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 Me Alexis Fitzjean Ó Cobhthaigh
Avocat au Barreau de Paris
5 rue Daunou, Paris 2e (75002)
France

CONTRE

La France, la République Tchèque, les États-Unis, le Royaume Uni, l'Allemagne, Business Software Alliance, Microsoft, Digitaleurope, les Pays-Bas.

TABLE DES MATIERES

1. FAITS ET PROCEDURE

1. Dans l'affaire T-738/16, les parties suivantes ont entendu intervenir au soutien des conclusions de la commission :

La République française, par un mémoire du 18 décembre 2017, reçu le 31 janvier 2018 ;

La République fédérale d'Allemagne (ci-après, l'« Allemagne »), par un mémoire du 15 décembre 2017, reçu le 31 janvier 2018 ;

Le Royaume-Uni de Grande-Bretagne et d'Irlande du Nord (ci-après, le « Royaume-Uni), par un mémoire du 18 décembre 2017, reçu le 31 janvier 2018 ;

Les États-Unis d'Amérique (ci-après, « les États-Unis »), par un mémoire du 22 décembre 2017, reçu le 31 janvier 2018 ;

Microsoft Corp. (ci-après, « Microsoft »), par un mémoire du 22 décembre 2017, reçu le 31 janvier 2018 ;

La République tchèque, par un mémoire du 15 décembre 2017, reçu le 31 janvier 2018 ;

Le Royaume des Pays-Bas (ci-après, les « Pays-Bas »), par un mémoire du 18 décembre 2017, reçu le 31 janvier 2018 ;

Business Software Alliance (ci-après, « BSA »), par un mémoire du 22 décembre 2017, reçu le 31 janvier 2018 ;

DigitalEurope, par un mémoire du 22 décembre 2017, reçu le 31 janvier 2018.

Ces mémoires ne modifient en rien l'argumentation précédemment articulée par les exposantes, dont elles souhaitent expressément conserver l'entier bénéfice. Néanmoins, ces mémoires appellent, de leur part, les observations suivantes.

2. DISCUSSION – RECEVABILITE DE LA REQUETE

2.1 Sur le bénéfice procuré aux parties par l'annulation de la décision attaquée

2. L'État français soutient que les effets de l'annulation ici demandée ne sauraient avoir des conséquences juridiques ou procurer un bénéfice à la partie qui l'a intentée, écartant ainsi l'intérêt à agir des exposantes. L'État français considère que le lien existant entre le présent recours en annulation et le recours pendant devant les juridictions nationales des requérantes est trop distant et indirect. En outre, la circonstance que ladite annulation demeure hypothétique distancierait d'autant les effets juridiques dont les requérants pourraient bénéficier dans ce contentieux national.

3. De la même manière, Microsoft soutient que les contentieux nationaux évoqués par les requérantes n'apportent aucun élément établissant que les exposantes sont visées par les services de renseignement américains à travers le bouclier de protection des données de quelque manière que ce soit.

4. Rappelons que, **en droit**, afin d'être recevable, l'intérêt à voir annuler l'acte attaqué suppose qu'une telle **annulation soit susceptible, par elle-même, d'avoir des conséquences juridiques ou que le recours soit susceptible, par son résultat, de procurer un bénéfice** à la partie qui l'a intenté (voir, en ce sens, ordonnance du 22 novembre 2017, Digital Rights Ireland/Commission, T-670/16, EU:T:2017:838, point 20).

5. Or, **en l'espèce**, *d'une part*, le résultat du recours est bel et bien susceptible de procurer un bénéfice aux exposantes.

6. En effet, le contentieux évoqué par les requérantes concerne la conformité au droit de l'Union du droit français en matière de surveillance administrative. Or, le présent recours aura précisément pour effet de définir plus précisément ce droit, en ce que les juridictions de l'Union seront amenées à en préciser la portée pour évaluer la conformité de la décision d'adéquation présentement attaquée.

7. À ce titre, ce lien entre le contentieux national et européen est directement souligné par les intervenants.

