travail. Le terme est tellement vague qu'il ne permet pas de déterminer si l'utilisation ultérieure est compatible avec la finalité initiale. Le groupe de travail «Article 29» recommande de supprimer cette exception.

Droit d'accès

Le principe complémentaire 9.e.i prévoit également une exemption à l'application du principe d'accès ou à la conclusion d'un contrat avec un responsable de traitement tiers pour les données relatives aux ressources humaines lorsque celles-ci portent sur des besoins opérationnels occasionnels liés à l'emploi, comme la réservation d'un vol ou d'une chambre d'hôtel, la couverture d'assurance ou les données à caractère personnel d'un petit nombre d'employés et pour autant que les principes «Notification» et «Choix» soient respectés. Le groupe de travail «Article 29» ne voit aucune justification raisonnable à cette exemption et recommande de supprimer ce paragraphe.

2.2.8 Produits pharmaceutiques et médicaux

Champ d'application

Le bouclier de protection des données considère que les transferts de données codées de l'Union européenne vers les États-Unis dans le cadre de produits pharmaceutiques et médicaux ne constituent pas des transferts soumis au bouclier (annexe II, section III.14.g.i). Toutefois, le transfert de données codées bénéficie d'une protection au titre de la législation européenne en matière de protection des données, ce qui signifie qu'en pratique, le bouclier de protection des données ne peut couvrir ces transferts. Le groupe de travail «Article 29» appelle la Commission européenne à indiquer explicitement que le projet de décision d'adéquation ne couvrira pas les transferts de données codées à des fins pharmaceutiques ou médicales et qu'en conséquence, ces transferts doivent être couverts par d'autres garanties, telles que les clauses contractuelles standards (ci-après «les CCS») ou les REC. Le groupe de travail «Article 29» suggère de clarifier ce point dans la décision d'adéquation finale.

Transferts à des fins de réglementation et de contrôle (annexe II, section III.14.d)

Le groupe de travail «Article 29» craint qu'au titre de ces dispositions, des données à caractère personnel relevant du contexte médical, essentiellement de nature sensible, puissent être transférées vers des autorités de réglementation aux États-Unis. Le bouclier de protection des données étant conçu pour les transferts de données entre des entités privées, il semble qu'un organisme public tel qu'une autorité de réglementation américaine ne soit pas admissible à l'autocertification au titre du bouclier, ce qui pose la question de la protection adéquate des données lors de tels transferts. Si ces derniers devaient être effectués pour des besoins réglementaires, il faudrait prendre des mesures adéquates pour garantir une protection continue des droits fondamentaux de la personne concernée de l'UE. Le groupe de travail «Article 29» souligne que le projet de décision d'adéquation n'inclut aucune constatation à ce sujet et qu'il n'a donc aucune garantie que les données sensibles des personnes concernées de l'UE bénéficieront d'une protection adéquate dans ce contexte.

Le groupe de travail note en outre qu'il ne comprend pas pourquoi la finalité «marketing» figure parmi les exemples de traitements pour la recherche scientifique future. Il est également difficile de savoir pourquoi les transferts ultérieurs vers des sites de sociétés et d'autres chercheurs (annexe II, section III.14.d) ont été placés dans la rubrique «Transferts à des fins de réglementation et de contrôle». Ces points doivent être éclaircis dans la décision d'adéquation finale.

Sécurité des produits, contrôle de l'efficacité (y compris notification des agences gouvernementales) et suivi des malades recourant à certains médicaments ou dispositifs médicaux

Le bouclier de protection des données prévoit une exemption aux principes «Notification», «Choix» «Responsabilité en cas de transfert ultérieur» et «Accès» lorsque le respect du principe interfère avec le respect des exigences réglementaires. Le projet de décision

d'adéquation ne contient aucune constatation relative à la situation dans laquelle les principes de protection de la vie privée interféreraient avec le respect des exigences réglementaires. Si le groupe de travail «Article 29» peut comprendre que la protection des enquêtes gouvernementales justifie des limitations de la notification et du droit d'accès, il ne voit aucune raison qui justifierait des exemptions aussi larges lorsque le traitement est effectué par l'organisation ou une tierce partie du secteur privé. Par exemple, les traitements des patients étant de plus en plus individualisés, une exemption aussi large aux principes de protection de la vie privée dans le cas du suivi des malades recourant à certains médicaments ou dispositifs médicaux est inacceptable puisque ce type de soin va devenir courant. Cela vaut également pour les situations dans lesquelles des données sont utilisées par des sociétés pharmaceutiques à des fins de contrôle de la sécurité ou de l'efficacité du produit (expérimentation ou vente de nouveaux médicaments).

2.2.9. Informations accessibles au public

L'exception au droit d'accès dans le cas d'informations accessibles au public et d'informations tirées de registres publics (annexe II, sections III.15.d et e) suscite des inquiétudes, car les individus qui exercent leur droit d'accès veulent savoir si un responsable de traitement particulier traite des données les concernant et aussi connaître les données traitées, afin de pouvoir contrôler le traitement de leurs données. Le groupe de travail «Article 29» a indiqué à de nombreuses reprises qu'en vertu du droit de l'Union, les personnes concernées avaient toujours le droit d'accéder à leurs données et, au besoin, d'en exiger la rectification ou la suppression si elles n'ont pas été traitées légalement ou si elles sont inexactes ou incomplètes, qu'elles aient été ou non publiées[37]. Si la demande d'accès du particulier est rejetée au motif que les données ont été obtenues auprès de sources accessibles au public ou de registres publics, le particulier n'a plus la possibilité de contrôler l'exactitude de ses données ni de vérifier que leur publication initiale était bien légale.

Le bouclier de protection des données exempte néanmoins les registres publics et les informations accessibles au public des principes «Notification», «Choix», «Responsabilité en cas de transfert ultérieur» et «Accès» (annexe II, section II.15.b). Ces exemptions semblent trop larges par rapport à la directive et suscitent des inquiétudes puisqu'elles limitent notamment les possibilités des personnes de contrôler l'exactitude de leurs données et d'en restreindre la diffusion.

2.3. Conclusions

Le groupe de travail «Article 29» reconnaît que les autorités américaines et la Commission européenne ont apporté des améliorations substantielles aux aspects commerciaux des transferts de données entre les deux continents. Compte tenu de l'analyse ci-dessus, le groupe de travail «Article 29» estime toutefois que de nombreux points du volet commercial du bouclier de protection des données nécessitent des clarifications. Il est notamment préoccupé par l'absence de principe explicite de conservation des données. Le groupe de travail

[37] Voir WP20, p. 4.

«Article 29» doute dès lors fortement que le bouclier de protection des données puisse garantir un niveau de protection substantiellement équivalent à celui de l'UE.

La décision d'adéquation doit expliciter davantage les principe «Choix» et «Limitation des finalités». Plusieurs principes restent exposés à un risque de faille, notamment les transferts ultérieurs, le mécanisme de traitement des réclamations et le traitement des données relatives aux ressources humaines et des données pharmaceutiques. Il convient en outre de préciser davantage la manière dont les principes du bouclier de protection des données seront appliqués aux sous-traitants (mandataires) de données et de veiller particulièrement à assurer une application claire et sans ambiguïté de la terminologie.

3. EXAMEN DES GARANTIES DE SECURITE NATIONALE DU PROJET DE DECISION D'ADEQUATION

3.1 Garanties et limitations applicables aux autorités de la sécurité nationale des États-Unis.

Des ingérences dans les droits fondamentaux au respect de la vie privée et à la protection des données peuvent être acceptables pour autant qu'elles puissent se justifier dans une société démocratique. Les principes de protection de la vie privée ne sont donc pas absolus et des dérogations sont possibles, mais uniquement si les garanties (essentielles) applicables sont réunies. Conformément à l'objectif d'un renforcement de la protection de la vie privée, les organisations doivent par ailleurs s'efforcer d'appliquer ces principes de manière complète et transparente, y compris en indiquant dans leurs codes de protection de la vie privée dans quels domaines les principes autorisés par le cadre juridique américain s'appliqueront de façon régulière. Pour la même raison, lorsque les principes et/ou les lois des États-Unis permettent aux organisations de faire un choix, celles-ci sont invitées à opter, dans la mesure du possible, pour le niveau de protection le plus élevé.

L'annexe II, section I.5, indique que «l'adhésion aux principes peut être limitée par a) les exigences relatives à la sécurité nationale, l'intérêt public et le respect des lois des États-Unis; 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 peut démontrer que le non-respect des principes est limité aux mesures nécessaires pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir; 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».

La question est donc de savoir si les dérogations visées à l'annexe II peuvent se justifier dans une société démocratique. Sur la base du projet de décision d'adéquation du bouclier de protection des données, la Commission a conclu que «des règles sont en place aux États-Unis, qui visent à limiter toute ingérence, pour les besoins de la sécurité nationale, dans l'exercice des droits fondamentaux des personnes dont les données à caractère personnel sont transférées de l'Union européenne vers les États-Unis dans le cadre du bouclier de protection des données

UE-États-Unis à ce qui est strictement nécessaire pour atteindre l'objectif légitime recherché»[38].

En se basant sur le cadre décrit à la section 1.2 du présent avis et en tenant compte des observations des autorités américaines et des conclusions de la Commission, le groupe de travail «Article 29» a évalué le cadre juridique en vigueur aux États-Unis, les pratiques des agences de renseignement américaines ainsi que les conditions dans lesquelles ils autorisent les ingérences dans les droits fondamentaux au respect de la vie privée et à la protection des données tels que protégés par le cadre juridique européen. Cette évaluation est basée sur l'analyse de la directive présidentielle nº 28 (PPD-28), le décret exécutif 12333 (EO12333) et les différentes bases juridiques établies par la loi sur le renseignement étranger (Foreign Intelligence Act ou FISA, sections 104, 402, 215, 501 et 702). Le groupe de travail «Article 29» s'est basé sur l'annexe VI du bouclier de protection des données, qui se compose d'une lettre préparée par le bureau du directeur du renseignement national américain (ODNI) au sujet des garanties et limitations applicables aux autorités de la sécurité nationale des États-Unis, résumant les informations qui ont été fournies à la Commission européennes au sujet des activités de renseignement d'origine électromagnétique des États-Unis.

3.2 Garantie A – Le traitement doit être conforme à la loi et reposer sur des règles claires, précises et accessibles

Selon le droit européen, toute ingérence doit respecter les lois et les politiques et procédures établies et être suffisamment claire et accessible (dans la limite de la marge discrétionnaire accordée aux différents pays), afin de donner aux citoyens une indication adéquate des circonstances et des conditions dans lesquelles les autorités publiques sont habilitées à recourir à des mesures de surveillance[39].

Le groupe de travail «Article 29» note que les activités de renseignement d'origine électromagnétique sont réalisées sur la base d'un cadre juridique accessible. Toutes les lois mentionnées à l'annexe VI (la PPD-28, la FISA, le USA FREEDOM ACT, le FOIA) sont accessibles au grand public en ligne (aux États-Unis et en dehors). L'annexe VI propose un résumé du cadre juridique en vigueur, des limitations en matière de collecte, des limitations en matière de conservation et de diffusion, du respect des exigences et de la surveillance, de la transparence et des recours. Le système juridique américain relatif aux activités de renseignement se compose de plusieurs documents différents, dont des rapports, politiques et procédures d'agences individuelles qui doivent être analysés afin de mieux comprendre la

[38] Projet de décision de la Commission conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis, considérant 75.

