Tribunal de
l'Union européenne
Affaire T-738/16
(2017/C 006/49)

Mémoire en réplique

POUR

La Quadrature du Net, dite « LQDN»
La Fédération des fournisseurs d'accès à Internet associatifs, dite « FFDN »
French Data Network (Réseau de données français), dit « FDN »

Représentées par
M[e] Alexis Fitzjean Ó Cobhthaigh
Avocat au Barreau de Paris
5 rue Daunou, Paris 2[e] (75002)
France

CONTRE

Commission européenne

Table des matières

1 Dans l'affaire T-738/16, la Commission européenne a produit, le 25 septembre 2017, un mémoire en défense. Ce mémoire ne modifie en rien l'argumentation précédemment articulée par les exposantes, dont elles souhaitent expressément conserver l'entier bénéfice. Néanmoins, ce mémoire appelle, de leur part, les observations qui suivent.

2 En particulier, sous couvert d'accusation d'une lecture tronquée, sélective et erronée, la Commission peine à masquer son malaise et les nombreuses lacunes et erreurs de droit et de fait, entachant la décision d'exécution attaquée, comme les exposantes le montraient déjà dans leurs précédentes écritures et le préciseront encore dans les considérations qui suivent.

I. Considérations générales

3 D'emblée, il convient de recentrer le débat et de rappeler les exigences que la Commission est tenue de respecter lorsqu'elle procède à un constat d'adéquation en matière de transfert de données à caractère personnel de l'Union européenne vers un pays tiers.

4 **En droit**, aux termes de l'article 25, paragraphe 6, de la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après, la « Directive 95/46 ») :

> « La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes. »

5 En effet, le niveau de protection « assuré » par un pays tiers au sens de cet article s'apprécie « en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes » (CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14, point 71), dans le but d'assurer « la continuité du niveau élevé de cette protection en cas de transfert de données à caractère personnel vers un pays tiers » (*ibid*, point 72). L'expression « niveau de protection adéquat » doit ainsi être comprise comme « exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la Charte » (*ibid*). À défaut, la décision d'adéquation méconnaîtrait l'objectif d'assurer un niveau élevé de protection pour les personnes concernées.

6 Aux termes du paragraphe 2 de l'article 25 de la Directive 95/46 :

> « Le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données ; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées. »

7 Cette appréciation du caractère adéquat du niveau de protection ne conduit pas, comme le relève d'ailleurs la Commission, à examiner si le droit du pays tiers en matière de données personnelles est « identique » au droit de l'Union et en particulier à la directive 95/46. Toutefois, si les moyens auxquels le pays tiers a recours « peuvent être différents de ceux mis en œuvre au sein de l'Union [...] ces moyens doivent néanmoins s'avérer, en pratique, **effectifs** afin d'assurer **une protection substantiellement équivalente à celle garantie au sein de l'Union** » (CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14, point 74).

8 En outre, signalons que la Commission dispose d'une marge d'appréciation particulièrement réduite du caractère adéquat du niveau de protection d'un pays tiers, ainsi que l'a jugé la Cour de justice — ce, y compris lorsque les limitations aux droits sont justifiées par des raisons tenant à la sécurité nationale comme cela était le cas dans l'affaire *Schrems* :

> « À cet égard, il convient de constater que, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, du nombre important de personnes dont les droits fondamentaux sont susceptibles d'être violés en cas de transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat, le pouvoir d'appréciation de la Commission quant au caractère adéquat du niveau de protection assuré par un pays tiers **s'avère réduit**, de sorte qu'il convient de procéder à un contrôle strict des exigences découlant de l'article 25 de la directive 95/46, lu à la lumière de la Charte (voir, par analogie, CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, points 47 et 48). »
> (CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14, point 78)

9 C'est donc au regard de ces critères que le niveau de protection du droit américain doit être apprécié et, par conséquent, que la validité de la décision attaquée doit être examinée.

10 Or, **en l'espèce**, alors que l'objectif poursuivi par le droit à la protection des données à caractère personnel de l'Union commande qu'elle procède avec vigilance, la Commission fait usage d'une marge d'appréciation trop large de l'adéquation du niveau de protection du droit des États-Unis.

11 Et ce, d'autant que le niveau de protection du droit américain n'offre pas une « protection substantiellement équivalente à celle garantie au sein de

l'Union ».

12 Une telle conclusion se fonde sur plusieurs éléments. D'abord, certains éléments concernant la réglementation des États-Unis dont il est fait état dans la décision attaquée (y comprises ses annexes) auraient dû conduire la Commission à conclure à un défaut d'adéquation. Ensuite, certains aspects de la réglementation des États-Unis et des pratiques des services de renseignement sont décrits de manière trop vague ou incertaine et auraient dû conduire la Commission à rechercher davantage d'éléments pour fonder sa décision. Enfin, des éléments concernant la réglementation des États-Unis et les pratiques des services de renseignement tels que relevés par d'autres institutions, tel que le groupe de travail de l'article 29 (ci-après le G29) (prod. n° **B.2**), ou par des organisations de la société civile telle que l'American Civil Liberties Union (ACLU) [1] (prod. n° **B.1**) permettent de démontrer que la décision de la Commission est erronée.

13 Ainsi, l'insuffisance des garanties contenues dans la réglementation des États-Unis s'infère, d'une part, du caractère généralisé de certaines collectes par les autorités étatsuniennes (section II), comme de l'absence de limitation au strict nécessaire de l'exploitation de ces données (section III page 10) ; d'autre part, cette lacune ressort tout aussi clairement de l'absence de recours effectif (section IV page 13) et de contrôle indépendant à l'égard de ces traitements (section V page 19).

14 Au préalable, il convient néanmoins de revenir sur la spécificité de la signification d'un constat d'adéquation dans le secteur de la sécurité nationale.

II. Sur le caractère généralisé de l'accès et des collectes autorisés par la réglementation des États-Unis

1. Sur l'accès généralisé au contenu de communications électroniques

15 La Cour de justice considère qu' « *une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant* ***atteinte au contenu essentiel du droit fondamental au respect de la vie privée****, tel que garanti par l'article 7 de la Charte* » (CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14, § 94). L'autorisation donnée aux autorités publiques d'accéder de manière généralisée aux communications de l'ensemble d'une population doit être considérée, de la même façon, comme portant une atteinte au contenu essentiel du droit au respect de la vie privée.

1. L'American Civil Liberties Union (ACLU) est une ONG œuvrant à travers les tribunaux, le législateur et dans les communautés pour défendre les droits et libertés individuelles garanties par la Constitution et les lois des États-Unis depuis 1920. https://www.aclu.org/

16 Or, à aucun moment les autorités américaines ne donnent l'assurance qu'un tel accès généralisé n'aurait pas lieu. À l'inverse, de nombreux éléments contenus dans les déclarations des autorités américaines ou dans les références faites par celles-ci laissent croire qu'il existe un accès généralisé aux contenus des communications électroniques, limité *a minima*, par exemple par territoire ou région entières.