8. En effet, Business Software Alliance (BSA, mémoire en réplique, § 33) fait valoir que *« de fait, les pouvoirs utilisés par les autorités publiques américaines pour obtenir l'accès aux données diffèrent très peu de ceux exercés au sein de l'UE. »* De surcroît, BSA pointe à cette occasion la pratique française *« de surveillance par boîte noire (…) permettant d'analyser un volume non précisé de trafics et de données de souscripteurs en temps réel afin d'établir de possibles liens terroristes »*, en faisant valoir une équivalence entre ce régime et celui existant aux États-Unis. C'est cette même pratique qui est questionnée

devant les juridictions nationales par les requérantes. La connexité entre ces deux contentieux ne saurait être plus ouvertement établie.

9. Partant, l'obtention d'une interprétation sur la conformité au droit de l'Union par les pratiques de renseignements des États-Unis aurait une incidence directe sur le recours national porté par les exposantes en cas d'annulation de la décision attaquée sur ce fondement.

10. De plus, les précisions apportées par une juridiction de l'Union européenne sur un droit dont l'application appelle des précisions, surtout dans un contexte où la juridiction nationale a refusé de transmettre des questions préjudicielles très liées, ne peut qu'être regardé comme procurant un bénéfice *certain* aux requérantes ayant formé ce recours.

11. En outre, en la matière, il est primordial que ces questions bénéficient d'une interprétation unifiée sur l'ensemble du territoire de l'Union européenne et ce, le plus tôt possible.

12. *D'autre part*, il est acquis que l'annulation de la décision attaquée est susceptible d'avoir des effets juridiques en ce qu'elle fera cesser les atteintes que celle-ci vient porter notamment au droit à la vie privée et à la protection des données personnelles des personnes physiques représentées par les requérantes.

13. **En conclusion**, l'existence d'un recours devant les juridictions nationales susceptible d'être éclairé et auquel peut être apporté des fondements juridiques supplémentaires, ne peut qu'être regardé comme procurant un bénéfice aux parties exposantes dans la mesure où les conséquences de cette procédure devant les juridictions européennes pourrait augmenter sensiblement la probabilité que leur argumentation, fondée sur l'interprétation des exigences du droit de l'Union en la matière, soit justement prise en compte par le juge national.

2.2 Sur la faculté de représentation par les requérantes de leur membres et salariés

14. L'État allemand soutient que les requérantes se borneraient à invoquer la violation générale des droits de tiers qui ne leur auraient pas cédés lesdits droits, rendant leur action irrecevable.

15. Devant cette argumentation, les exposantes renvoient à leurs précédentes écritures (mémoire en réplique, § 5 et suivants), qui réfutent déjà pleinement ces vaines allégations.

2.3 Sur l’affectation directe des intérêts des requérantes

16. **À titre introductif**, la République tchèque prétend que les requérantes ne bénéficient pas de l’habilitation nécessaire pour invoquer une violation des droits des tiers et, en l’occurrence, des salariés et membres des associations exposantes. Elle soutient à ce titre qu’une telle habilitation ne pourrait être déduite de la seule qualité de membre ou salarié ni de la *« large faculté de représentation »* de leur membres conférée aux requérantes dans leur statuts. De cette manière, la République Tchèque allègue que le critère d’affectation directe dont dépend l’intérêt à agir des requérantes doit être apprécié au regard de la violation des droits propres des associations exposantes.

17. Or, comme il a été précédemment souligné, par renvoi aux écritures précédentes, La Quadrature du Net, ainsi que FDN et la Fédération FDN prévoient dans leur statuts une faculté de représentation de leurs membres personne physiques, lesquels sont directement affectés par la décision attaquée. Leur situation juridique, et notamment leur droit à la vie privée et à la protection de leurs données personnelles, ne saurait être plus directement altérée.

18. Mais encore, les requérantes bénéficient d’un intérêt propre à agir, en raison de la violation de leurs droits propres.

2.3.1 L’affectation directe des droits propres des requérantes

19. L’Allemagne allègue que les requérantes n’auraient évoqué aucune violation de ses droits propres, en tant qu’association.

20. La République Tchèque et la France soutiennent que le désavantage concurrentiel pour les requérantes induit par la décision attaqué est insuffisamment étayé et ne saurait, en tout état de cause, justifier le caractère « direct » de l’affectation des droits des associations exposantes en ce qu’un tel désavantage n’altérerait pas leur *situation juridique*. Plus précisément, la République Tchèque se prévaut de ce que la circonstance que l’acte attaqué « puisse avoir des répercussions sur les possibilités de commercialisation » des services électroniques et numériques proposés par les requérantes ne porterait atteinte qu’à leur situation *de fait*.