[39] Cour européenne des droits de l'homme, arrêt Zakharov, point 247: « La Cour a déjà eu l'occasion de dire que l'exigence de "prévisibilité" de la loi n'allait pas jusqu'à imposer aux États l'obligation d'édicter des dispositions juridiques énumérant dans le détail tous les comportements pouvant conduire à la décision de soumettre un individu à une surveillance secrète pour des motifs de "sécurité nationale". Par la force des choses, des menaces dirigées contre la sécurité nationale peuvent être de différentes natures et peuvent être imprévues ou difficiles à définir à l'avance (Kennedy, précité, § 159). La Cour a cependant également souligné que, s'agissant de questions touchant aux droits fondamentaux, la loi irait à l'encontre de la prééminence du droit, l'un des principes de base d'une société démocratique consacrés par la Convention, si le pouvoir d'appréciation accordé à l'exécutif en matière de sécurité nationale ne connaissait pas de limite. En conséquence, elle doit définir l'étendue et les modalités d'exercice d'un tel pouvoir avec une clarté suffisante – compte tenu du but légitime poursuivi – pour fournir à l'individu une protection adéquate contre l'arbitraire […].»

manière dont les activités sont réalisées, tant en théorie qu'en pratique. À cet égard, le groupe de travail «Article 29» s'est concentré sur un nombre limité de points qu'il considère essentiels.

3.2.1 Décret exécutif 12333 et directive présidentielle nº 28

La portée du décret exécutif 12333 est vaste; en principe, toutes les activités de collecte de renseignements étrangers peuvent être réalisées à la discrétion du président des États-Unis sur la base de ce décret. Toutefois, certains observateurs ont indiqué que, depuis l'introduction de la FISA, le décret exécutif 12333 ne pouvait être utilisé que pour la collecte de données hors du territoire des États-Unis. Le groupe de travail «Article 29» note que le décret exécutif 12333 fournit peu de détails concernant sa portée géographique, la mesure dans laquelle des données peuvent être collectées, conservées ou diffusées, la nature des infractions susceptibles d'entraîner une surveillance ou encore le type d'informations pouvant être collectées ou utilisées.

Le groupe de travail «Article 29» croit comprendre que la finalité première de la directive présidentielle nº 28 (PPD-28) est de définir les limites de la collecte et du traitement de données à caractère personnel, quels que soient le programme de surveillance utilisé et le lieu où les données ont été obtenues.

La PPD-28 est une directive du président des États-Unis établissant des principes de cohérence sur la base desquels la collecte de renseignements d'origine électromagnétique est autorisée et réalisée, mais elle ne constitue pas une base légale pour la collecte. La PPD-28 agit en imposant ces principes aux organismes de la communauté du renseignement afin qu'ils les appliquent dans leurs politiques et procédures. Elle s'applique aux activités de renseignement d'origine électromagnétique quel que soit l'emplacement des données au moment de leur collecte, aux États-Unis ou ailleurs. Elle s'applique donc également aux données collectées à des fins de renseignement d'origine électromagnétique lorsqu'elles sont transférées de l'UE vers les États-Unis.

En particulier, la PPD-28 indique que les activités de renseignement d'origine électromagnétique doivent être aussi adaptées aux besoins que possible[40]. En ce qui concerne l'utilisation des données, elle établit des procédures de limitation des données (y compris les conditions relatives à leur conservation et à leur diffusion), de sécurité et de consultation des données par le personnel compétent (c'est-à-dire des règles contenant des garanties limitant les risques d'abus et d'usage abusif), de qualité des données et de surveillance. Ces garanties s'appliquent quelle que soit la nationalité des personnes concernées (américaine ou étrangère).

Pendant la transmission des données vers les États-Unis, les garanties établies par la PPD-28 sont également applicables. L'annexe VI contient un engagement de l'ODNI selon lequel en cas de collecte par les services de renseignement américains de données originaires de câbles

[40] «Les activités de renseignement d'origine électromagnétique sont aussi adaptées aux besoins que possible. Pour déterminer s'il y a lieu de collecter des renseignements d'origine électromagnétique, les États-Unis doivent tenir compte de la disponibilité d'autres informations, y compris provenant de sources diplomatiques ou publiques, et privilégier la collecte par ces moyens, dans la mesure de ce qui est approprié et faisable» (article 1er, point d).

transatlantiques pendant leur transmission vers les États-Unis, cette collecte se ferait «dans le respect des limitations et garanties visées dans les présentes, y compris des exigences de la PPD-28»[41]. Le groupe de travail «Article 29» note un manque persistant de jurisprudence établie déterminant la légalité de l'interception de communications par câble, quel que soit le pays qui l'effectue. En tout état de cause, les États-Unis ne confirment ni ne démentent se servir de l'interception de communications par câble dans un but de collecte de renseignements.

La notion de «renseignement d'origine électromagnétique» n'est définie ni dans la PPD-28, ni dans un autre texte applicable.

3.2.2 Foreign Intelligence Surveillance Act

Dans l'ensemble, le texte de la FISA paraît plus clair et plus précis. Toutefois, l'interprétation d'un grand nombre de ses dispositions à la lumière de la PPD-28 et, dès lors, l'application pratique de celles-ci dépendent en grande partie de la mise en œuvre qui en est faite par les différentes agences. Si aucun rapport complet sur la mise en œuvre des nouvelles garanties n'est disponible à ce jour, les délégués américains ont informé les représentants du groupe de travail «Article 29» que la mise en œuvre des garanties de la PPD-28 avait bien été effectuée et ce, de manière homogène dans tous les services de renseignement américains.

Plus précisément, l'article 501 est relativement clair au sujet des types d'activités de renseignement pouvant être réalisées: «la présentation de tout élément matériel (y compris des livres, des enregistrements, des documents papier, ou d'autres articles)». Il est toutefois à noter que l'inclusion d'«autres articles» dans la définition de «tout élément matériel» élargit fortement la portée de cette disposition.

L'article 702, qui autorise la collecte de données auprès de ressortissants non américains dont il est raisonnable de penser qu'ils se trouvent hors des États-Unis pour se procurer des informations en matière de renseignement extérieur[42], ne contient pas autant de détails que l'article 501. En ce qui concerne sa portée, l'article 702 cible les fournisseurs de services de communications électroniques établis aux États-Unis pour la collecte de renseignements étrangers sur des individus situés en dehors des États-Unis. La définition de «renseignements étrangers» est vaste. Elle inclut entre autres «les informations relatives à une puissance étrangère ou à un territoire étranger en rapport avec la conduite des affaires étrangères des États-Unis»[43], ce qui entraîne une certaine incertitude au sujet des types d'informations pouvant concrètement être collectées.

Malgré la déclassification des documents, des rapports au Congrès et des rapports de surveillance du Conseil de surveillance du droit au respect de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board, ci-après «PCLOB»), l'application de la

[41] Annexe VI du bouclier de protection des données, lettre du bureau du directeur du renseignement national (Office of the Director of National Intelligence - ODNI) concernant les garanties et les restrictions applicables aux autorités de la sécurité nationale des États-Unis, p. 2.
[42] 50 U.S. Code § 1181a (d)(1).
[43] 50 U.S. Code § 1801 (e)(2)).

FISA, y compris sa portée et son utilisation des critères de sélection indiqués, demeure confuse et déroutante. L'utilisation des critères de sélection indiqués («sélecteurs») est mentionnée dans un rapport du PCLOB[44], mais le groupe de travail «Article 29» croit comprendre qu'elle ne correspond pas aux règles de ciblage établies par l'article 702[45]. En effet, dans la mesure où le groupe de travail «Article 29» a pu le confirmer, ces sélecteurs ne sont pas mentionnés dans des règles généralement accessibles.

3.2.3 Conclusion

Globalement, le groupe de travail «Article 29» note que les textes applicables en matière d'activités de renseignement sont disponibles en ligne et que les autorités américaines ont pris plusieurs mesures importantes en vue d'améliorer la transparence.

Le groupe de travail «Article 29» reconnaît que depuis 2013, un grand nombre de documents tels que des stratégies, des procédures, des décisions de la FISC et d'autres documents déclassifiés ont été publiés. Par ailleurs, le PCLOB a publié des rapports importants sur les activités réalisées sur la base de l'article 702 et du USA FREEDOM Act. Un rapport similaire est attendu sur les activités au titre du décret exécutif 12333.

Plusieurs annexes législatives susceptibles d'apporter des précisions sur les implications du décret exécutif sur les particuliers situés en dehors des États-Unis et les éventuelles garanties applicables sont classifiées et ne sont donc pas accessibles au public ou aux individus susceptibles d'être affectés par leur application. Les textes qui ont été déclassifiés n'apportent que peu de valeur et d'information sur les activités de renseignement.

Malgré les efforts déployés pour expliquer le fonctionnement du décret exécutif 12333 à la suite des révélations d'Edward Snowden, notamment via l'adoption de la PPD-28, l'actuelle application concrète du décret reste difficile à cerner. Le groupe de travail «Article 29» note que l'annexe VI du bouclier de protection des données ne fournit aucune information détaillée sur le fonctionnement du décret exécutif 12333.

Si le groupe de travail «Article 29» se félicite des limitations établies par la PPD-28, il estime difficile de déterminer si le cadre juridique des États-Unis en matière de surveillance est suffisamment prévisible, en d'autres termes, s'il contient «[des] indication[s] adéquate[s] sur les circonstances et les conditions dans lesquelles les autorités publiques sont habilitées à recourir à des mesures de surveillance», d'autres précisions, notamment la publication du rapport du PCLOB sur le décret exécutif 12333, étant attendues.

[44] Rapport du PCLOB sur le programme de surveillance mis en œuvre conformément à l'article 702 de la FISA, p. 32.
[45] 50 U.S. Code § 1881a (d).

3.3 Garantie B - La nécessité et la proportionnalité au regard des objectifs légitimes poursuivis doivent être démontrées

3.3.1 Directive présidentielle nº 28

La PPD-28 a introduit des limitations en ce qui concerne les finalités pour lesquelles les données à caractère personnel peuvent être utilisées et les conditions dans lesquelles ces données peuvent être diffusées, ainsi qu'en ce qui concerne les incidences de la collecte de renseignements d'origine électromagnétique, quelle que soit la base juridique utilisée.

En particulier, l'article 1er de la PPD-28 indique que les activités de renseignement d'origine électromagnétique doivent toujours être «aussi adaptées aux besoins que possible». Tout en prenant acte de cette limitation, il est difficile de déterminer si l'expression «aussi adaptées aux besoins que possible» signifie que toutes les collectes de données doivent être nécessaires et proportionnées.

La PPD-28 reconnaît à cet égard que la collecte en vrac reste autorisée «afin de détecter les menaces nouvelles ou émergentes ainsi que d'autres informations cruciales de sécurité nationale souvent dissimulées dans le vaste et complexe système des communications mondiales modernes»[46]. Le groupe de travail «Article 29» note que d'après la PPD-28, «on entend par collecte «en vrac» de renseignements d'origine électromagnétique la collecte autorisée de grandes quantités de données d'origine électromagnétique qui, pour des raisons techniques ou opérationnelles, est effectuée sans utiliser de discriminants (par exemple des identifiants ou des critères de sélection spécifiques)».

La PPD-28 impose des limites en ce qui concerne les finalités de l'utilisation des renseignements d'origine électromagnétique collectés en vrac. Les six finalités pour lesquelles les données peuvent être collectées «en vrac» incluent la lutte contre le terrorisme et les autres formes graves de criminalité (transnationale). D'après l'analyse du groupe de travail «Article 29», la limitation des finalités est très (voire trop) large pour une limitation censée être ciblée.