17 En effet, la lettre du 22 février 2016 du Bureau du directeur du renseignement national, jointe en Annexe VI de la décision attaquée, souligne 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.** » (Annexe VI, p. 3)

18 L'expression « partie réduite de l'internet » est incroyablement vague et pourrait recouvrir en réalité un champ très large de communications électroniques. Il est d'ailleurs notable que, à aucun moment, les autorités américaines ne donnent l'assurance que de telles collectes en vrac n'aient pas lieu sur l'ensemble de l'Union européenne.

19 Au contraire, par deux fois les autorités américaines ont refusé de garantir l'absence d'accès généralisé aux communications entre l'Union vers les États-Unis :

> « Les stratégies et les procédures décrites dans la présente lettre s'appliquent à tous les types de collecte en vrac de renseignements les signaux d'origine électromagnétique, y compris la **collecte en vrac de communications à destination et en provenance de l'Europe**, sans que cette lettre ne confirme ni l'infirme la réalité d'une telle collecte. »
>
> (Annexe VI de la décision attaquée, Lettre du 21 juin 2016 du Bureau du directeur du renseignement national)

> « sans confirmer ni infirmer les dires des médias selon lesquels les services de renseignement américains collecteraient des données originaires de câbles transatlantiques pendant leur transmission vers les États-Unis, précisons que, si les services de renseignement américains collectaient des données provenant de câbles transatlantiques, ils le feraient dans le respect des limitations et garanties ici mentionnées, y compris des exigences de la PPD-28. »
>
> (Annexe VI de la décision attaquée, Lettre du 22 février 2016 du Bureau du directeur du renseignement national)

20 De récentes révélations indiquent que les États-Unis collectent de vastes quantités d'informations au titre de l'EO 12333. Par exemple, la NSA collecte des milliards de données de localisation, quotidiennement, ou encore 200 millions de messages-textes dans le monde quotidiennement, ou encore l'intégralité des appels téléphoniques à destination de, à l'origine de, ou à

l'intérieur d'au moins deux pays entiers, ou encore la collecte de centaines de millions de contacts ou de carnets d'adresses de comptes email ou de messagerie instantanée (rapport de l'ACLU *précité*, § 61) (prod. n° **B.1**).

21 Dans la pratique, cette lacune au sein du droit des États-Unis permet au gouvernement américain de procéder à une exploitation massive des données collectées. Ainsi, selon le rapport de l'ACLU, la méthode de la « recherche en vrac » [2] permet au gouvernement de rechercher des informations dans le contenu d'une vaste quantité de communications électroniques au moyen d'une large gamme de mots-clés ou "termes de sélection", comme cela est le cas dans le programme *Upstream* ou dans l'application de l'EO12333 (rapport de l'ACLU *précité*, § 57) (prod. n° **B.1**). Ce type d'exploitation n'est par ailleurs aucunement limitée par la Presidential Policy Directive 28 (« la PPD 28 ») (rapport *précité*, § 69).

2. Sur le caractère généralisé de la collecte « en vrac »

22 À la section 2.3.2 de son mémoire, la Commission prétend que la collecte « en vrac » de renseignements, décrite aux considérant 71 à 76 de la décision attaquée, ne revêt pas un « caractère généralisé ». Ce faisant, elle fait sienne les prétendues garanties données par l'ODNI selon lesquelles « la collecte en vrac n'est ni "massive" ni effectuée "à l'aveugle" » (considérant 71 de la décision attaquée) et en déduit que le niveau de protection assuré par le droit américain concernant ces collectes de données serait adéquat. Pourtant, une analyse attentive des considérations retenues dans la décision attaquée démontre le contraire.

2.1. Le niveau de protection garanti en droit de l'Union européenne

23 La grande chambre de la Cour de justice a consacré l'exigence d'un niveau élevé de protection au sein de l'Union. La Cour a ainsi invalidé la directive 2006/24 en raison de l'absence de limitations au strict nécessaire tenant à la conservation des données par des opérateurs, à l'accès et à l'utilisation de ces données par les autorités et tenant, enfin, à la durée de conservation de ces données par les autorités.

24 Ainsi, **en premier lieu,** n'est pas compatible avec le niveau de protection garanti au sein de l'Union une réglementation qui prévoit une conservation des données de communications électroniques relatives à la quasi-totalité de la population européenne et qui « couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées » en fonction de l'objectif poursuivi (CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, point 57 cité au point 93 de l'arrêt *Schrems*, CJUE, g^{de} ch., 6 oct. 2015, *Schrems*,

2. Traduction libre de "bulk searching".

C-362/14).

25 En particulier, la directive 2006/24 est jugée invalide en ce qu'elle :

— « concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions graves. En outre, elle ne prévoit aucune exception, de sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel » (point 58) ;

— « ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la prévention, à la détection ou à la poursuite d'infractions graves » (point 59).

26 **En second lieu,** n'est pas non plus compatible avec le niveau de protection garanti au sein de l'Union une réglementation qui « ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins » qui « au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte » peuvent « être considérées comme suffisamment graves pour justifier une telle ingérence » (point 60).

27 En particulier, la directive 2006/24 est jugée invalide en ce qu'elle : « ne prévoit aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi » (point 62).

28 Surtout, n'est pas compatible avec le niveau de protection garanti au sein de l'Union une réglementation dans quelle « l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi » (point 62).

29 **En troisième lieu,** la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire.

30 En particulier, la directive 2006/24 imposait la conservation de données « pendant une période d'au moins six mois sans que soit opérée une quel-

conque distinction entre les catégories de données prévues [...] en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées », cette durée se situant en outre, entre six mois au minimum et vingt-quatre mois au maximum.

31 Il y a lieu de préciser que, contrairement à ce qu'affirme la Commission, chacune de ces exigences doit être respectée. C'est donc à tort que la Commission affirme que « c'est l'effet cumulatif de l'absence de toute "différenciation, limitation ou exception (...) en fonction de l'objectif poursuivi" **et** de l'absence de "critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises" qui dépasse selon la Cour les limites du strict nécessaire » (point 101 de son mémoire). Force est de constater d'ailleurs à cet égard que la Commission développe ici le même raisonnement que l'avocat général M. H. Saugmandsgaard Øe, dont l'argumentation sur ce point n'a pas été suivie par la Cour de justice dans l'arrêt *Tele2* (CJUE, g^{de} ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15, points 104 à 112).