21. Rappelons que, **en droit**, le caractère « direct » de l’affectation des droits des requérants à un recours en annulation devant le Tribunal exige " premièrement, que la mesure incriminée produise **directement des effets sur la situation juridique du particulier** et, deuxièmement, qu’elle ne laisse aucun pouvoir d’appréciation aux destinataires de cette mesure chargés de sa mise en œuvre, celle-ci ayant un caractère purement automatique et découlant de la seule réglementation incriminée sans application d’autres règles intermédiaires" (affaire T-262/10 *Microban International Ltd et Microban (Europe) Ltd contre Commission européenne*).

22. L'argumentation des intervenants se concentre sur le premier critère, tiré des effets produits sur la situation juridique et c'est sur ce point qu'entendent répondre les exposantes. Pour le surplus, il convient de renvoyer aux développements du mémoire en réplique adressé par les requérantes à la Commission.

23. Or, **en l'espèce**, contrairement à ce que prétend la République Tchèque, ce ne sont pas les *possibilités* de commercialisation qui sont susceptibles d'être affectées par la décision attaquée mais ses *conditions* de commercialisation, en créant une rupture d'égalité entre les acteurs économiques soumis au droit de l'Union, plus exigeant, et ceux relevant du droit des États-Unis moins protecteur.

24. Car, au sujet du Privacy Shield, tel qu'il a été relevé par le Conseil national du numérique français :

*« À la question – essentielle – du respect de la vie privée des citoyens européens s'ajoutent des « **considérations plus économiques** ». Celles-ci ne sauraient être négligées. »*[1]

25. À ce titre, il poursuit en soulignant que dans le cadre du Bouclier, « *les contrôles, particulièrement faibles, liés aux mécanismes d'auto-certification ont pu entraîner une perte de compétitivité pour les entreprises européennes, soumises à des exigences plus strictes*. »[2]

26. De cette manière, les entreprises américaines ayant adhéré au Privacy Shield bénéficient des données des citoyens de l'Union – lesquelles revêtent une valeur économiques considérable – alors même que le degré de protection qu'elles doivent garantir à ces données est bien plus faible et bien moins contraignant que celui imposé aux acteurs de l'Union européennes proposant des services analogues, à l'image des requérantes.

27. En outre, la situation des membres personne physique et des requérantes que sont les fournisseurs d'accès internet (FAI) est altérée du fait de leur relation contractuelle si le marché des communications électroniques européen impose aux FAI plus d'efforts et de charges que le marché américain, afin d'assurer une plus grande sécurité de la confidentialité des communications. La décision attaquée, en facilitant les échanges avec un pays moins exigeant en termes de protection de la confidentialité des communications a pour effet de perturber l'équilibre économique de ces FAI.

28. **En conclusion**, la rupture d'égalité dans les conditions d'exercice de l'activité économique des requérantes en tant qu'elles sont soumises à un droit plus exigeant que celui des entreprises ayant adhéré au Privacy Shield et bénéficiant néanmoins du transfert de données

---

1 Conseil national du numérique, "Pourquoi le Privacy Shield doit être renégocié", *Communiqué*, 19 septembre 2017. Disponible à l'adresse : https://cnnumerique.fr/pourquoi-le-privacy-shield-doit-etre-renegocie

2 *Ibid.*

des citoyens de l'Union ne peut qu'être regardée que comme affectant leur situation juridique et ce de façon suffisamment directe.

29. Enfin, **à titre infiniment subsidiaire**, la circonstance que le Privacy Shield implique, tel qu'il sera démontré ci-après, une surveillance généralisée des citoyens européens doit être prise en compte dès le stade de la recevabilité. **Une ingérence d'une telle ampleur** devrait, en toute hypothèse, justifier que soit reconnu l'intérêt à agir des requérantes.

30. Pour rappel, les enjeux sont de taille puisqu'à ce jour la population européenne traite et conserve numériquement la quasi-totalité de son capital informationnel. Du fait de leur caractère souverain, les activités des services de renseignement ne sont que trop peu régulées.

31. Cet élément est à la source de l'attaque internationale WanaCrypt, ayant infecté des millions d'ordinateurs d'entreprises et de particuliers le 12 mai 2017. Le programme malveillant (*malware*) dérobé aux services de renseignement américains[3] a eu pour conséquence de retarder les opérations de patients du service national de santé anglais[4].