La PPD-28 n'a pas éliminé la possibilité de collecte indifférenciée de données à caractère personnel en vrac et l'ampleur des possibilités de collectes de ce type demeure floue et potentiellement vaste. Le groupe de travail «Article 29» remarque à cet égard qu'à l'annexe VI, l'ODNI affirme que «les activités de collecte en vrac de communications internet menées par les services de renseignement américains au travers du renseignement d'origine électromagnétique ne portent que sur une partie réduite de l'internet[47]» et souhaiterait dès lors que d'autres preuves soient fournies moyennant des mesures de transparence.

[46] PPD-28, article 2, et annexe VI du bouclier de protection des données, lettre du bureau du directeur du renseignement national (Office of the Director of National Intelligence - ODNI) concernant les garanties et les restrictions applicables aux autorités de la sécurité nationale des États-Unis, p. 3.

[47] Annexe VI du bouclier de protection des données, lettre du bureau du directeur du renseignement national américain (ODNI) sur les garanties et limitations applicables aux autorités de la sécurité nationale des États-Unis, p. 4; le groupe de travail «Article 29» renvoie à cet égard au rapport sur les conclusions des coprésidents de l'Union européenne du groupe de travail ad hoc Union européenne-États-Unis sur la protection des données à caractère personnel», indiquant que «les données

3.3.2 Foreign Intelligence Surveillance Act

Les procédures d'atténuation des articles 215 et 702 de la FISA ont été introduites afin de protéger les citoyens américains contre l'accès intrusif du gouvernement à leurs données. Ces limitations ne s'appliquent pas officiellement aux étrangers, bien que les représentants du gouvernement américain aient déclaré à de nombreuses reprises, lors de réunions privées et publiques avec les représentants du groupe de travail «Article 29», que le champ d'application des mesures d'atténuation avait depuis lors été concrètement élargi afin de couvrir tous les individus, quels que soient leur nationalité ou leur lieu habituel de résidence.

L'article 702 précise qu'une collecte autorisée doit être effectuée «conformément au quatrième amendement à la Constitution des États-Unis, en se limitant à ce qui est considéré comme conforme au principe de recherche raisonnable. À cet égard, aucune distinction n'est opérée entre les entreprises américaines et non américaines». En d'autres termes, si le quatrième amendement était appliqué à toutes les données collectées aux États-Unis, les collectes «en vrac» réalisées aux États-Unis seraient «déraisonnables» et donc anticonstitutionnelles.

Le groupe de travail «Article 29» salue la conclusion du rapport du PCLOB selon laquelle «dans les faits, les "ressortissants non américains" bénéficient également des limitations de l'accès et de la conservation exigées par les différentes procédures d'atténuation et/ou de ciblage des agences: en effet, compte tenu du coût et de la difficulté de détecter et supprimer des informations relatives aux ressortissants américains dans un vaste corpus de données, en général, l'ensemble des données est entièrement traité en respectant les normes américaines les plus strictes en matière de protection des données».

Le groupe de travail «Article 29» note également que selon les constatations du PCLOB, «le programme ne fonctionne pas en collectant des communications en vrac». Le rapport 2014 sur la transparence en matière statistique publié par l'ODNI confirme cette conclusion. En outre, selon le rapport du PCLOB, des «sélecteurs», comme par exemple une adresse e-mail ou un numéro de téléphone, sont utilisés pour cibler la surveillance[48].

Toutefois, les règles publiques correspondantes disponibles en matière de ciblage n'incluent pas de telles règles ciblées et n'ont pour but que d'éviter le ciblage de ressortissants américains ou de personnes basées aux États-Unis. Par ailleurs, les avantages qui, selon le PCLOB, s'appliquent en pratique aux ressortissants non américains ne sont ni juridiquement contraignants, ni établis par la loi, vu que la législation disponible concernant le ciblage ne prévoit pas de telles règles ciblées et ne vise qu'à éviter le ciblage de ressortissants américains ou de personnes basées aux États-Unis.

Le groupe de travail «Article 29» rappelle par ailleurs qu'aux fins de l'article 702, les «personnes» ne sont pas seulement des particuliers, mais aussi des groupes, des entités, des

---

de communications représentent une très faible partie du trafic internet mondial», étant donné que «la plus grande partie du trafic internet mondial consiste en diffusions en continu à volume élevé et en téléchargements de contenus tels que des séries télévisées, des films et des événements sportifs» (point 3.1.2 du rapport).

[48] Rapport du PCLOB sur le programme de surveillance mis en œuvre conformément à l'article 702 de la FISA, p. 32.

associations, des sociétés ou des puissances étrangères. En outre, la justification de la collecte au motif qu'«un objectif important de l'acquisition [est] d'obtenir des informations en matière de renseignement extérieur» entraîne une certaine incertitude au sujet de sa finalité et de sa nécessité. Le groupe de travail «Article 29» prend néanmoins note des informations fournies à l'annexe VI, selon lesquelles le nombre total d'individus ciblés au titre de l'article 702 en 2014 était d'environ 90 000[49]. Le premier réexamen du bouclier de protection des données sera l'occasion d'apporter d'autres preuves sur les règles relatives au ciblage.

Il n'existe à ce jour aucune jurisprudence déterminante sur la légalité de la collecte massive et indifférenciée de données et l'utilisation ultérieure de données à caractère personnel aux fins de la lutte contre la criminalité, y compris sur la détermination des circonstances dans lesquelles la collecte et l'utilisation susmentionnées sont autorisées. La CJUE devrait aborder cette question à tout le moins dans une certaine mesure en 2016, dans les affaires jointes Tele2 Sverige AB/Post- och telestyrelsen et Secretary of State for the Home Department/Davis e.a.[50] ainsi que dans l'avis qu'elle rendra sur la validité de l'accord PNR Canada[51]. Le groupe de travail «Article 29» rappelle entre-temps qu'il a toujours considéré que la collecte massive et indifférenciée de données ne saurait jamais être considérée comme proportionnée[52].

3.3.3 Conclusion

Malgré les limitations apportées par l'introduction de la PPD-28, les inquiétudes du groupe de travail «Article 29» demeurent, en particulier celles relatives à la proportionnalité de la collecte de données. Premièrement, certaines indications laissent entendre que les États-Unis continuent d'effectuer des collectes massives et indifférenciées ou, à tout le moins, n'excluent pas la possibilité de continuer de le faire à l'avenir. Le groupe de travail «Article 29» a toujours considéré que ce type de collecte de données n'était pas conforme au droit de l'Union et n'était donc pas acceptable.

Deuxièmement, le groupe de travail «Article 29» note que les traitements de données ciblés ou «aussi spécifiques que possible» peuvent tout de même être considérés comme massifs. La question de savoir si la collecte de données massive doit être autorisée ou non fait actuellement l'objet d'une procédure devant la CJUE. C'est pourquoi le groupe de travail «Article 29» n'effectuera pas d'analyse finale de la légalité des traitements ciblés, mais massifs. Il souligne néanmoins que dans le cas où les traitements de données ciblés, mais massifs seraient autorisés, les principes de ciblage devraient s'appliquer à la fois à la collecte de données et à leur utilisation ultérieure et ne peuvent être uniquement limités à l'utilisation. Quoi qu'il en soit, une clarification du projet de décision d'adéquation est nécessaire en ce qui concerne les six finalités mentionnées dans la PPD-28 pour lesquelles des données peuvent être collectées «en vrac». À ce stade, le groupe de travail «Article 29» n'est pas convaincu

[49] Annexe VI, p. 11.
[50] CJUE, affaires jointes C-203/15 et C-698/15.
[51] CJUE, affaire A-1/15
[52] WP 215 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_fr.pdf

que ces finalités soient suffisamment limitées pour garantir que la collecte de données se cantonne bien à ce qui est nécessaire et proportionné.

3.4 Garantie C - Un mécanisme de surveillance indépendant doit avoir été mis en place

Les États-Unis ne disposent pas d'un organe de surveillance unique au niveau fédéral chargé de superviser les implications des programmes de renseignement et de surveillance pour la protection de la vie privée et des données. Au contraire, les activités du renseignement américain sont soumises à un processus de surveillance à plusieurs niveaux, une distinction pouvant être opérée entre la surveillance interne et externe. Le groupe de travail «Article 29» reconnaît que les pratiques des organes de surveillance des États-Unis en matière de rapport sont très détaillées et, pour la plupart, publiques.

3.4.1 Surveillance interne

Toutes les agences de renseignement et de sécurité comptent parmi leur personnel des agents responsables de veiller au respect de leur cadre législatif, dont des inspecteurs généraux ayant pour tâche principale d'évaluer la conformité générale du travail des agences avec la législation, y compris, mais pas exclusivement, les lois relatives à la protection de la vie privée et des données. La fonction d'inspecteur général est établie par la loi. Tous les inspecteurs généraux sont (ou seront bientôt) nommés par le Président, et leur nomination entérinée par le Sénat, afin de garantir leur indépendance sur le plan organisationnel et de veiller à ce qu'ils rendent compte au Congrès. Selon le groupe de travail «Article 29», il est donc vraisemblable que les inspecteurs généraux remplissent le critère relatif à l'indépendance organisationnelle telle que définie par la CJUE et la Cour européenne des droits de l'homme (CEDH), du moins dès lors que le nouveau processus de nomination s'applique à tous. Pour le moment, il subsiste quelques inquiétudes en ce qui concerne les inspecteurs généraux qui sont toujours nommés par le directeur de l'agence qu'ils supervisent.

Les inspecteurs généraux peuvent formuler des recommandations qui peuvent ensuite être transmises au ministère de la justice et au Conseil de surveillance de la vie privée et des libertés civiles, voire même à la commission du Congrès, qui peut alors les appliquer. Lorsque l'inspecteur général constate une violation, celle-ci peut être traitée via des mesures internes et stratégiques et être notifiée au Congrès. L'inspecteur général est par exemple habilité à effectuer des audits et des inspections.

Le groupe de travail «Article 29» note que l'accès du public aux rapports des inspecteurs généraux peut être refusé et qu'un inspecteur général peut également être empêché de signaler une infraction si les informations inspectées sont classifiées. Toutefois, les rapports sont soumis en permanence au contrôle du Congrès, ce qui est une garantie essentielle, même si elle ne permet pas des recours individuels.

Toutes les agences possèdent des responsables de la vie privée et des libertés civiles qui participent au système obligatoire de notification spontanée sous le contrôle du Congrès.

Dans l'ensemble, les mécanismes de contrôle interne mis en place peuvent être considérés comme relativement solides; toutefois, pour justifier une ingérence dans les droits fondamentaux à la protection de la vie privée et des données, le contrôle doit être entièrement indépendant. Si le groupe de travail «Article 29» respecte et salue le travail des différents responsables de la vie privée et des libertés civiles, il ne peut conclure qu'ils possèdent le niveau d'indépendance requis pour agir en tant qu'autorité de contrôle indépendante.

3.4.2 Surveillance externe

La surveillance externe comprend plusieurs mécanismes de surveillance judiciaire différents, prévus par les articles 501 et 702 et relevant de la responsabilité de la Cour FISA (ci-après la «FISC»), la supervision des commissions du renseignement du Congrès et les missions confiées au PCLOB.

Le groupe de travail «Article 29» rappelle qu'idéalement, comme l'ont également déclaré la CJUE et la Cour européenne des droits de l'homme, la surveillance devrait être confiée à un juge afin de garantir l'indépendance et l'impartialité de la procédure. Jusqu'à récemment, la procédure de la FISC était une procédure non contradictoire, ne prévoyant pas la possibilité pour les particuliers de se faire entendre, ni même d'être informés de l'affaire. La procédure de la FISC reste encore aujourd'hui non contradictoire, mais à la suite de l'adoption du USA FREEDOM Act, il est possible à un *amicus curiae* d'intervenir auprès de la FISC. L'amicus curiae agit en toute indépendance, mais n'a pas pour but de défendre des personnes données susceptibles d'être impliquées dans l'affaire.