2.2. Le niveau de protection constaté par la Commission dans la décision d'adéquation

32 **En premier lieu,** la collecte « en vrac » est comprise comme :

> « l'acquisition d'un volume relativement important d'informations ou de données issues du renseignement d'origine électromagnétique dans des conditions où les services de renseignement ne peuvent pas utiliser d'identifiant associé à une cible spécifique (tels que l'adresse électronique ou le numéro de téléphone de la cible) pour orienter la collecte. »
> (Annexe VI de la décision attaquée, Lettre du 21 juin 2016 du Bureau du directeur du renseignement national)

33 Il s'agit donc, par définition, d'une collecte « à l'aveugle », qui n'est pas orientée.

34 L'exemple est également donné à l'Annexe VI de la décision attaquée d'une collecte de l'intégralité des communications électroniques à destination et en provenance d'une région :

> « À titre d'exemple, les services de renseignement peuvent être amenés à acquérir des renseignements d'origine électromagnétique sur les activités d'un groupe terroriste opérant dans une région du Proche-Orient, dont on suppose qu'il planifie des attaques contre des pays d'Europe occidentale, mais sans connaître les noms, numéros de téléphone et adresses électroniques ou autres identifiants des individus associés à ce groupe terroriste. Nous pourrions choisir de cibler ce groupe en collectant des communications à destination et en provenance de cette région, qui seront ensuite passées au crible et analysées afin de déterminer les communications qui se rapportent à ce groupe. Ce

faisant, les services de renseignement chercheraient à réduire autant que possible le champ de la collecte. Cette activité serait considérée comme une collecte «en vrac», puisque l'utilisation de discriminants n'est pas possible, mais il ne s'agirait pas d'une collecte «massive» ou «indifférenciée» : au contraire, elle serait orientée aussi précisément que possible.

« Ainsi, même lorsqu'un ciblage au moyen de sélecteurs spécifiques n'est pas possible, les États-Unis ne collectent pas l'ensemble des communications provenant de l'ensemble des installations de communication existant dans le monde, mais ils appliquent des filtres et d'autres outils techniques pour orienter cette collecte vers les canaux de communication susceptibles d'avoir une valeur en termes de renseignement étranger. De cette manière, les activités américaines de renseignement d'origine électromagnétique ne touchent qu'une fraction des communications transitant sur le réseau internet. »

(Annexe VI de la décision attaquée, Lettre du 21 juin 2016 du Bureau du directeur du renseignement national)

35 L'administration des États-Unis considère donc manifestement être en droit de collecter l'ensemble des communications à destination et en provenance d'une région du Moyen-Orient, pour ne trier qu'ultérieurement les données pertinentes, au moment de leur exploitation. Une région du Moyen-Orient pourrait par exemple ici désigner les territoires combinés de l'Irak, de la Syrie et du Liban. Les communications internationales (appels à l'étranger, utilisation d'Internet, etc.) de tous les habitants de ces pays (60 millions de personnes) pourraient donc être licitement captées.

36 On peine à concevoir comment il serait objectivement possible de ne pas qualifier une telle collecte de « massive », celle-ci concernant l'ensemble des communications à destination et en provenance d'une population ou une « partie » de l'internet.

37 Il ressort de cette description que la collecte « en vrac » peut porter de manière globale sur l'ensemble des personnes faisant usage de services de communications électroniques sans que les personnes dont les données sont collectées se trouvent, même indirectement, dans une situation susceptible de justifier l'ingérence dans la confidentialité des communications. En particulier, la collecte en vrac s'applique même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec les finalités du renseignement.

38 En outre, à aucun moment et en aucune manière, le PPD-28 ne donne l'assurance que des exceptions existent pour les personnes dont les communications sont soumises au secret professionnel.

39 Par conséquent, les pratiques de collecte en vrac couvrent des fractions entières de l'Internet et, de ce fait, doivent être comprises comme « généralisée » et s'appliquent à l'ensemble des communications internet de telles fractions, sans « qu'aucune différenciation, limitation ni exception soient opérées » en fonction de l'objectif poursuivi.

40 La circonstance que la collecte « en vrac » n'intervienne que lorsque « *les services de renseignement ne peuvent pas utiliser d'identifiant* » révèle immédiatement qu'elle concerne toute une population, sans « aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi », et ce précisément parce que ces différenciations sont opérationnellement impossibles. Ainsi qu'il est décrit dans la lettre du 21 juin 2016 susmentionnée, ces différentiations et limitations n'interviendront au mieux qu'ultérieurement, au moment de l'exploitation. De la même manière, il semble difficile de ne pas considérer une telle collecte comme opérée « à l'aveugle ».

41 De plus, il convient de signaler que, même si la collecte « en vrac » pourrait éventuellement ne concerner qu'une région délimitée, elle n'en serait pas pour autant « ciblée » puisque, au sein de cette région, toute la population pourrait être affectée, sans aucune différenciation, limitation ou exception. De même, il importe peu que l'administration des États-Unis tente de minimiser les cas où elle recourt à une collecte « en vrac », dans la mesure où elle ne donne à cet égard aucune « assurance » ou garantie. *

42 Il convient également de constater que les assurances de l'ODNI, qui synthétisent le contenu des mesures de la PPD-28, font expressément mention des limitations en matière de collecte (Annexe VI p 2, p 92 de la décision) ainsi qu'en matière de conservation et diffusion (Annexe VI p 5, p 95 de la décision), mais qu'aucun élément concernant la limitation en matière d'exploitation ou d'utilisation de ces données n'y ait exposé.

43 Par ailleurs, il y est précisé que *« les composantes des services de renseignement sont donc tenues de supprimer les informations relatives à des ressortissants non américains qu'elles ont collectées par le renseignement d'origine électromagnétique* ***dans les cinq ans suivant leur collecte****, à moins qu'il ne soit établi qu'elles répondent à un besoin de renseignement étranger autorisé ou que le DNI ne considère, après prise en compte du point de vue de l'agent de l'ODNI pour la protection des libertés civiles et des responsables de la protection de la vie privée et des libertés civiles des agences, qu'une conservation prolongée répond aux intérêts de la sécurité nationale ».*

44 Il faut déduire de cette constatation de l'ODNI qu'une donnée pourra être collectée et conservée sans que la finalité de sa collecte soit immédiatement définie, ceci pouvant être établi jusqu'à cinq ans après la collecte initiale.

45 Il s'infère de tout ce qu'il précède que le droit des États-Unis permet une collecte et un accès généralisés aux données personnelles et au contenu des communications en provenance de l'Union européenne. En constatant l'inverse, la Commission a commis une erreur manifeste d'appréciation.

46 De ce chef, déjà, l'annulation est inévitable.

III. Sur l'absence de nécessité dans l'exploitation des données collectées

47 A la section 2.4 de son mémoire, la Commission allègue que la réglementation mise en place par les États-Unis respecterait le principe de limitation au strict nécessaire de l'exploitation de données. Elle refuse de voir un caractère vague dans la finalité d'exploitation que constituent les menaces à la cybersécurité et affirme que les finalités d'exploitation des données collectées de manière ciblée seraient effectivement constatées par la décision attaquée.

48 Cette analyse est pourtant faussée à de multiples égards.

1. Le niveau de protection garanti en droit de l'Union européenne

49 Dans l'arrêt *Schrems*, la Cour de justice a considéré que « n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les ÉtatsUnis [. . .] sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données » (CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14, § 93).