32. De même, les services américains ont collaboré avec les services anglais en s'introduisant frauduleusement dans un routeur du fournisseur d'accès à internet belge Belgacom, afin de pouvoir collecter et utiliser les données de communication de la Commission européenne et du Parlement européen[5].

---

[3] « Les cyber-attaques de vendredi semblaient être la première fois qu'une cyber-arme développée par la NSA, financée par les contribuables américains et volée par un adversaire avait été lâchée par des cybercriminels contre des patients, hôpitaux, entreprises, gouvernements et citoyens» *("The cyber-attacks on Friday appeared to be the first time a cyberweapon developed by the N.S.A., funded by American taxpayers and stolen by an adversary had been unleashed by cybercriminals against patients, hospitals, businesses, governments and ordinary citizens*"), extraits de l'article de D. Sanger et N. Perlroth, "Hackers Hit Dozens of Countries Exploiting Stolen N.S.A. Tool", *New York Times* (New-York, 12 mai 2017) disponible en ligne https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html, consulté le 12 mai 2017.

[4] Article de D. Gayle, A. Topping, I. Sample, S. Marsh et V. Dodd, "NHS seeks to recover from global cyber-attack as security concerns resurface" *the Guardian* (Londres, 13 mai 2017) https://www.theguardian.com/society/2017/may/12/hospitals-across-england-hit-by-large-scale-cyber-attack, consulté le 3 juin 2017.

[5] Dans deux des documents Snowden le plus important opérateur de télécommunications belge, Belgacom est décrit comme ayant été attaqué par les services anglais dans le cadre de leur collaboration avec les services américains. Une présentation interne de2011 par QCHQ indique: « Objectif ultime - permettre l'accès CNE [c'est à dire "Computer Network Exploitation", aussi appelé hacking ou atteintes aux systèmes de traitement automatisé de données] aux routeurs GRX de base BELGACOM » https://search.edwardsnowden.com/docs/MobileNetworksinMyNOCWorld2014-12-13nsadocs.
Parmi les clients de Belgacom figurent la Commission européenne et le Parlement européen. Voir l'article de R. Gallagher, "Operation Socialist The Inside Story of How British Spies Hacked Belgium's Largest Telco" *the Intercept* (13 décembre 2014). Disponible en ligne https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/, consulté le 3 mars 2018.

33. Pour les requérantes offrant un service d’accès à internet, il est absolument critique de pouvoir se reposer sur un droit européen qui encadre les activités étatiques ayant un impact sur leurs activités économiques. Pour cela, les requérantes luttent pour le renforcement de la protection de la confidentialité des communications ainsi que l’interprétation des garanties fondamentales consacrées par la Charte.

3. DISCUSSION – FOND DE LA REQUETE

3.1 Propos introductifs

3.1.1 Contexte de l'arrêt Schrems

34. **À titre liminaire**, plusieurs parties intervenantes telles que le Royaume-Uni (RU) (paragraphe 10) confortent le mémoire de la Commission dans son souhait de rappeler que le contexte dans lequel a été rendu l'arrêt *Schrems* (CJUE, gde ch., 6 oct. 2015, *Schrems*, C-362/14) doit s'apprécier dans la présente affaire. Le paragraphe 27 dudit arrêt énonce que « toute personne résidant sur le territoire de l'Union et désirant utiliser Facebook est tenue de conclure, lors de son inscription, un contrat avec Facebook Ireland, filiale de Facebook Inc., elle-même établie aux États-Unis. Les données à caractère personnel des utilisateurs de Facebook résidant sur le territoire de l'Union sont, en tout ou en partie, transférées vers des serveurs appartenant à Facebook Inc., situés sur le territoire des États-Unis, où elles font l'objet d'un traitement. »

35. Or, compte tenu du « droit et [d]es pratiques » états-uniennes, la CJUE a estimé que la surveillance américaine n'était pas assujettie à des critères objectifs. Les faits d'espèce mettent en exergue les mêmes enjeux tranchés par les juges de l'Union. Les requérantes dénoncent que toute personne physique résidant sur le territoire de l'Union ayant contracté avec un fournisseur de services américain s'expose à ce que ses données soit transférées aux États-Unis pour la réalisation du service ou la sauvegarde (ou *backup*) des données.