Le USA Freedom Act a créé un groupe d'*amici curiae* chargés d'informer la FISC sur les affaires importantes. La Cour a sélectionné cinq avocats ayant obtenu les habilitations de sécurité nécessaires, qui rendent des avis techniques, assistent aux audiences de la FISC, fournissent des informations et se prononcent sur le fond d'une affaire du point de vue de la protection de la vie privée et des droits civils. Toutefois, ils n'agissent ainsi que dans les affaires importantes ou lorsque de nouvelles questions juridiques sont soulevées[53].

L'article 215 est presque entièrement soumis à une surveillance judiciaire ex ante (mais pas ex post), puisque tous les programmes utilisant l'article 215 comme base pour leurs opérations de collecte sont soumis à l'approbation de la FISC. Le rapport du PCLOB précise que «l'article 702 s'écarte de ce cadre traditionnel de la surveillance électronique de la FISA, tant au niveau des normes appliquées qu'au niveau de l'absence de décisions individuelles prises par la FISC. En vertu de cette loi, le procureur général et le Directeur du renseignement national effectuent des certifications annuelles autorisant le ciblage de ressortissants non américains dont il est raisonnable de penser qu'ils se trouvent hors des États-Unis pour se procurer des informations en matière de renseignement extérieur, sans préciser à la FISC quels sont les ressortissants non américains qui seront ciblés. […] En outre, le gouvernement n'est pas tenu de démontrer qu'il a des raisons de penser qu'une cible au titre de l'article 702

[53] Freedom Act TITRE IV--RÉFORMES DU TRIBUNAL DE SURVEILLANCE DU RENSEIGNEMENT EXTÉRIEUR — article 401. Nomination d'*amici curiae*

est une puissance étrangère ou l'agent d'une puissance étrangère, comme exigé dans le cadre traditionnel de la FISA»[54].

Au sein du Congrès, les commissions du renseignement (Select Committees on Intelligence) ont également une mission de surveillance consistant à approuver les activités de renseignement, notamment via le vote du budget. Les commissions du renseignement du Sénat et de la Chambre reçoivent des briefings classifiés au sujet des activités de renseignement. Le procureur général doit rendre compte à ces commissions tous les six mois au sujet de la surveillance électronique au titre de la FISA. Le groupe de travail «Article 29» n'a pas pu déterminer avec précision la mesure dans laquelle ils peuvent discuter du traitement de données à caractère personnel d'individus, en particulier de ressortissants non américains.

Le PCLOB est une partie indépendante de l'organe exécutif du gouvernement américain, investie de deux pouvoirs fondamentaux: 1) examiner et analyser les mesures prises par le pouvoir exécutif pour protéger la nation [américaine] du terrorisme, en veillant à ce que la nécessité de ces actions soit mise en balance avec la nécessité de protéger la vie privée et les libertés civiles, et 2) veiller à ce que les questions en rapport avec la liberté soient dûment prises en compte dans l'élaboration et la mise en œuvre des lois, règlements et politiques relatifs aux efforts visant à protéger la nation du terrorisme. Le groupe de travail «Article 29» note que le PCLOB possède un pouvoir d'assignation et peut accéder aux informations classifiées. Dans l'exercice de cette fonction, il vérifie également l'efficacité des programmes. Il exerce sa surveillance non pas avant, mais après les faits. Le PCLOB a prouvé son indépendance en manifestant son désaccord avec le président des États-Unis sur des questions juridiques. Il a notamment considéré que le programme de métadonnées téléphoniques au titre de l'article 215 n'était pas autorisé par la loi et a conclu qu'il n'était pas efficace puisqu'il n'existait aucune preuve d'attaque perturbatrice. Le PCLOB a également réalisé pendant un an une étude du programme 702 et conclu qu'il était légal et manifestement autorisé par la loi et que l'article 702 s'était révélée très efficace, y compris en matière de terrorisme. Enfin, il a pris des mesures en ce qui concerne l'exigence de transparence et constaté que plusieurs faits classifiés ne devaient pas l'être. D'après les informations du groupe de travail, le PCLOB devrait prochainement rendre compte de la mise en œuvre de la PPD-28. Il considère à cet égard que pour conserver des informations sur un étranger, le seul fait qu'il s'agisse d'un étranger ne suffit pas.

Le groupe de travail «Article 29» note enfin que le décret exécutif 12333 ne prévoit aucun mécanisme de contrôle judiciaire, de surveillance ou de recours pour les programmes de surveillance mis en œuvre en son nom.

3.4.3 Conclusion

Le projet de décision d'adéquation démontre qu'une approche à plusieurs niveaux, composée de mécanismes de surveillance internes et externes, est en place aux États-Unis. Bien que le

[54] Rapport du PCLOB sur le programme de surveillance mis en œuvre conformément à l'article 702 de la FISA, pp. 24-25.

fonctionnement des mécanismes de surveillance puisse être difficile à comprendre, le groupe de travail «Article 29» est convaincu que des mécanismes suffisants de contrôle interne sont en place. Le groupe de travail «Article 29» craint toutefois que le contrôle des programmes de surveillance mis en œuvre au titre du décret exécutif 12333 soit insuffisant.

Le groupe de travail «Article 29» note que ses précédentes critiques selon lesquelles les procédures devant la FISC ne sont pas contradictoires n'ont été atténuées que dans une certaine mesure par la désignation des *amici curiae*, chargés de «défendre la protection de la vie privée et des libertés civiles». La FISC ne prévoit néanmoins aucun contrôle judiciaire effectif du ciblage de ressortissants non américains. Quelques doutes persistent également au sujet de la capacité de la FISC d'évaluer efficacement les procédures de ciblage et d'atténuation, comme l'a également souligné le PCLOB[55].

3.5 Garantie D - La personne concernée doit avoir à sa disposition des moyens de recours effectifs

3.5.1 Recours judiciaires

3.5.1.1 Exigence relative à la qualité pour agir

Le système américain des recours judiciaires contient une limitation importante: la Constitution américaine exige des individus qu'ils démontrent qu'ils ont qualité pour agir, c'est-à-dire qu'ils apportent la preuve qu'ils «ont subi ou subiront un préjudice direct et que ce préjudice est réparable. Au niveau fédéral, il n'est pas possible d'intenter une action en justice au seul motif qu'un individu ou un groupe est mécontent d'une action ou loi gouvernementale»[56]. Cette exigence semble être annulée par la non-notification des individus soumis à une surveillance même après la fin de ces mesures. La CJUE et la Cour européenne des droits de l'homme ont déclaré à de nombreuses reprises que toute personne doit pouvoir accéder à des recours administratifs ou judiciaires. La Cour européenne des droits de l'homme a confirmé dans son arrêt Zakharov qu'en vertu de la jurisprudence, toute personne pouvait saisir les tribunaux si elle avait une raison légitime de soupçonner une ingérence dans ses droits fondamentaux[57].

Par ailleurs, les étrangers se trouvant en dehors des États-Unis ne bénéficient pas d'une protection totale au titre de la constitution aux États-Unis, conformément à la jurisprudence de la Cour suprême des États-Unis[58]. C'est notamment le cas pour le quatrième amendement, qui protège les citoyens américains - mais pas les individus non américains - contre les fouilles et saisies déraisonnables et duquel est dérivé le droit américain au respect de la vie privée. Les citoyens européens et les autres résidents européens vivant en dehors des États-Unis sont tout simplement exclus de la protection du quatrième amendement[59].

---

[55] Rapport du PCLOB sur le programme de surveillance mis en œuvre conformément à l'article 702 de la FISA, p. 11.
[56] https://www.law.cornell.edu/wex/standing; https://www.law.cornell.edu/wex/standinghttps://www.law.cornell.edu/wex/standing; Clapper c. Amnesty International USA
[57] Cour européenne des droits de l'homme, Zakharov, point 171.
[58] U.S. c. Verdugo — Urquidez, p. 264-266.
[59] Rapport des coprésidents de l'Union européenne, section 2.

L'application limitée de la loi sur le recours juridictionnel (tant sur le fond, la sécurité nationale étant exclue, qu'en ce qui concerne les personnes pouvant se prévaloir de cette loi), les nombreuses exemptions et l'insécurité juridique relative aux agences auxquelles s'appliquera cette loi font que l'obligation d'offrir un mécanisme de recours effectif à toutes les personnes concernées par une affaire de surveillance du renseignement aux fins de la sécurité nationale n'est pas respectée.

3.5.1.2 Directive présidentielle nº 28

Le groupe de travail «Article 29» note que la PPD-28 n'est qu'une directive et qu'elle ne peut dès lors pas créer de droits pour les personnes. Seule la législation est source de droits. Dès lors, les personnes ne peuvent pas saisir un tribunal sur la base d'une violation alléguée des garanties de la PPD-28.

3.5.1.3 Foreign Intelligence Surveillance Act

La FISA prévoit plusieurs recours pour les personnes en cas de surveillance illégale. Selon la FISA, «toute personne lésée, autre qu'une puissance étrangère ou un agent d'une puissance étrangère […], respectivement, ayant fait l'objet d'une surveillance électronique ou dont des informations obtenues par surveillance électronique ont été divulguées ou utilisées en violation de l'article 1809 du présent titre dispose d'un droit d'action contre toute personne ayant commis la violation en question». Cette disposition exclut toutefois expressément les puissances étrangères ou les agents de puissances étrangères ayant fait l'objet de la mesure. Cependant, comme déjà indiqué, le plaignant devra démontrer qu'il a qualité pour agir, ce qui, concrètement, ne sera pas possible.

Le USA Freedom Act a créé un comité consultatif *amicus curiae* auprès de la FISA Court chargé de rendre un avis (facultatif) en cas de nouvelle interprétation juridique importante. La mission de ce comité est toutefois de donner un avis impartial, et non pas de défendre les intérêts d'une personne donnée à la demande de celle-ci.

3.5.2 Recours administratifs

3.5.2.1 Inspecteurs généraux

Une autre voie de recours consiste à s'adresser à l'inspecteur général, auprès duquel une réclamation peut être introduite. Toutefois, les inspecteurs généraux n'ont aucune obligation d'examiner toutes les réclamations: il n'y a pas de droit d'être entendu, mais plutôt un pouvoir discrétionnaire. L'inspecteur général peut également publier des rapports contenant des constatations de violations lorsque les informations sont déclassifiées. Toute personne qui s'estime affectée par un rapport serait alors en mesure de saisir la justice sur la base de la constatation de violation de la loi.

3.5.2.2. Loi pour la liberté d'information (Freedom of Information Act)

Un recours accessible à tous les individus consiste à introduire une demande d'accès à l'information au titre du Freedom of Information Act (FOIA). Selon le gouvernement américain, toute personne (qu'il s'agisse ou non d'un citoyen américain) peut introduire une demande au titre du FOIA en demandant simplement l'accès à n'importe quel dossier d'une agence. Il peut s'agir d'un dossier la concernant, bien que, dans ce cas, une preuve d'identité soit nécessaire. Toutefois, si l'information en question est classifiée dans l'intérêt de la sécurité nationale, il est peu probable que la demande soit acceptée, car une exemption existe: les agences ne sont pas tenues d'accorder l'accès aux informations classifiées, même si elles concernent l'individu qui a introduit la demande. Les informations relatives aux enquêtes d'application de la loi en cours ne peuvent pas faire l'objet d'une demande au titre du FOIA. Enfin, le groupe de travail «Article 29» croit comprendre que les demandes au titre du FOIA ne donnent pas droit à un examen de la légalité du traitement par une autorité indépendante.