50 En outre, l'objectif poursuivi par les mesures engendrant une ingérence (notamment dans le droit à la confidentialité des communications électroniques) « **doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux** » (CJUE, g^{de} ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15, point 115).

51 Ainsi, *en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales*, la **lutte contre la criminalité grave** est **le seul objectif d'intérêt général** susceptible de justifier une mesure de conservation de données de connexion, dès lors qu'une telle mesure constitue une ingérence particulièrement grave (point 102 de l'arrêt *Tele2*).

52 En d'autres termes, plus l'ingérence est grave et de grande ampleur, plus l'objectif poursuivi par les mesures causant cette ingérence doit être considéré comme sérieux, grave et restreint.

2. Le niveau de protection constaté par la Commission dans la décision d'adéquation

53 Les finalités poursuivies par les services de renseignement étatsuniens ne sont pas liées à la gravité et à l'ampleur de l'ingérence portée aux droits fondamentaux engendrée par les pratiques de collecte de données et d'accès

aux communications, ni pour la collecte en vrac, ni pour la collecte ciblée.

2.1. Finalités de l'utilisation des données résultant de la collecte en vrac

54 **En premier lieu,** les finalités poursuivies par les services de renseignement étatsuniens ne sont pas en relation avec la gravité et l'ampleur de l'ingérence dans les droits fondamentaux causée par les pratiques de collecte de données et d'accès aux communications décrits ci-avant.

55 Par exemple, s'agissant de la collecte en vrac, les finalités poursuivies incluent notamment « la cybersécurité » (Annexe VI précité). La poursuite d'une finalité si large, quoique légitime, ne saurait être interprétée comme étant suffisamment restreinte et en relation avec la gravité et l'ampleur des pratiques de collecte en vrac constatées.

56 **En second lieu**, la décision attaquée constate que la PPD 28 justifie notamment l'exploitation de données collectées « en vrac » par la lutte contre les « *menaces pour la cybersécurité* » (considérant 74), ce qui est trop imprécis pour constituer un critère objectif.

57 La Commission explique que « *la notion de cybersécurité est utilisée par le législateur américain dans son acception courante, et elle désigne la sécurité des réseaux de communication électronique* » (point 93 de son mémoire). Cette expression manque à nouveau de précision, celle-ci pouvant notamment désigner l'assurance et la maintenance globale du bon fonctionnement technique d'un réseau et ce indépendamment des fins auxquelles celui-ci est utilisé.

58 De plus, dans son acception courante telle que celle exposée sur l'encyclopédie en ligne Wikipédia, la cybersécurité est définie comme un « *néologisme désignant l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels(. . .) des états et des organisations (. . .)* » [3]

59 Cette définition recouvre ainsi un large éventail d'hypothèses pouvant inclure la sécurité d'une infrastructure – que celle-ci fonctionne en réseau ou non –, mais aussi la protection d'informations sous prétexte qu'elles sont contenues dans une base de données, voire la protection physique d'une personne responsable de la sécurité informatique d'une "organisation" privée.

60 Une telle énumération, pourtant loin d'être exhaustive, suffit à démontrer que l'acception « courante » d'une telle notion ne saurait constituer un critère objectif.

61 **En troisième lieu**, la Commission justifie la mobilisation par le droit des États-Unis de « *la notion que ce terme a dans le langage courant* » par le

3. Définition de l'encyclopédie Wikipedia au 19 décembre 2017 https://fr.wikipedia.org/wiki/Cybers%C3%A9curit%C3%A9)

fait qu'une « *définition trop précise de ces menaces finirait par être trop restrictive (nuisant à la capacité de faire face aux nouvelles menaces)* » (point 90 de son mémoire).

62 Ce faisant, la Commission reconnaît explicitement que le droit des États-Unis a consciemment refusé de limiter l'exploitation des données collectées « en vrac » par un critère objectivement défini, car un tel critère aurait limité ses pouvoirs d'action. Or, une telle restriction de pouvoirs constitue précisément l'un des buts assigné à la réglementation sur la collecte de données, matérialisé par l'exigence que celle-ci poursuive une finalité objective.

63 **En quatrième lieu**, dans un rapport d'expertise spécifiquement adressé aux requérantes, l'American Civil Liberties Union (ACLU) a procédé à une présentation du droit des Etats-Unis et des conséquences de son application pratique. Ce rapport permet de comprendre l'importance des risques concrets qu'impliquent les manquements juridiques dénoncés par les requérantes (prod. n° **B.1**). Quant aux finalités énoncées par la PPD-28, ce rapport explique que celles-ci sont sujettes à de très larges interprétations (v. rapport de l'ACLU *précité* ; § 68). (prod. n° **B.1**)

64 Par ailleurs, les autorités nationales de protection des données personnelles de l'Union, au sein du groupe de travail Article 29 (le G29), ont publié le 5 décembre 2017 leur premier rapport conjoint relatif au Privacy Shield. Fondé sur les faits rapportés par le gouvernement américain et les rencontres ayant eu lieu à Washington les 18 et 19 septembre 2017, celui-ci fait un constat critique de la réglementation des États-Unis permettant la mise en place du bouclier (prod. n° **B.2**).

65 Après avoir rappelé sa position quant à l'impossibilité qu'une surveillance de masse et indiscriminée puisse revêtir un caractère proportionnel et nécessaire (page 14), le G29 fait état de plusieurs préoccupations quant à la législation en vigueur aux États-Unis. Notamment, le rapport déplore qu'aucune information nouvelle n'ait été donnée au G29 quant à l'interprétation retenues des six finalités prévues par la PPD-28 permettant l'utilisation de données (page 16).

66 La Commission ne parvient donc pas à combler le manque de clarté du droit des États-Unis et ne démontre nullement en quoi la cybersécurité constitue un « critère objectif » permettant de délimiter l'utilisation ultérieure des données collectées à « *des fins précises, strictement restreintes et susceptibles de justier l'ingérence* ». Au contraire, elle laisse entendre qu'une telle finalité doit englober de nombreuses hypothèses.

2.2. Finalités de l'utilisation des données résultant de la collecte ciblée

67 La Commission échoue à indiquer quelle constatation de la décision attaquée permettrait de démontrer l'existence d'un « critère objectif » limitant l'utilisation des données collectées de manière ciblée.

68 La Commission cite des constatations de la décision attaquée relatives à la détermination de finalités « précises [et] strictement restreintes» mais qui ne concernent pas **l'exploitation** des données collectées de façon ciblée. En effet, aux points 104 à 106 de son mémoire, elle explique que la décision attaquée constaterait que l'accès aux données est encadré, mais ce cadre ne concerne en réalité que le *stockage*, la *conservation* (considérants 84 et 86) et la*diffusion* (considérants 86 et 87) des données. La Commission ne mentionne aucune limitation relative à *l'exploitation* de ces données une fois collectées ou diffusées.