36. Il incombe aujourd'hui au juge européen de s'assurer que le droit américain présentait des critères objectifs lors de la décision de la Commission européenne créant le Bouclier de protection (ou *Privacy Shield*).

37. En application du paragraphe 33 de la décision Schrems, ces critères objectifs, pour être garants d'une surveillance à l'image d'une société démocratique, doivent également être justifiés dans les mêmes conditions.

38. Or, les associations exposantes se sont appuyées, en particulier, sur les motifs retenus par la grande chambre de la Cour de justice développées dans l'arrêt *Schrems* (reprenant par analogie l'arrêt CJUE, gde ch., 8 avr. 2014, *Digital Rights Ireland*, C-293/12, C-594/12) et qui constituent le soutien nécessaire du dispositif de cet arrêt, dès lors que la Cour a soigneusement pris en compte les circonstances tenant au droit états-unien que la décision 2000/250 de la Commission a été annulée.

3.1.2 Prise en compte de l'amélioration du droit des États-Unis

39. La République Tchèque fait valoir que les requérantes omettent « l'amélioration indubitable de la protection des personnes concernées à la suite de toute une série de nouvelles mesures de production des particuliers introduites par la décision attaquée dans son ensemble ».

40. Pourtant, Věra Jourova, commissaire européenne à la Justice, qui a elle-même signé la décision attaquée, déclarait le 29 janvier 2018[6] :

« L'Ombudsperson permanent (Médiateur), qui doit permettre aux Européens de faire valoir leurs droits, n'a toujours pas été nommé. Et la plupart des postes du comité de surveillance de la vie privée et des libertés civiles (Privacy and Civil Liberties Oversight Board) sont vacants. »

« Nous devons avoir une discussion sérieuse avec les Américains. Ils doivent agir. Quand j'y étais il y a un an, les postes clés n'étaient pas encore pourvus. Je le comprends très bien. Ils avaient eu peu de temps et ce sont de hautes fonctions, qui nécessitent une validation du Sénat. De longs mois ont passé depuis, et ma patience a des limites. »

3.1.3 Appréciation dans le cadre d'un constat d'adéquation

41. Au point 31 de son mémoire Digital Europe expose que :

« *La Demande ne conteste que l'évaluation d'adéquation par la Décision en ce qui concerne le droit sur la surveillance américain. Elle ne conteste aucun élément de fond du Bouclier de protection, ni le contenu des Principes relatifs à la protection des données à caractère personnel eux-mêmes* ».

42. Cet argument résume malgré lui la démarche entreprise par les requérantes, qui consiste à démontrer que les constations de la Commission ne permettent pas de démontrer que les États-Unis assurent un niveau de protection adéquat permettant le transfert des données des ressortissants de l'Union. Au vu de la législation de cet État et de la manière dont elle est appliquée par le gouvernement états-unien, la Commission aurait dû aboutir des conclusions différentes.

43. C'est là tout le sens des écritures, précédentes et présentes, des requérantes. Sur la signification du constat d'adéquation, les requérantes renvoient ainsi directement aux développements de la partie I de leur réplique à la Commission (§§ 3 à 12).

---

6 Voir « Vera Jourova : Sur le Privacy Shield, ma patience a des limites », publié le 29 janvier 2018 sur le site https://context.com

3.1.4 Contexte de la sécurité nationale

44. La République tchèque (jointe par le Royaume-Uni et l'Allemagne en des termes similaires) prétend qu'il n'y a pas lieu « d'apprécier le niveau de protection garanti par un pays tiers, en matière de traitement des données à caractère personnel en rapport avec la garantie de la sécurité nationale à la lumière des exigences découlant de la jurisprudence » de la Cour de justice de l'Union européenne (jurisprudence sur laquelle les requérantes fondent leurs moyens).

45. Or, les atteintes permises au nom de la sécurité nationale doivent aussi être considérées dans l'évaluation de l'adéquation d'un droit étranger à celui de l'Union. En effet, le règlement 2016/679 (règlement général sur la protection des données), entré en vigueur deux mois avant la décision attaquée, précise à son considérant 104, sans aucune ambiguïté, que « la Commission devrait, dans son évaluation d'un pays tiers, d'un territoire ou d'un secteur déterminé dans un pays tiers, prendre en considération la manière dont un pays tiers déterminé respecte l'état de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, ainsi que sa législation générale et sectorielle, y compris la législation sur la sécurité publique, la défense et la **sécurité nationale** ainsi que l'ordre public et le droit pénal ».