3.5.3 Médiateur du bouclier de protection des données

3.5.3.1 Création d'un poste de médiateur

Le bouclier de protection des données établit un nouveau mécanisme permettant aux «particuliers de l'UE» de soumettre des demandes relatives au «renseignement américain d'origine électromagnétique» au nouveau médiateur du bouclier de protection des données. Le poste de médiateur, comme expliqué dans le mémorandum joint à la lettre du secrétaire d'État John Kerry du 22 février 2016, sera occupé par la sous-secrétaire C. Novelli. Elle assumera cette fonction en plus de son rôle de «coordinatrice principale de la diplomatie internationale en matière de technologie de l'information», créé au titre de l'article 4, point d), de la PPD-28. Cette lettre, de même que le mémorandum, souligne que «le sous-secrétaire rend compte directement au secrétaire d'État et est indépendant des services de renseignement».

Le mémorandum explique que, malgré son nom, le médiateur du bouclier de protection des données ne traitera pas uniquement les demandes concernant l'accès pour raison de sécurité nationale aux données transmises depuis l'Union européenne vers les États-Unis au titre du bouclier de protection des données, mais aussi les demandes relatives à des données transmises au titre de clauses contractuelles types, de règles d'entreprise contraignantes, de dérogations (au sens de l'article 26 de la directive 95/46/CE) ou d'«éventuelles futures dérogations» au sens de la note de bas de page 2 du mémorandum.

Le fonctionnement théorique du mécanisme peut être résumé comme suit: un particulier de l'UE introduit une demande auprès d'un organisme d'un État membre compétent en matière de surveillance des services de sécurité nationale ou d'un «organe européen de traitement des plaintes individuelles», dans le cas où un tel organe serait créé ou désigné. L'autorité transmettant la demande au médiateur doit tout d'abord s'assurer que la demande est

complète, conformément au point 3(b) de la lettre[60]. Une fois la demande transmise au médiateur du bouclier de protection des données et jugée conforme au point 3(b), le médiateur fournit une réponse confirmant de manière définitive «i) que la plainte a été correctement instruite et ii) que les lois et autres actes législatifs, ordonnances exécutives, directives présidentielles et politiques des agences des États-Unis, compte tenu des limites et garanties décrites dans la lettre du bureau du directeur du renseignement national américain (ODNI), ont été respectées ou, dans l'hypothèse inverse, que ces cas de non-respect ont été corrigés»[61]. La réponse du médiateur du bouclier de protection des données «ne confirmera ni ne démentira que la personne a fait l'objet d'une surveillance, pas plus qu'elle ne confirmera la mesure de réparation spécifique appliquée»[62]. S'agissant de la manière dont le médiateur effectue son enquête, il est expliqué que le médiateur du bouclier de protection des données «travaillera en étroite collaboration avec d'autres représentants du gouvernement américain, et notamment les organes de surveillance indépendants appropriés»[63] et, plus particulièrement, «sera en mesure d'assurer une coordination étroite avec l'ODNI, le ministère de la justice et d'autres départements et agences impliqués dans la sécurité nationale des États-Unis selon les besoins, ainsi qu'avec les inspecteurs généraux, les responsables de l'application de la loi sur la liberté de l'information et les responsables des libertés civiles et du respect de la vie privée»[64]. Grâce à cette coordination, le médiateur du bouclier de protection des données pourra envoyer une réponse incluant les confirmations décrites ci-dessus.

3.5.3.2 Examen du nouveau mécanisme de médiation

Le groupe de travail prend acte des efforts déployés par la Commission européenne et le gouvernement américain en vue de mettre en place un nouveau mécanisme destiné à améliorer les possibilités de recours en justice concernant les activités du renseignement américain. Il estime que l'évaluation de ce mécanisme, qui représente une nouveauté dans le domaine des relations internationales en ce qui concerne le renseignement d'origine électromagnétique ou la sécurité nationale, revêt une importance particulière.

Dans la présente section, le groupe de travail «Article 29» examinera la mesure dans laquelle la création du médiateur du bouclier de protection des données répond aux besoins de recours

[60] b. L'organe européen de traitement des plaintes individuelles s'assurera que la demande est complète en procédant aux actions suivantes:
i) vérifier l'identité de la personne et vérifier que la personne agit pour son propre compte, et non en qualité de représentant d'une organisation gouvernementale ou intergouvernementale;
ii) s'assurer que la demande est faite par écrit et qu'elle contient les informations de base suivantes:
• toute information constituant le fondement de la demande,
• la nature des informations ou de la réparation demandées,
• les entités du gouvernement américain dont la personne pense qu'elles sont impliquées, le cas échéant, et
• les autres mesures prises pour obtenir les informations ou la réparation demandées et les réponses obtenues à la suite de ces autres mesures;
iii) vérifier que la demande porte sur des données dont on peut raisonnablement penser qu'elles ont été transférées depuis l'Union européenne vers les États-Unis au titre du bouclier de protection des données, de clauses contractuelles types, de règles d'entreprise contraignantes, de dérogations ou d'éventuelles futures dérogations;
iv) constater qu'a priori la demande n'est pas dénuée de fondement, vexatoire ou faite de mauvaise foi.
[61] Annexe III du bouclier de protection des données, section 4.e.
[62] Annexe III du bouclier de protection des données, section 4.e.
[63] Annexe III du bouclier de protection des données, section 2.a.
[64] Annexe III du bouclier de protection des données, section 2.a.

en justice des particuliers, tels que définis par la charte, la CEDH et la jurisprudence des juridictions européennes.

3.5.3.3 La création d'un poste de médiateur est-elle suffisante à elle seule?

La première question à se poser est de savoir si la création d'un poste de «médiateur» peut être considérée comme conforme à l'article 47 de la charte - qui mentionne un recours effectif devant un tribunal impartial[65] -, à tout le moins s'il n'existe aucun autre moyen d'introduire un recours en justice. Cette question est importante étant donné que dans l'arrêt Schrems et, plus particulièrement, dans son important point 95, la CJUE fait référence à l'article 47 de la charte, et ce sans indiquer aucunement que l'article 47 est censé être interprété avec des modifications dans le contexte de mesures de surveillance. Au contraire, la CJUE avait déjà appliqué, dans l'affaire Kadi II[66], l'article 47 de la charte à des mesures de surveillance prises dans l'intérêt de la sécurité nationale et internationale[67].

La jurisprudence de la Cour européenne des droits de l'homme indique toutefois très clairement que le recours en justice devant une juridiction de droit commun n'est pas une condition permettant de considérer un mécanisme de surveillance comme conforme à l'article 8 (et l'article 13 de la CEDH)[68]. Au contraire, la Cour a précisé qu'en vertu de l'article 8 un recours devant d'autres autorités pouvait être une garantie nécessaire dans le cadre des activités de surveillance. La Cour a néanmoins des attentes élevées vis-à-vis des autres autorités apportant un recours effectif, puisqu'elle indique qu'elles doivent être «indépendant[e]s des autorités qui procèdent à la surveillance [et] investi[e]s de pouvoirs et attributions suffisants pour exercer un contrôle efficace et permanent»[69].

Dans les affaires Kennedy et Klass, la Cour européenne des droits de l'homme a apporté des explications sur ce que ces attentes pouvaient signifier dans le contexte de la surveillance secrète, lorsque la personne concernée n'est pas notifiée du traitement de ses données. Dans ces deux arrêts, la Cour a considéré que les autorités étaient indépendantes, en particulier vis-à-vis des organismes effectuant la surveillance, mais aussi vis-à-vis des instructions[70] de toute autre autorité. Plus précisément, dans l'affaire Kennedy, la Cour a donné raison à une autorité impartiale et indépendante qui avait adopté ses propres règles de procédure et dont les membres exerçaient de hautes fonctions judiciaires ou étaient des avocats expérimentés[71].

---

[65] Elle a également déclaré, dans ses explications relatives à la charte des droits fondamentaux, que l'article 47 devait être interprété comme apportant une garantie au droit à un recours effectif devant un tribunal (explications relatives à la charte des droits fondamentaux, explication de l'article 47 (2007/C 303/02)).

[66] Affaires jointes C-584/10 P, C-593/10 P et C-595/10 P, Commission européenne et Royaume-Uni/Kadi, 18 juillet 2013

[67] Kadi II, points 97 et 100: tous les actes de l'Union, y compris ceux destinés à mettre en œuvre les résolutions adoptées par le Conseil de sécurité au titre du chapitre VII de la Charte des Nations unies, sont soumis à un examen de leur licéité par les juridictions de l'Union européenne (le chapitre VII traite de l'action en cas de menace contre la paix, de rupture de la paix et d'actes d'agression).

[68] L'article 13 de la CEDH oblige les États membres à veiller à ce que «toute personne dont les droits et libertés (…) ont été violés a droit à l'octroi d'un recours effectif devant une instance nationale». Cette instance ne doit pas obligatoirement être une autorité judiciaire, comme la Cour européenne des droits de l'homme l'a précisé aux points 56 et 67 de l'arrêt Klass.

[69] Voir l'arrêt Klass, points 56 et 67.

[70] Cour européenne des droits de l'homme, Klass, points 21 et 53.

[71] La Commission G 10 comptait (au moment de l'arrêt) trois membres, dont le président, qui devait avoir les qualifications requises pour accéder à la magistrature (voir l'arrêt Klass, points 21 et 53).

Lors de leur examen des plaintes introduites par des particuliers, les autorités concernées dans les deux affaires avaient en outre accès à toutes les informations pertinentes, y compris les documents confidentiels. Enfin, toutes deux étaient habilitées à remédier aux manquements[72].

Outre la question de savoir si le médiateur peut être considéré comme un «tribunal», l'application de l'article 47, paragraphe 2, de la charte soulève une autre question, vu que cet article dispose que le tribunal doit être «établi par la loi». Toutefois, il est douteux qu'un mémorandum spécifiant le fonctionnement d'un nouveau mécanisme puisse être considéré comme une «loi».

Dès lors - et en gardant à l'esprit le principe d'équivalence substantielle -, au lieu de se demander si un médiateur peut être formellement considéré comme un tribunal établi par la loi, le groupe de travail a décidé d'analyser les nuances établies par la jurisprudence en ce qui concerne les critères spécifiques à satisfaire pour qu'un «recours en justice» soit considéré comme conforme aux droits fondamentaux consacrés aux articles 7, 8 et 47 de la charte et à l'article 8 (et 13) de la CEDH. Dans la suite de son examen, concernant le champ d'application du nouveau mécanisme, le groupe de travail se concentrera dès lors sur les critères suivants: l'obligation de soumettre une demande au médiateur et de recevoir une réponse («qualité pour agir»), l'indépendance du médiateur, ses pouvoirs d'enquête lui permettant d'accéder aux documents nécessaires, y compris ceux qui sont classifiés, et de demander l'assistance d'autres agences et, enfin, sa capacité de remédier aux manquements.

3.5.3.4 Champ d'application du mécanisme de médiation

En ce qui concerne l'accès au mécanisme de médiation, le groupe de travail «Article 29» considère que toutes les personnes soumises au droit de l'Union devraient être couvertes par les garanties offertes au titre du bouclier de protection des données. Il ne serait pas acceptable d'opérer une distinction fondée sur la nationalité, surtout compte tenu du fait que les droits fondamentaux dans l'UE s'appliquent à tous les individus, et non pas uniquement à ceux qui détiennent un passeport de l'UE. L'annexe III mentionne un «particulier de l'UE» sans préciser davantage ce que cette expression recouvre. Le groupe de travail regrette cette imprécision et suggère d'apporter une clarification en indiquant que toutes les personnes soumises au droit de l'Union ont le droit de voir leur demande adressée au médiateur traitée conformément aux conditions du mémorandum. Par ailleurs, la Commission et les États-Unis doivent déterminer la mesure dans laquelle le bouclier de protection des données s'appliquera également aux citoyens/résidents des pays de l'EEE et de la Suisse qui, par le passé, étaient également couverts par le mécanisme de la sphère de sécurité.