69 Or, tel est l'exact objet du moyen soulevé dans la requête, ce à quoi la Commission ne répond pas.

70 **En conclusion**, la Commission ne parvient pas à démontrer que la décision attaquée constate effectivement l'existence d'un « critère objectif » limitant l'exploitation ultérieure de données collectées aussi bien « en vrac » que de façon ciblée à « des ns précises, strictement restreintes et susceptibles de justier l'ingérence ».

71 La décision attaquée est donc, tout à la fois, entachée d'erreur manifeste d'appréciation et d'erreur de droit.

72 A cet égard, encore, la censure est acquise.

IV. Sur l'absence de recours effectif

73 A la section 2.5 de son mémoire, la Commission prétend que les différentes voies de recours *ex post* prévues par la décision attaquée constituent des voies de recours présentant les garanties exigées par le droit de l'Union.

1. Le niveau de protection garantie en droit de l'Union européenne

74 L'article 47 de la Charte dispose que *« toute personne dont les droits et libertés garantis par le droit de l'Union ont été violés a droit à un recours effectif devant un tribunal dans le respect des conditions prévues au présent article. »*

75 L'arrêt *Schrems* précise en son considérant 95 qu'une *« réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte »* (CJUE, g^{de} ch., 6 oct. 2015, *Schrems*, C-362/14, § 95),

76 L'arrêt Télé 2 a permis d'apporter un éclairage concernant les obligations en matière de notification. Au paragraphe 121, la Cour énonce qu'il « importe que les autorités nationales compétentes auxquelles l'accès aux données

conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités. En effet, cette information est, de fait, nécessaire pour permettre à celles-ci d'exercer, notamment, le droit de recours, explicitement prévu à l'article 15, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 22 de la directive 95/46, en cas de violation de leurs droits» (CJUE, g^{de} ch., 21 déc. 2016, *Tele2 Sverige*, C-203/15, C-698/15, §121).

77 La Commission soutient que l'arrêt *Schrems* doit être interprété en ce qu'il condamne et considère comme contraire à la Charte uniquement une situation ou aucune possibilité d'exercer des voies de droit n'existerait. Elle considère que la décision attaquée contiendrait «*des constatations détaillées sur la protection juridictionnelle garantie aux États-Unis à l'encontre des activités de renseignement notamment de type électromagnétique*» (et en déduit donc que la réglementation des États-Unis ne serait pas concernée par l'hypothèse sanctionnée par l'arrêt (points 113 et 114 de son mémoire).

78 Cette lecture est grossièrement erronée. En effet, rappelons que c'est** l'effectivité** du recours qui doit être examinée au regard du droit de l'Union et non la constatation de sa seule existence formelle. Cette position de la Cour rejoint celle de la Cour européenne des droits de l'homme, pour laquelle la Convention EDH « a pour but de protéger des droits non pas théoriques ou illusoires, mais concrets et effectifs » (CEDH 9 oct. 1979, *Airey c/ Irlande*, req. n° 6289/73, série A, n° 32).

79 La Cour a également affirmé que l'existence même d'un contrôle juridictionnel effectif destiné à assurer le respect des dispositions du droit de l'Union est inhérente à l'existence d'un État de droit (voir, en ce sens, CJCE, 23 avril 1986,*Les Verts/Parlement*, 294/83, § 23 ; CJCE, 15 mai 1986, *Johnston*, 222/84, § 18-19 ; CJUE, 15 octobre 1987, *Heylens* e.a., 222/86, § 14, ainsi que CJCE, 11 septembre 2008, *UGTRioja e.a.*, C428/06 à C434/06, § 80).

2. Le niveau de protection constaté par la Commission dans la décision d'adéquation

80 La décision attaquée consacre un paragraphe aux voies de recours s'ouvrant aux ressortissants de l'Union qui auraient subi une violation dans leur droit à une protection de leurs données personnelles. (Paragraphe 3.1.2 intitulé "Protection juridictionnelle effective"). Cependant, les propres constatations de la Commission permettent de démontrer que celles-ci ne sont pas suffisamment effectives afin de garantir une correction de cette violation telle qu'exigée par un constat d'adéquation.

2.1. En ce qui concerne la voie de recours prévue par la loi sur la liberté d'information

81 La Commission fait valoir que la loi sur la liberté d'information (*Freedom of information Act* 'FOIA') exposée au considérant 114 de la décision attaquée constitue une possibilité d'accéder aux informations détenues par des autorités gouvernementales (point 128 de son mémoire).

82 Cependant, la Commission avait elle même constatée dans ce considérant que le « FOIA ne prévoit pas de voie de recours pour des actions individuelles contre les ingérences proprement dites en matière de données à caractère personnel» et que les possibilités d'accès aux informations pertinentes détenues par les agences nationales du renseignement semblent limitées, car « les agences peuvent retenir des informations qui relèvent d'une liste d'exceptions ».

83 Pour l'ACLU, le mécanisme prévu par cette disposition ne saurait être regardé comme une voie de recours réparatrice en cas de surveillance irrégulière puisqu'il ne s'agit que d'une simple mesure de transparence des activités étatiques envers le public (v. rapport de l'ACLU *précité*, § 113). (prod. n° **B.1**) Elle constate également que cette transparence est particulièrement limitée lorsque sont mises en cause les activités de surveillance visant les données ou communications d'une personne prise individuellement (*ibid*). (prod. n° **B.1**)

84 Ainsi, dans la mesure où ce texte ne prévoit qu'un accès limité à des informations concernant les personnes non américaines, elle ne saurait être considérée comme une voie de recours effective leur permettant d'obtenir des informations susceptibles d'établir l'existence, à leur égard, d'une mesure de surveillance.

2.2. En ce qui concerne le recours devant les juridictions ordinaires

85 La Commission affirme qu'une personne non américaine peut demander l'exclusion, dans une procédure judiciaire, d'informations récoltées sous l'autorité des lois autorisant une telle collecte pour des raisons de sécurité nationale tel que le FISA si celle-ci sont illégales (point 129 de son mémoire).

86 Cependant, selon les propres constatations de la Commission, « les moyens d'action sont limités et les réclamations introduites par des personnes physiques (même américaines) seront déclarées irrecevables lorsqu'elles ne peuvent démontrer leur qualité pour agir, ce qui restreint l'accès aux juridictions ordinaires » (considérant 115 de la décision attaquée).

87 Si la Commission précise que chaque État peut légitimement établir les conditions spécifiques qui gouvernent la qualité pour agir devant ses tribunaux", il convient de rappeler qu'en droit de l'Union, cette autonomie procédurale s'exerce dans la mesure où ces règles ne font pas échec, dans les faits, à l'effectivité des garanties attachées à ces voies de recours. En effet, ces règles de procédure nationale ne doivent pas « *rendre pratiquement*

impossible ou excessivement difficile l'exercice des droits conférés par l'ordre juridique communautaire » (CJCE 7 juill. 1981, *Rewe*, 33/76 et CJCE, 16 déc. 1976, *Comet*, 45/76). Concernant un État tiers, la logique est analogue dans le sens où ces même règles de procédures ne doivent pas rendre pratiquement impossible ou excessivement difficile la mise en œuvre des garanties contenues dans le droit de cet État, regardées comme substantiellement équivalente à celles conférées par l'ordre juridique de l'Union, et constituant ici la seule justification au transfert des données des citoyens européens.

88 Or, c'est précisément le cas en l'espèce.

— En effet, aucune action civile engagée sur le fondement de la section 702 du FISA ou de l'EO 12333 dans le but de remettre en cause la licéité d'une mesure de surveillance étatique n'a donné lieu a une appréciation par un juge, et n'a, *a fortiori*, donné lieu à la réparation du préjudice causé par une telle mesure (rapport de l'ACLU *précité*, § 100) (prod. n° **B.1**).

89 A ce titre, la Commission cite un arrêt du 23 mai 2017 rendu par la U.S. Court of Appeals (*Wikimedia Found. v. NSA*, 857 F.3d 193 (4th Cir. 2017)). Si la partie requérante s'est vue reconnaitre sa qualité à agir pour contester l'application d'une mesure du FISA, celle-ci a été refusée dans la même instance à huit autres organisations, pourtant exposées à une possible surveillance. Par ailleurs, la Cour n'a pas définitivement statué sur la recevabilité du requérant, qui pourra encore être remise en cause par le gouvernement des États-Unis (voir rapport de l'ACLU §§105 à 109). (prod. n° **B.1**) Un tel précédent isolé et tronqué ne saurait dès lors attester de l'accessibilité du recours aux justiciables de l'Union. (prod. n° **B.1**)

90 Dans son rapport du 28 novembre 2017, le G29 a également constaté que les voies de recours permises par l'Administrative Procedure Act et le FISA sont soumises à des règles de recevabilité et que les critères devant être pris en compte afin de déterminer les règles de recevabilité sont ceux fixés par la jurisprudence de la CJUE et la CEDH (page 18) . Le G29 conclut qu'il semble difficile et incertain qu'un citoyen européen puisse satisfaire les règles procédurales de recevabilité lorsqu'il exerce un recours en vertu de la section 702 FISA ou de l'EO12333. (prod. n° **B.2**)

91 **En conclusion**, si les personnes concernées de l'Union européenne disposent de voies de recours devant les juridictions ordinaires des États-Unis, l'impossibilité en pratique de démontrer sa qualité à agir empêchent celles-ci d'être considérées comme effectives.

2.3. En ce qui concerne le Médiateur

92 La Commission soutient que l'effectivité du mécanisme additionnel du Médiateur serait liée, d'une part, à une indépendance fonctionnelle vis-à-vis des services de renseignement, et bénéficierait, d'autre part, de la possibilité de coopérer avec des autorités de contrôle (point 138 de son mémoire). Cette description est cependant insuffisante à déduire des constatations de

la décision attaquée que ce mécanisme comporte les garanties attachées à toute voie de recours équivalente dans l'Union européenne.

93 **En premier lieu**, le Médiateur ne saurait, en aucun cas et en aucune manière, être regardé comme indépendant.

94 En effet, la Commission constate au considérant 116 de la décision attaquée que « ce mécanisme repose sur la désignation, au titre de la PPD-28, d'un coordinateur chevronné (niveau de sous-secrétaire) au département d'État» Comme le souligne le rapport d'expertise rédigé par l'ACLU, le Médiateur fait partie intégrante du département d'État (rapport de l'ACLU *précité*, § 118) (prod. n° **B.1**) et participe directement à la "communauté de surveillance". Le G29 rejoint d'ailleurs cette analyse puisqu'il exprime clairement sa réserve sur la nomination d'un fonctionnaire du département d'État (voir avis *précité*, p 19) (prod. n° **B.2**).

95 Aucun texte ne confère par ailleurs au médiateur le pouvoir de mener une analyse juridique et factuelle des plaintes qu'il reçoit de façon complète et indépendante v. rapport de l'ACLU *précité*, § 119) (prod. n° **B.1**). A ce titre, la circonstance que le médiateur « rapporte toute tentative d'influence – interne ou externe au Département d'État – directement au secrétaire d'Etat » [4] ne saurait constituer une garantie effective.

96 Enfin, il convient de noter que dans sa décision *DPC v. Facebook Ireland Limited and Max Schrems* [2016 No. 4809 P.], la High Court irlandaise a récemment jugé que le Médiateur ne pouvait garantir une protection juridictionnelle effective en ce qu'il n'était pas indépendant du pouvoir exécutif (voit notamment §110 de la décision). [5]

97 **En second lieu**, les pouvoirs insuffisants dont dispose le Médiateur ne permettent pas aux personnes concernées par le transfert de données autorisé dans le cadre du Privacy Shield de disposer d'un recours juridictionnel leur permettant d'avoir accès à des données à caractère personnel les concernant, ou d'obtenir la rectification ou la suppression de telles données.

98 Au considérant 118 de la décision attaquée, la Commission estime qu'en attribuant au médiateur « l'obligation de **confirmer** le respect du droit ou la correction d'un manquement au droit, le mécanisme reflète l'engagement pris globalement par le gouvernement américain de traiter les réclamations introduites par des personnes de l'Union européenne et d'y apporter une réponse », constatant dès lors les pouvoirs restreints de cette entité.

99 En effet, le Médiateur opère un contrôle limité, ne lui permettant pas d'apprécier la nécessité et la proportionnalité des procédures de surveillance mises en place par la décision attaquée, dont il se borne à vérifier la conformité (v. rapport de l'ACLU *précité*, §115) (prod. n° **B.1**). Le Médiateur n'est ainsi en mesure de délivrer au requérant qu'une " confirmat[ion] que la plainte a été dûment étudiée, et que le droit des États-Unis [. . .], contenant

4. Premier réexamen annuel du bouclier de protection des données UE-États-Unis, disponible à l'adresse http://europa.eu/rapid/press-release_MEMO-17-3967_fr.htm

5. Décision disponible à l'addresse https://www.dataprotection.ie/docimages/documents/Judgement3Oct17.pdf

les limitations et garanties décrites dans la lettre de l'ODNI, a été respecté ou, en cas de non respect, qu'il a été remédié à celui-ci" [6].

100 Le G29 estime n'avoir pas pu disposer d'assez d'éléments -la plupart étant classifiée - lui permettant d'établir que le Médiateur disposait de pouvoirs suffisants en matière d'accès aux informations et de rectification en cas de violation. En effet, ceux-ci sont limités à informer ou non le requérant de la conformité d'une mesure. Le G29 estime que ces pouvoirs ne sont pas comparables à ceux attribués aux tribunaux ou autres entités indépendantes similaires pour exercer leur rôle. Il lui est dès lors impossible d'affirmer que le Médiateur possède des pouvoirs adéquats pour exercer de manière effective ses fonctions [7]. (voir avis *précité*, p 19) (prod. n° **B.2**)

101 De plus, aucune précision n'est apportée au requérant sur la possible surveillance dont il aurait fait l'objet et sur la manière de remédier à cette surveillance irrégulière (voir rapport de l'ACLU *précité*, § 118) (prod. n° **B.1**). Les personnes dont les données ont été conservées par des autorités nationales ne peuvent donc se voir communiquer cette information dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités.