Le groupe de travail «Article 29» constate en outre un certain flou au sujet du champ d'application du mécanisme de médiation. Si le mémorandum indique que le médiateur est compétent en matière de traitement des demandes relatives aux transferts, aux fins de la sécurité nationale, de données transmises depuis l'UE vers les États-Unis au moyen de tous les outils de transfert disponibles en vertu du droit de l'UE, il mentionne tout aussi clairement

[72] Cour européenne des droits de l'homme, Kennedy, point 167; Klass, points 21 et 53.

l'établissement d'un mécanisme «concernant le renseignement d'origine électromagnétique». Ce terme laisse entendre que les seuls transferts de données couverts sont ceux pour lesquels les données ont été collectées par le biais du renseignement d'origine électromagnétique, ce qui soulève la question de savoir si les données collectées au titre de la FISA, par exemple, sont considérées comme des «renseignements d'origine électromagnétique». Cela semble être le cas en ce qui concerne l'article 702, comme expliqué dans la déclaration de l'ODNI, p. 10[73]. Le groupe de travail «Article 29» regrette néanmoins que l'utilisation du terme «renseignement d'origine électromagnétique» engendre une incertitude inutile dans ce contexte.

Une autre conséquence est que, d'après ce que le groupe de travail croit comprendre, le mécanisme de médiation ne couvre pas les demandes relatives à l'accès par les agences d'application de la loi[74]. Si c'est bien le cas, il reste à déterminer si les demandes de certaines agences, notamment la CIA, seraient couvertes par le mécanisme.

3.5.3.5 «Qualité pour agir» et procédure de demande

Il est très difficile de saisir les tribunaux de droit commun aux États-Unis contre des mesures de surveillance du gouvernement américain. Le groupe de travail est au courant que la Cour suprême a refusé d'accorder la qualité pour agir dans des affaires de renseignement, lorsque le plaignant n'était pas en mesure de démontrer un «préjudice concret, caractérisé et réel ou imminent»[75]. La création du poste de médiateur constitue à cet égard une étape importante, puisqu'elle ajoute la possibilité d'une certaine forme de recours en justice qui n'existerait pas autrement. Le groupe de travail se félicite dès lors de la clarification apportée à la section 3(c). Sur la base de cette section, il n'est pas nécessaire de démontrer que les données du demandeur ont bien été consultées via des activités de renseignement électromagnétique pour introduire une demande au titre du nouveau mécanisme.

Le groupe de travail approuve en grande partie la procédure d'identification du plaignant prévue dans le cadre du mécanisme de médiation. Il est parfaitement logique que cette identification ait lieu sur le territoire de l'UE, comme c'est également le cas pour le mécanisme d'accès prévu par l'accord TFPT2 entre l'UE et les États-Unis. Le groupe de travail ne comprend toutefois pas pourquoi la vérification dans l'UE devrait être effectuée par les «autorités de contrôle chargées, dans les États membres, de la surveillance des services de sécurité nationale». Premièrement, il semble peu probable, en vertu de l'article 4, paragraphe 2, du traité sur l'Union européenne, que la Commission européenne soit en mesure d'assigner à ces organes des missions qui relèvent manifestement de la compétence des États membres.

En outre, compte tenu de la variété de mécanismes de surveillance des services de sécurité nationale des États membres, l'implication des autorités correspondantes pourrait sérieusement nuire à l'efficacité du système pour les citoyens des États membres. C'est le cas,

[73] Annexe VI du bouclier de protection des données, p. 10.
[74] Mémorandum relatif à la création d'un poste de médiateur, p. 1.
[75] Clapper c. Amnesty International USA, 568 U.S. ___ (2013) II., p. 10.

par exemple, lorsque plusieurs autorités sont chargées de la surveillance des services de sécurité nationale et qu'il peut s'avérer difficile pour le particulier de déterminer celle qui est pertinente, lorsque les règles juridiques nationales applicables ne prévoient pas la possibilité pour les particuliers d'entrer en contact avec l'organe de surveillance en question ou lorsque ces autorités ne sont pas établies de manière à être en mesure d'effectuer les tâches qui leur sont imposées dans le projet de décision d'adéquation[76]. Compte tenu de l'implication des APD dans l'application et la supervision du bouclier de protection des données ainsi que de leur rôle similaire dans le cadre de l'accord TFTP2, il est plus logique d'attribuer ce rôle aux autorités nationales de protection des données des États membres. Le groupe de travail souligne qu'il estime peu probable que des informations classifiées soient traitées dans le cadre d'une procédure devant le médiateur du bouclier de protection des données, vu que toute réponse ne serait que: «conforme ou non conforme, mais corrigé».

3.5.3.6 Indépendance

Les déclarations du secrétaire d'État indiquent clairement que le poste de médiateur sera occupé par un sous-secrétaire du département d'État. Celui-ci sera nommé par le Président et sa nomination devra être entérinée par le Sénat. Le rôle de médiateur ne nécessite pas de confirmation supplémentaire; l'attribution du poste suffit. Le sous-secrétaire est nommé par le Président des États-Unis, il agit en tant que médiateur sous la direction du secrétaire d'État et son rôle de sous-secrétaire est confirmé par le Sénat américain. Comme le soulignent les déclarations figurant dans la lettre et le mémorandum, le médiateur est «indépendant des services de renseignement américains». Le groupe de travail «Article 29» se demande néanmoins si le poste de médiateur est créé au sein du département le plus approprié. En effet, il semble nécessaire de posséder quelques connaissances et une certaine compréhension des services de renseignement pour assumer efficacement le rôle de médiateur; parallèlement, une distance suffisante avec les services de renseignement est également nécessaire pour agir en toute indépendance.

Le bouclier de protection des données n'établit pas de critères spécifiques pour le licenciement du médiateur. Le groupe de travail en déduit donc que le médiateur peut être licencié en tant que médiateur de la même manière qu'il peut être licencié en tant que sous-secrétaire du département d'État, ce qui pourrait compromettre son indépendance.

De prime abord, la désignation d'un sous-secrétaire du département d'État comme médiateur est manifestement différente, en ce qui concerne l'indépendance, de la détermination de la compétence d'un tribunal de droit commun pour le recours juridique d'un individu. La question est donc de savoir si le médiateur peut être considéré, sur le plan de son indépendance, comme étant égal aux autres organes de surveillance indépendants qui ont été jugés conformes. En matière de surveillance, il s'agit notamment de l'Investigatory Powers Tribunal (IPT) au Royaume-Uni et de la Commission G 10 en Allemagne.

[76] Par exemple, dans certains États membres de l'UE, les particuliers ne peuvent obtenir l'accès aux informations détenues par les services de sécurité nationale qu'en s'adressant à une haute cour de justice.

Lorsque la réponse est positive, il convient d'analyser également les pouvoirs conférés au médiateur «indépendant».

3.5.3.7 Pouvoirs d'enquête

Dans l'affaire Kadi II, la CJUE a jugé, en se basant sur l'article 47 de la charte, que «l'intéressé [devait pouvoir] connaître les motifs sur lesquels est fondée la décision prise à son égard soit par la lecture de la décision elle-même, soit par une communication de ces motifs faite à sa demande, sans préjudice du pouvoir du juge compétent d'exiger de l'autorité en cause qu'elle les communique, afin de lui permettre de défendre ses droits dans les meilleures conditions possibles»[77]. Les juridictions de l'Union européenne doivent veiller à ce que la décision soit prise sur une base factuelle suffisamment solide[78]. L'arrêt Kadi II indique clairement que «le secret ou la confidentialité [des] informations ou éléments» ne constitue pas une objection valable, à tout le moins devant les juridictions de l'Union européenne[79]. Le groupe de travail en conclut donc qu'afin de répondre aux exigences de la CJUE le médiateur doit recevoir les informations et des éléments de preuve étayant les motifs invoqués pour l'adoption d'une mesure[80].

L'étendue des pouvoirs d'enquête du médiateur n'est pas encore bien définie. Le projet de décision de la Commission et l'annexe III du département d'État sont tous deux avares de détails sur ce point. D'après ce que le groupe de travail comprend, le médiateur est censé recevoir suffisamment d'informations pour pouvoir indiquer si une opération de traitement de données effectuée par les services de sécurité est conforme à la loi et, dans le cas contraire, pour pouvoir remédier à la situation. Toutefois, ni la lettre du département d'État, ni le projet de décision de la Commission ne précise si le médiateur disposera d'un accès direct aux données détenues au sujet de la personne concernée et pourra donc mener sa propre enquête, ou s'il devra se contenter des rapports d'autres agents du gouvernement américain.

3.5.3.8 Pouvoirs de réparation

Il reste difficile de savoir, sur la base du mémorandum, par quels moyens le médiateur pourra ordonner la réparation de la non-conformité. En outre, si l'on y ajoute le manque de clarté relatif aux pouvoirs d'enquête, il est tout aussi difficile de déterminer dans quelle mesure le médiateur pourra effectivement ordonner la réparation des non-conformités et quel sera le résultat d'une telle initiative. Cela pourrait-il signifier que les données obtenues de manière non conforme (c'est-à-dire illégalement) ne peuvent plus être utilisées dans d'autres procédures et doivent être supprimées?

Le groupe de travail croit également comprendre que le bouclier de protection des données ne prévoit aucun recours contre la «décision» du médiateur, ni réexamen de celle-ci.

[77] Kadi II, point 100.
78 Kadi II, point 119.
79 Kadi II, point 125.
[80] Kadi II, point 122; bien que l'autorité concernée ne soit pas tenue de produire toutes les informations et éléments de preuve étayant les motifs d'une mesure.

Enfin, s'agissant de la communication du médiateur au plaignant après examen d'une plainte, le médiateur ne peut pas divulguer l'éventuelle existence d'un comportement illicite de la part des services de renseignement. La réponse donnée sera toujours la même et elle devra rester générique. Dans l'affaire Kadi II, la CJUE a jugé que l'autorité compétente (en tant qu'organe de surveillance) avait une obligation de motivation en toutes circonstances, bien que l'article 296 TFUE n'exige pas de réponse détaillée[81].

3.5.4 Conclusion

L'existence de recours effectifs pour les particuliers reste un sujet de préoccupation pour le groupe de travail «Article 29». Premièrement, le projet de décision d'adéquation n'apporte aucune réponse claire à la question de savoir dans quelles situations et dans quelles conditions préalables un particulier peut saisir un tribunal afin de connaître ses droits.

Le groupe de travail «Article 29» reconnaît et salue l'introduction d'un mécanisme de règlement alternatif sous la forme du médiateur, qui représente une décision unique dans le cadre des relations entre l'UE et un pays tiers. Indépendamment de la nécessité de clarifier le terme «particuliers de l'UE», comme déjà indiqué, le mécanisme offre à ceux-ci un moyen supplémentaire pour demander réparation auprès de l'administration américaine afin de veiller à ce que toutes les données à caractère personnel du demandeur soient traitées conformément au droit américain.

Parallèlement, le groupe de travail «Article 29» a constaté d'importantes lacunes lors de son examen du mécanisme de médiation sur la base des normes établies par l'article 47 de la charte en matière d'établissement d'un tribunal indépendant et des exigences spécifiées par la CJUE et la Cour européenne des droits de l'homme dans leur jurisprudence relative aux affaires de surveillance. Premièrement, il n'est pas évident de déterminer si le médiateur peut être considéré comme étant (formellement et pleinement) indépendant, en particulier compte tenu de la facilité relative avec laquelle les personnes faisant l'objet d'une nomination politique peuvent être révoquées. Deuxièmement, des doutes persistent au sujet de la capacité du médiateur d'exercer un contrôle efficace et permanent. Le groupe de travail «Article 29» ne peut, sur la base des informations disponibles à l'annexe III, conclure que le médiateur disposera systématiquement d'un accès direct à l'ensemble des informations, dossiers et systèmes informatiques nécessaires pour effectuer sa propre évaluation, ni qu'il pourra réellement contraindre les agences de renseignement compétentes à mettre fin aux éventuels traitements de données non conformes, en cas de désaccord sur la conformité ou non du traitement avec la loi. Un éclaircissement sur la position et les pouvoirs du médiateur pourrait éventuellement dissiper les doutes du groupe de travail «Article 29».

3.6 Conclusions sur les garanties et limitations applicables aux autorités de la sécurité nationale des États-Unis

Tout d'abord, le groupe de travail «Article 29» félicite la Commission et les autorités américaines pour tous les efforts qu'elles ont déployés pour accroître la transparence au sujet

[81] Kadi II, point 116.

des incidences éventuelles des programmes de surveillance américains sur les données transférées au titre du bouclier de protection des données - ou de tout autre outil de transfert. Des mesures considérables ont été prises depuis les premières révélations d'Edward Snowden en juin 2013. Le groupe de travail «Article 29» note néanmoins que certaines inquiétudes subsistent et qu'il serait au moins nécessaire d'apporter de plus amples explications et des éclaircissements au sujet des droits et obligations au titre du bouclier de protection des données.

Les deux grandes inquiétudes du groupe de travail «Article 29» portent sur le fait que les autorités américaines n'excluent pas totalement la possibilité de poursuivre la collecte massive et indifférenciée de données et sur le fait que les pouvoirs et la position du médiateur n'ont pas été définis plus en détail. Par ailleurs, les APD nationales devraient être habilitées à introduire une procédure auprès du médiateur au nom d'un individu, au lieu d'attribuer cette tâche aux organes de surveillance des agences de renseignement. En outre, bien que le groupe de travail «Article 29» reconnaisse pleinement les efforts entrepris pour répondre aux inquiétudes soulevées par les APD, d'autres garanties seraient bienvenues pour s'assurer que toute éventuelle ingérence des programmes de surveillance américains est réellement nécessaire dans une société démocratique.

4. EXAMEN DES GARANTIES APPORTEES PAR LE BOUCLIER DE PROTECTION DES DONNEES EN MATIERE D'APPLICATION DE LA LOI

4.1 Introduction

En ce qui concerne l'accès du public aux données à caractère personnel aux fins de l'application de la loi, le groupe de travail «Article 29» note que les principes de protection de la vie privée inclus à l'annexe II du bouclier de protection des données contiennent une dérogation identique à celle établie dans les principes de la sphère de sécurité relatifs à la protection de la vie privée. Le caractère général de la dérogation a donc été maintenu, ce qui veut dire que les nouveaux principes du bouclier de protection des données permettent les ingérences dans les droits fondamentaux des personnes dont les données à caractère personnel sont transférées depuis l'Union européenne vers les États-Unis au motif d'«exigences relatives à la sécurité nationale et à l'intérêt public ou [de] la législation interne des États-Unis»[82].

L'une des principales critiques formulées par la Cour dans l'arrêt Schrems à l'égard de la décision relative à la sphère de sécurité était toutefois que celle-ci «ne comporte aucune constatation quant à l'existence, aux États-Unis, de règles à caractère étatique destinées à limiter les éventuelles ingérences dans les droits fondamentaux des personnes dont les données sont transférées depuis l'Union vers les États-Unis».

Le groupe de travail «Article 29» salue donc les efforts entrepris par l'administration américaine pour expliciter davantage le cadre juridique en ce qui concerne l'ingérence dans

[82] Arrêt Schrems, point 87.

les données à caractère personnel transférées au titre du bouclier de protection des données à des fins d'application de la loi, y compris les limitations et garanties applicables. Parallèlement, le groupe de travail «Article 29» souligne qu'il s'agit de la question de l'accès du public, sachant que dans une société démocratique, toute ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel doit pouvoir se justifier. Le groupe de travail «Article 29» a donc analysé les garanties apportées par le bouclier de protection des données en matière d'application de la loi en utilisant le cadre présenté à la section 1.2 du présent avis.

4.2 Application des garanties essentielles européennes à l'accès des autorités répressives aux données détenues par les sociétés

4.2.1 L'accès des autorités d'application de la loi aux données à caractère personnel doit être conforme à la loi et reposer sur des règles claires, précises et accessibles

L'annexe VII du bouclier de protection des données contient une lettre du ministère américain de la justice proposant «un bref aperçu des principaux outils d'enquête utilisés pour obtenir des données commerciales et d'autres informations auprès de sociétés aux États-Unis à des fins de répression pénale ou d'intérêt public (civil et réglementaire), y compris les limitations d'accès qui accompagnent ces pouvoirs».

Toutes les procédures mentionnées à l'annexe VII découlent soit directement de la Constitution américaine (quatrième amendement), soit du droit écrit et procédural, soit des lignes directrices et politiques du ministère de la justice. L'annexe VII ne fait toutefois pas spécifiquement référence à toutes les lois qui prévoient ces procédures, mais consiste essentiellement en une brève description des procédures elles-mêmes. L'annexe VII indique également qu'«il existe d'autres bases juridiques permettant aux sociétés de contester des demandes de données émanant d'agences administratives, en fonction de leur secteur d'activité et du type de données en leur possession», en donnant plusieurs exemples non exhaustifs tels que la loi sur le secret bancaire (Bank Secrecy Act), la loi sur l'impartialité des rapports de solvabilité (Fair Credit Reporting Act) ou la loi sur le droit à la confidentialité financière (Right to Financial Privacy Act).

Le groupe de travail «Article 29» note que le cadre de lois, de procédures et de politiques est fragmenté et que la base juridique applicable à une demande d'accès donnée dépendra de la nature des données demandées, de la nature de la société, de la nature des procédures judiciaires (pénales, administratives et en rapport avec d'autres intérêts publics) ainsi que de la nature de l'entité demandant l'accès.

À partir du moment où toutes les règles applicables pour limiter l'accès des autorités répressives aux données transférées au titre du bouclier de protection des données sont basées sur la Constitution, sur le droit écrit et sur les politiques transparentes du ministère de la justice, le groupe de travail tient compte d'une présomption d'accessibilité de ces règles. Toutefois, la clarté et la précision des règles ne peuvent être évaluées que pour chaque type de procédure et chaque demande d'accès. Le groupe de travail «Article 29» constate donc à

regret que, sur la base des informations disponibles à l'annexe VII du bouclier de protection des données et des conclusions du projet de décision, cet examen ne peut être effectué actuellement.

4.2.2 La nécessité et la proportionnalité au regard des objectifs légitimes poursuivis doivent être démontrées

Le groupe de travail «Article 29» prend bonne note du fait qu'une demande d'accès à des données à des fins d'application de la loi peut être considérée comme répondant à un objectif légitime. Par exemple, l'article 8, paragraphe 2, de la CEDH autorise l'ingérence d'une autorité publique dans le droit à la protection de la vie privée pour autant qu'elle soit «nécessaire […] à la sûreté publique […], à la défense de l'ordre et à la prévention des infractions pénales». Toutefois, ces ingérences ne sont acceptables qu'à condition d'être nécessaires et proportionnées[83].

Selon la jurisprudence constante de la CJUE, le principe de proportionnalité exige que les mesures législatives proposant des ingérences dans les droits à la protection de la vie privée et à la protection des données à caractère personnel soient «aptes à réaliser les objectifs légitimes poursuivis par la *réglementation en cause* et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs»[84] (caractères italiques ajoutés). L'évaluation de la nécessité et de la proportionnalité est donc toujours réalisée par rapport à une mesure spécifique envisagée par la législation.

Les autorités américaines précisent à l'annexe VII que les procureurs fédéraux et les enquêteurs fédéraux peuvent obtenir l'accès à des documents et à d'autres informations auprès d'organisations en utilisant «plusieurs types de procédures juridiques contraignantes, dont des citations à comparaître devant un grand jury ("*grand jury subpoenas*"), des injonctions administratives et des mandats de perquisition» et peuvent obtenir d'autres communications «grâce aux pouvoirs fédéraux relatifs aux écoutes téléphoniques et aux enregistreurs graphiques»[85]. En outre, les agences investies de responsabilités civiles et réglementaires peuvent adresser des injonctions aux organisations afin d'accéder à des «documents commerciaux, à des informations électroniques ou à d'autres éléments tangibles»[86]. L'annexe VII indique également que ces procédures judiciaires servent généralement à obtenir des informations auprès de «sociétés» aux États-Unis, qu'elles soient ou non certifiées au titre du cadre du bouclier de protection des données et «sans distinction de nationalité de la personne concernée». En d'autres termes, il semble que les sujets de ces protections soient les organisations, et non pas les personnes elles-mêmes.

[83] Voir le document de travail relatif aux garanties essentielles européennes, pp. 7-9. Pour une analyse générale des notions de nécessité et de proportionnalité, voir «l'avis 01/2014 du groupe de travail «Article 29» sur la protection des données en ce qui concerne l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif», 27 février 2014.
[84] Digital Rights Ireland, point 46, et jurisprudence citée.
[85] Annexe VII, p. 2.
[86] Annexe VII, p. 4.

En plus de l'annexe VII, le projet de décision - basé sur les principes du bouclier de protection des données - contient des conclusions de la Commission relatives à l'existence, aux États-Unis, de règles visant à limiter les entraves aux droits fondamentaux des personnes dont les données personnelles sont transférées de l'UE vers les États-Unis au titre du bouclier de protection des données.

En particulier, les conclusions du projet de décision mentionnent les limitations et garanties applicables au titre du quatrième amendement de la Constitution américaine, en vertu duquel les perquisitions et saisies effectuées par les autorités répressives nécessitent essentiellement un mandat délivré par un tribunal sur la base d'une présomption sérieuse[87]. Elles évoquent également le fait que, dans les cas exceptionnels où l'exigence de mandat ne s'applique pas, l'application de la législation est soumise à une mesure du caractère raisonnable[88].

Les conclusions n'indiquent cependant pas clairement la manière dont ces garanties s'appliquent aux ressortissants non américains. Le projet de décision reconnaît en fait dans un considérant que «la protection au titre du quatrième amendement ne s'applique pas aux personnes non américaines qui ne résident pas aux États-Unis»[89]. On relève également dans les mêmes paragraphes du projet de décision que les ressortissants non américains «bénéficient indirectement de la protection accordée aux entreprises américaines qui détiennent les données à caractère personnel et qui sont les destinataires des demandes de mesures d'exécution». Le groupe de travail «Article 29» constate toutefois à regret que cette conclusion ne contient aucune référence à une source de droit (droit écrit ou jurisprudence).

Dans l'ensemble, le groupe de travail «Article 29» remarque que le système d'outils d'enquête utilisés pour obtenir des données commerciales et d'autres informations auprès de sociétés aux États-Unis à des fins de répression pénale ou d'intérêt public - ainsi que les limitations d'accès et garanties - constitue un ensemble complexe de mesures. Il est impossible d'effectuer, sur la base des informations disponibles, une évaluation générale de ce système. Une analyse spécifique de chaque cas est nécessaire pour véritablement évaluer la nécessité et la proportionnalité des mesures d'enquête prises par les services répressifs en ce qui concerne les droits fondamentaux à la protection de la vie privée et à la protection des données.