102 En outre, et surtout, la décision rendue par le Médiateur au terme de ce contrôle limité revêt un caractère exécutoire tout aussi restreint puisque qu'il ne dispose d'aucun pouvoir d'injonction envers les services concernées afin d'assurer sa pleine exécution. Aucun appel n'est d'ailleurs possible à l'issue de la décision rendue (voir rapport de l'ACLU *précité*, § 119) (prod. n° **B.1**).

103 Le G29 regrette cette absence de révision des décisions rendues par le Médiateur, tout recours étant impossible si une mesure n'est pas étudiée par le Médiateur. Le G29 estime ainsi ne pas être en mesure de le considérer comme un « recours effectif devant un tribunal » au sens de l'article 47 de

6. Traduction libre de : "The Privacy Shield Ombudsperson will provide a response to the submitting EU individual complaint handling body confirming (i) that the complaint has been properly investigated, and (ii) that the U.S. law, statutes, executives orders, presidential directives, and agency policies, providing the limitations and safeguards described in the ODNI letter, have been complied with, or, in the event of non-compliance, such non-compliance has been remedied." E.U-U.S Privacy Shield Ombudsperson mecanism regarding signals intelligence available at https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004q0g

7. Traduction libre de : "The procedures governing the access to relevant information by the Ombudsperson and governing the interactions of the Ombudsperson with the other members of the Intelligence Community, including the oversight bodies, remain classified. Only examples illustrating how cases would be handled were shared with the WP29 after the Joint Review. Nevertheless, as long as the applicable procedures will remain classified and will not be shared, the WP29 will not be in a position to assess whether the Ombudsperson is vested with sufficient powers to access information and to remedy non-compliance. Based on the available information, the WP29 doubts that the powers to remedy non-compliance vis-à-vis the intelligence authorities are sufficient, as the "power" of the Ombudsperson seems to be limited to decide not to confirm compliance towards the petitioner. As the WP29 understands, she is not vested with powers, which courts or other similarly independent bodies would usually be granted to fulfil their role. Therefore, the WP29 is not in position to hold that the Ombudsperson is vested with adequate powers to effectively exercise its duty".

la Charte (voir avis *précité*, p 19) (prod. n° **B.2**).

104 **En conclusion**, dans ces conditions, la Commission ne saurait valablement prétendre que le mécanisme du Médiateur tel que présenté dans la décision attaquée, constitue ou contribue à un recours effectif au bénéfice des personnes concernées par le transfert de donnée autorisé par la décision attaquée.

105 Au regard de ces différents moyens de recours, il est impossible de constater le moindre commencement de recours effectif.

106 Partant, la décision attaquée est tout à la fois entachée d'erreur de droit et d'erreur manifeste d'appréciation.

107 Derechef, l'annulation est encourue.

V. Sur l'absence d'indépendance du contrôle

108 La Commission soutient que les différentes autorités de contrôle des activités américaines de surveillance constituent un « contrôle indépendant » limitant l'accès et l'utilisation des données des citoyens de l'Union européenne.

1. Le niveau de protection garantie en droit de l'Union européenne

109 La Cour de justice a conclu dans sa décision *Digital Rights Ireland*, que « l'accès aux données conservées par les autorités nationales compétentes [doit être] subordonné à un contrôle préalable eectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux ns d'atteindre l'objectif poursuivi et [doit intervenir] à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales. » (CJUE, g^{de} ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12, point 62)

2. Le niveau de protection constaté par la Commission dans la décision d'adéquation

110 Les mécanismes de contrôle prévus par la réglementation américaine sont décrits par la Commission la décision attaquée dans une sous-section "Surveillance"(considérants 92 à 110). Néanmoins ces constations ne suffisent pas à établir que ces différentes entités soient en mesure de limiter l'accès aux données et l'utilisation des données des citoyens de l'Union.

2.1. Concernant le pouvoir exécutif

111 La décision attaquée constate que les activités de renseignement des autorités américaines font l'objet d'une surveillance de la part « notamment des délégués à la protection des libertés civiles ou de la vie privée, des inspecteurs généraux, le bureau de l'ODNI chargé des libertés civiles et de la vie privée, le conseil de surveillance de la vie privée et des libertés civiles (PCLOB) et le conseil de surveillance du renseignement du président (PIOB)» (considérant 95).

112 **En premier lieu**, la Commission cite l'avis 01/2016 du G29 (prod. n° **B.3**) qui considèrerait le contrôle interne par les délégués de protection comme "assez solide", auxquels s'ajoutent les Inspecteurs généraux qui "respectent le critère d'indépendance organisationnelle telle que définie par la CJUE et la CEDH" (point 156 de son mémoire). Cependant, la suite de l'avis -non citée - affirme que ce niveau de solidité est acquis "au moins à partir du moment ou le processus de nomination sera appliqué à tous les inspecteurs généraux. Pour le moment, certaines réserves demeurent puisque ceux-ci sont nommés par le Directeur de l'agence qu'ils contrôlent." [8]

113 Le manque d'indépendance des inspecteurs généraux n'est par ailleurs pas réellement garanti. En effet, si la décision attaquée affirme que les inspecteurs généraux sont en principe inamovibles (Considérant 97, note de bas de pas n° 110), cette inamovibilité n'est pas effective en pratique. En effet, le rapport de l'ACLU soutient que si historiquement les inspecteurs généraux étaient protégés par des principes politiques, la force de ces principes est incertaine sous l'administration du Président Trump. En effet, plusieurs membres du Congrès ont écrit à l'administration à la suite de signalements que l'équipe administrative de transition du Président Trump a menacé de licencier plusieurs inspecteurs généraux avant l'investiture (rapport de l'ACLU *précité*, § 92) (prod. n° **B.1**).

114 **En second lieu**, la Commission décrit le PCLOB comme un « organe dit 'bipartisan' doté d'une large indépendance, reconnue encore une fois par les autorités européennes de protection des données».

115 Dans ce même avis (prod. n° **B.3**), le G29 conclut pourtant que

> « Cependant, pour justifier une ingérence dans les droits fondamentaux de respect de la vie privée et des données personnelles, le contrôle doit être totalement indépendant. Si le G29 respecte et apprécie le travail des différents délégués de protection, il ne peut conclure qu'ils respectent le niveau requis d'indépendance pour agir en tant que superviseur indépendant » (§3.4.1, p41)

116 De même, l'ACLU explique dans son rapport que le PCLOB n'est pas conçu pour corriger certaines pratiques de la surveillance mis en place par les Etats-Unis. Il n'a jamais prévu de voie de recours en cas de violation

8. Traduction libre de "at least from the moment the new nomination process applies to all. For the time being, some concerns remain regarding Inspectors-General that are still appointed by the Director of the agency they oversee".

de droits, ni fonctionné comme un mécanisme de protection des données personnelles. Ses recommandations ne consistent d'ailleurs qu'en de simples avis, dépourvus de toute contrainte pour le pouvoir exécutif.