4.2.3 Un mécanisme de surveillance indépendant doit avoir été mis en place

Le groupe de travail «Article 29» prend bonne note du fait que la plupart des procédures décrites à l'annexe VII présupposent l'adoption d'une décision par un tribunal avant que les autorités ne puissent accéder aux données (p.ex. une ordonnance judiciaire pour les enregistreurs graphiques et dispositifs de traçage, une ordonnance judiciaire pour la surveillance conformément à la loi fédérale relative aux écoutes téléphoniques ou un mandat de perquisition - règle 41). Il semblerait toutefois que l'implication préalable d'un tribunal ne soit pas toujours nécessaire. Par exemple, les autorités civiles et réglementaires «peuvent

[87] Projet de décision d'adéquation, considérant 107.
[88] Bouclier de protection des données, article 107.
[89] Projet de décision d'adéquation, considérant 108.

adresser des injonctions»[90]. Il est alors possible d'effectuer un contrôle juridictionnel ex post du caractère raisonnable de l'injonction, puisque «le destinataire d'une injonction administrative peut contester l'exécution de celle-ci devant un tribunal»[91].

Sur la base des informations disponibles, le groupe de travail «Article 29» note qu'en ce qui concerne l'accès des autorités répressives aux données détenues par des entreprises aux États-Unis, un mécanisme de surveillance relativement solide et indépendant semble être en place.

4.2.4 La personne concernée doit avoir à sa disposition des moyens de recours effectifs

Comme déjà indiqué, «la protection au titre du quatrième amendement ne s'applique pas aux personnes non américaines qui ne résident pas aux États-Unis»[92], ce qui signifie qu'un ressortissant non américain ne pourrait pas contester un mandat de perquisition ou une injonction devant un tribunal en invoquant le quatrième amendement. Le projet de décision d'adéquation précise que les ressortissants non américains bénéficient indirectement de la protection accordée aux entreprises américaines qui détiennent les données à caractère personnel et qui sont les destinataires des demandes de mesures d'exécution. Le groupe de travail «Article 29» note toutefois que même si cette protection était effective, cela ne signifierait pas que les particuliers disposent de recours effectifs, vu que dans ce scénario le sujet du droit à un recours effectif semble être l'entreprise recevant la demande d'accès, et non pas le particulier dont les données sont en cause.

L'annexe VII ne contient pas d'informations supplémentaires concernant les recours mis à disposition des ressortissants non américains par le droit écrit lorsque des autorités ou des entreprises fournissent ou obtiennent illégalement un accès au contenu de leurs données.

Le groupe de travail «Article 29» se félicite que la loi sur le recours juridictionnel (Judicial Redress Act)[93], récemment adoptée, accorde des droits aux ressortissants non américains en matière de recours judiciaire. Ces droits se limitent toutefois à certains motifs de recours clairement définis: le droit d'obtenir la rectification de ses données, l'accès à celles-ci et le remboursement de ses honoraires d'avocat lorsqu'une «agence fédérale donnée ou un élément de celle-ci» refuse la modification des données ou l'accès à celles-ci, ainsi que le droit d'obtenir réparation au civil en cas de divulgation «délibérée ou volontaire» de données.

En outre, la jurisprudence américaine mentionnée aux notes de bas de page des considérants pertinents du projet de décision, en particulier les arrêts City of Ontario v. Quon[94], Maryland v. King[95] et Samson v. California[96], est dénuée de pertinence s'agissant de déterminer si des ressortissants non américains ont le droit de saisir un tribunal pour contester la licéité d'une

[90] Annexe VII, p. 4.
[91] Annexe VII, p. 4.
[92] Projet de décision d'adéquation, considérant 108.
[93] Judicial Redress Act, 2015, H.R. 1428.
[94] *City of Ontario, Cal., v. Quon*, 130 S. Ct. 2619, 2630 (2010).
[95] *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).
[96] *Samson v. California*, 547 U.S. 843, 848 (2006).

intrusion dans leur vie privée[97]. Toutes ces affaires portent sur le droit de citoyens américains au respect de leur vie privée et toutes incluent une décision de la Cour suprême des États-Unis qui limite l'application du quatrième amendement.

Dans l'ensemble, le groupe de travail «Article 29» prend acte et se félicite de l'adoption de la loi sur le recours juridictionnel, mais conserve ses doutes sur le fait que des recours effectifs soient réellement disponibles pour les différentes personnes concernées.

4.3 Conclusions

Le groupe de travail «Article 29» reconnaît et salue les efforts entrepris par l'administration américaine pour expliciter davantage le cadre juridique concernant l'ingérence dans les données à caractère personnel transférées au titre du bouclier de protection des données UE-États-Unis à des fins d'application de la loi, y compris les limitations et garanties applicables.

Le groupe de travail «Article 29» observe que le système d'outils d'enquête dont disposent les autorités répressives, y compris les limitations et garanties applicables, est à la fois vaste et complexe mais qu'en revanche les informations incluses dans le bouclier de protection des données sont brèves. Le groupe de travail regrette dès lors, sur la base du peu d'informations dont il dispose (à l'annexe VII du bouclier de protection des données et dans les conclusions du projet de décision), être incapable de fournir une analyse complète de l'accessibilité, de la prévisibilité ainsi que de la nécessité et la proportionnalité des règles actuellement applicables. Sans préjudice des autres conclusions formulées par le groupe de travail dans le présent avis au sujet du bouclier, une telle analyse pourrait faire partie d'un réexamen annuel du bouclier de protection des données.

En ce qui concerne l'accès des autorités répressives, le groupe de travail «Article 29» constate qu'un mécanisme de surveillance relativement solide et indépendant semble avoir été mis en place. Le groupe de travail salue par ailleurs l'adoption de la loi sur le recours juridictionnel, qui accorde des droits de recours judiciaire aux ressortissants non américains. Il remarque toutefois que ces droits sont limités. Outre la constatation qu'un ressortissant non américain ne serait pas en mesure de contester un mandat de perquisition ou une injonction devant un tribunal en invoquant le quatrième amendement, des doutes subsistent également quant à la disponibilité réelle de recours effectifs pour les personnes concernées dans le domaine de l'application de la loi.

[97] Dans l'arrêt *Ontario v. Quon*, la Cour a considéré que la ville d'Ontario n'avait pas violé les droits de ses employés au titre du quatrième amendement, vu que sa consultation du contenu des messages privés de l'employé en question présentait un caractère raisonnable puisque motivée par un motif légitime lié au travail et que sa portée n'était pas excessive. Dans l'arrêt *Samson v. California*, la Cour a jugé que «le quatrième amendement n'[interdisait] pas à un officier de police de procéder à la fouille d'un libéré conditionnel en l'absence de tout soupçon». Dans l'arrêt *Maryland v. King*, la Cour a estimé que lorsque des officiers de police procèdent à une arrestation motivée par une présomption sérieuse justifiant l'arrestation et le placement en garde à vue d'un suspect pour infraction grave, le prélèvement et l'analyse d'un échantillon buccal de l'ADN de la personne arrêtée constituait, de même que les empreintes digitales et les photographies, une procédure légitime de détention jugée raisonnable au titre du quatrième amendement.

5. CONCLUSIONS ET RECOMMANDATIONS

Le groupe de travail «Article 29» est tout d'abord satisfait de constater que moins de cinq mois après l'invalidation de la sphère de sécurité, un nouveau projet de décision d'adéquation, incluant de nombreuses améliorations par rapport au précédent mécanisme, a été présenté. Il se félicite particulièrement de la transparence accrue offerte par la publication de deux listes du bouclier de protection des données sur le site web du ministère américain du commerce: l'une énumérant les organisations participant au bouclier, et l'autre les organisations qui ont adhéré au bouclier par le passé, mais qui l'ont désormais quitté. La transparence accrue au niveau de l'accès du public aux données transférées au titre du bouclier de protection des données, que ce soit pour des raisons de sécurité nationale ou à des fins répressives, est également bienvenue. Enfin, le groupe de travail «Article 29» est ravi d'apprendre que tous les transferts de données vers les États-Unis bénéficieront désormais de la même protection: aucune disposition légale spécifique ne donne l'avantage à un outil en particulier.

5.1 Trois inquiétudes

Il subsiste néanmoins trois grandes inquiétudes que le groupe de travail «Article 29» voudrait voir traiter.

La première est le fait que le langage utilisé dans le projet de décision d'adéquation ne contraigne pas les organisations à supprimer les données qui ne sont plus nécessaires, alors que cette obligation constitue un élément essentiel de la législation européenne en matière de protection des données, qui garantit que les données ne sont pas conservées plus longtemps que le temps nécessaire à la réalisation des finalités pour lesquelles elles ont été collectées. Deuxièmement, le groupe de travail «Article 29» déduit de l'annexe VI que l'administration américaine n'exclut pas totalement la possibilité de poursuivre la collecte de données massive et indifférenciée. Le groupe de travail «Article 29» a toujours considéré que ce type de collecte de données constituait une ingérence injustifiée dans les droits fondamentaux des personnes. Le troisième sujet de préoccupation concerne l'introduction du mécanisme de médiation. Si le groupe de travail «Article 29» se félicite de cette mesure sans précédent qui crée un mécanisme de recours et de surveillance supplémentaire pour les particuliers, il se demande toujours si les pouvoirs conférés au médiateur lui suffiront pour fonctionner efficacement. Il conviendrait au minimum de clarifier les pouvoirs et la position du médiateur pour démontrer que son rôle est véritablement indépendant et peut représenter un recours effectif en cas de traitement de données non conforme.

5.2 Clarifications recommandées

En plus des points susmentionnés, le groupe de travail «Article 29» a indiqué tout au long du présent avis différents points qui nécessiteraient davantage de précisions dans la décision d'adéquation. Il s'agit surtout de la nécessité de veiller à ce que les grandes notions relatives à la protection des données utilisées dans le bouclier de protection des données soient définies et appliquées de manière cohérente, ce qui n'est pas le cas actuellement. L'inclusion d'un glossaire dans la FAQ du bouclier de protection des données, contenant des définitions

idéalement convenues entre l'UE et les États-Unis, serait bienvenue. Le groupe de travail «Article 29» conclut également que les transferts ultérieurs de données à caractère personnel de l'UE ne sont pas suffisamment encadrés, surtout en ce qui concerne leur portée, la limitation de leurs finalités et les garanties applicables aux transferts à des mandataires. S'agissant de l'accès aux données relevant du bouclier de protection des données par les autorités répressives, la prévisibilité de la législation pose un problème particulier, en raison du caractère vaste et complexe du système répressif américain, tant au niveau fédéral qu'au niveau des États, et du peu d'informations contenues dans la décision d'adéquation.

Le bouclier de protection des données est la première décision d'adéquation formulée depuis l'accord de principe sur les textes du RGPD. Toutefois, bon nombre des améliorations du niveau de protection des données offert aux particuliers ne sont pas prises en compte dans le bouclier de protection des données. Le groupe de travail «Article 29» recommande par conséquent d'effectuer un réexamen de cette décision d'adéquation, ainsi que de celles adoptées pour d'autres pays tiers, peu après l'entrée en vigueur du RGPD.

Une dernière recommandation du groupe de travail «Article 29» à souligner ici concerne le réexamen conjoint. Le groupe de travail «Article 29» se félicite que la décision d'adéquation du bouclier de protection des données fasse l'objet d'un réexamen annuel, auquel participeront un vaste éventail d'APD et d'autres parties concernées. Il souhaiterait voir conclure, suffisamment en amont du premier réexamen, un accord sur les modalités de ces réexamens conjoints, y compris sur la rédaction et la présentation du rapport de réexamen par toutes les parties.