117 De plus, le PCLOB n'est aucunement indépendant dès lors, notamment, que les rapports qu'il publie peuvent ne pas être rendus public en vertu d'un privilège présidentiel. Du reste, son champ d'action peut être limité par le Congrès (rapport de l'ACLU *précité*, §§ 88 à 90). (prod. n° **B.1**)

118 **En conclusion**, les organes exécutifs que constituent les délégués, les inspecteurs généraux et le PCLOB ne peuvent être qualifiés d'entités indépendantes permettant de contrôler que l'accès aux données et leur utilisation soient limités à ce qui est strictement nécessaire aux ns d'atteindre l'objectif poursuivi.

2.2. Concernant le pouvoir législatif

119 La Commission affirme que le contrôle serait également exercé par le Congrès depuis l'adoption de la loi USA FREEDOM, lui permettant de connaître le nombre d'ordonnances et de directives demandées et obtenues au titre du FISA et des estimations du nombre des personnes, américaines ou non, visées par la surveillance. Pour la Commission, cela « *constitue une ultérieure garantie que les activités de surveillances seront conduites d'une manière proportionnée* » (point 159 de son mémoire).

120 Les mesures mises en place par cette loi sont décrites par les assurances de l'ODNI (Annexe VI, p10, p 100 de la décision attaquée).

121 Dans son rapport, l'ACLU décrit cependant une pratique inverse à celle que la loi USA FREEDOM était censée prévoir puisque les membres du Congrès parviennent avec difficulté à accéder à ces informations. De plus, le pouvoir exécutif a pu refuser de donner au Congrès les estimations du nombre de communications de citoyens américains soumis à la surveillance prévue par la section 702 du FISA (rapport de l'ACLU *précité*, §§ 83 et 84) (prod. n° **B.1**).

122 Dès lors, ces mesures de transparence ne sont pas effectives et ne peuvent, en outre, donner au pouvoir législatif une influence sur les autorités de renseignement, et sur la possibilité de limiter l'accès aux données et leur utilisation.

2.3. Concernant le pouvoir judiciaire

123 La Commission prétend que serait mis en place un contrôle des mesures de collecte à travers les tribunaux FISA et FISCR. Pourtant, elle se contredit d'emblée lorsqu'elle « ajoute seulement que le FISC procède à des certifications annuelles pour des programmes de surveillance de large portée»(Point 161 de son mémoire).

124 En effet, la Commission admettait dans ses propres constatations que :

> « le FISC n'autorise **pas de mesures de surveillance individuelle**, mais plutôt des **programmes de surveillance (comme PRISM ou UPSTREAM) sur la base de certifications annuelles** préparées par le procureur général et le directeur du renseignement national (DNI). » (considérant 109 de la décision, p 25)

125 Elle ajoutait que « les certifications qui doivent être approuvées par le FISC **ne contiennent pas d'informations sur les personnes à cibler individuellement** mais déterminent plutôt des catégories d'informations en matière de renseignement extérieur. Même si le FISC **n'évalue pas**, à l'aune d'une cause ou de tout autre critère, **si les personnes sont correctement ciblées** pour se procurer des informations en matière de renseignement extérieur, son contrôle s'étend à la condition qu'«un objectif important de l'acquisition soit d'obtenir des informations en matière de renseignement extérieur».

126 Par cette pratique, le FISC autorise un accès nécessairement large aux services de rensignement, et de surcroit s'interdit tout controle au delà de la seule constatation qu'un objectif **important** justifie la collecte, comme par exemple "des motifs raisonnables de penser qu'un moyen de communication spécifique est utilisé pour communiquer des informations en matière de renseignement extérieur", ce qui expose potentiellement tout moyen de communication à être surveillé (rapport de l'ACLU *précité*, §§32 à 35) (prod. n° **B.1**) .

127 Ce mécanisme autorise donc la définition *a priori* d'une large quantité de cibles de collecte, qu'il n'est pas possible de prendre individuellement, uniquement limitée par un objectif qui est également largement défini.

128 Par ailleurs, lorsque la collecte n'est en l'occurence pas justifié par l'objectif poursuivi, ce contrôle n'est en pratique pas effectif et ne permet pas de limiter l'accès aux données, malgré l'illégalité constatée de leur collecte.

129 En effet, le rapport de l'ACLU explique que le FISC se repose sur les faits rapportés par la communauté de renseignement elle-même pour être notifiée de violations, parfois plusieurs années après que les manquements aient commencé. Même lorsque certaines violations sont divulguées au FISC, les circonstances à l'orginie de ces problèmes peuvent perdurer pendant une certaine durée (voir rapport de l'ACLU *précité*, §§77 et 78). (prod. n° **B.1**)

130 La Cour FISC n'effectue donc aucunement un contrôle visant à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire.

131 **En conclusion**, le manque de garanties d'indépendance concernant respectivement les pouvoirs exécutif, législatif et judiciaire aurait dû empêcher la Commission de constater que les activités de renseignement des États-Unis sont subordonné à un contrôle préalable eectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux ns d'atteindre l'objectif poursuivi.

132 **Par conséquent,** la décision attaquée est entachée de très nombreuses et substantielles scories entraînant une atteinte disproportionnée aux droits fondamentaux des citoyens de l'Union européenne.

133 A tous égards, l'annulation est inévitable.

Par ces motifs, et tous autres à produire, déduire, suppléer, au besoin même d'office, les associations requérantes persistent dans les conclusions de leurs précédentes écritures.

Le 29 décembre 2017 à Leipzig,

M^e^ Alexis Fitzjean Ó Cobhthaigh

Avocat au barreau de Paris

Annexes

A. Annexes A.1 à A.15 : pièces communiquées dans la requête introductive

B. —

1. Rapport d'expert d'Ashely Gorski - ACLU
2. Avis du G29 du 28 novembre 2017 sur la révision annuelle du Privacy Shield
3. Avis 2016/01 du G29 du 13 avril 2016
4. Annexes du rapport de l'ACLU - Exhibit 1 à 13
5. Annexes du rapport de l'ACLU - Exhibit 14 à 44
6. Annexes du rapport de l'ACLU - Exhibit 45 à 50
7. Annexes du rapport de l'ACLU - Exhibit 50 à 51
8. Annexes du rapport de l'ACLU - Exhibit 52 à 74
9. Annexes du rapport de l'ACLU - Exhibit 75 à 126

Table des jurisprudences

CJUE, g^de ch., 8 avr. 2014, *Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres*, C-293/12, C-594/12

CJUE, g^de ch., 6 oct. 2015, *Maximilian Schrems contre Data Protection Commissioner*, C-362/14

CJUE, g^de ch., 21 déc. 2016, *Tele2 Sverige AB c. Postoch telestyrelsen et Secretary of State for the Home Department*, C-203/15, C-698/15