46. Cette exigence est le simple reflet législatif de l'arrêt Schrems, rendu un an et demi avant l'adoption de ce règlement. L'arrêt reprochait précisément à la décision d'adéquation 2000/520 d'avoir constaté certaines atteintes aux libertés fondamentales permises en droit des États-Unis au nom de la sécurité nationale tout en échouant à en constater les garanties qui en assureraient la proportionnalité. Pour parvenir à cette conclusion, la Cour de justice relevait notamment que :

- § 87, « la décision 2000/520 […] rend ainsi possible des ingérences, fondées sur des exigences relatives à la **sécurité nationale** et à l'intérêt public ou sur la législation interne des États-Unis, dans les droits fondamentaux des personnes dont les données à caractère personnel sont ou pourraient être transférées depuis l'Union vers les États-Unis » ;
- § 88, « la décision 2000/520 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, ingérences que des entités étatiques de ce pays seraient autorisées à pratiquer lorsqu'elles poursuivent des buts légitimes, tels que la **sécurité nationale** » ;
- § 90, « les autorités américaines pouvaient accéder aux données à caractère personnel transférées à partir des États membres vers les États-Unis et traiter celles-ci d'une manière incompatible, notamment, avec les finalités de leur transfert, et **au-delà de ce que qui était strictement nécessaire et proportionné à la protection de la sécurité nationale** » ;

47. Les juges ont donc invalidé la décision d'adéquation 2000/520, ayant conclu que « le droit et les pratiques en vigueur dans ce pays ne garantissaient pas une protection suffisante des données » (*Schrems*, paragraphe 28). L'arrêt Schrems met en exergue qu'en droit européen la sécurité nationale n'est pas une finalité permettant de justifier de sortir du champ d'application de la Charte des droits fondamentaux de l'Union telle qu'interprétée par les juridictions de l'Union.

3.2 Moyens

3.2.1 En ce qui concerne la nature des collectes autorisées par le droit des États-Unis

48. À la partie IV. A de son mémoire en intervention, le gouvernement des États-Unis soutient que la législation états-unienne interdirait la collecte en vrac auprès des entreprises du bouclier de protection des données.

49. L'État tiers décrit, en ce sens, le protocole prétendument suivi par les services de renseignements lors de collecte d'informations. Selon ses développements, une telle collecte ne serait permise qu'après demande auprès des entreprises membres du Bouclier de Protection établies aux États-Unis (IV.A.1 du mémoire), laquelle serait limitée par les lois des États-Unis qui interdiraient toute collecte en vrac (IV.A.2 du mémoire).

50. Ces allégations ne résistent nullement à l'analyse.

51. En effet, le gouvernement des États-Unis donne ici une description tronquée et faussée des limitations existantes dans le cadre juridique applicable à une collecte de données. Il tente vainement d'omettre un texte primordial en matière de renseignement : le décret présidentiel 12333 ou "Executive Order 12333" (ci-après l'EO 12333, produit en annexe n° 2 du rapport de l'ACLU, pièce B.5 en annexes du mémoire du 23 janvier 2018) pourtant appliqué à l'ensemble des transferts de données concernés par la décision attaquée.

52. De plus, le gouvernement des États-Unis refuse de constater l'insuffisance substantielle des limitations du Foreign Intelligence Surveillance Act (ci-après le FISA).

53. Or l'application de ces deux textes permet *de fait* une collecte généralisée de données contraire au droit de l'Union. Ainsi, il convient d'analyser successivement ces deux textes.

3.2.1.1 L'Executive Order 12333

54. En ce qui concerne l'Executive Order (EO) 12333, son analyse appelle quelques propos introductifs. Cet instrument du droit américain n'est mentionné à aucune reprise dans le mémoire en intervention des États-Unis et ne l'est pas davantage dans le mémoire en réplique de la Commission ni dans aucune des écritures présentées par les parties intervenantes à son soutien.

55. Pourtant, au considérant 68 de la décision attaquée, lorsque la Commission européenne constate l'existence des différents textes de loi régissant le renseignement extérieur aux États-Unis, celui-ci y est logiquement bien mentionné :

« Actuellement les deux instruments juridiques essentiels à cet égard sont ***le décret présidentiel n°12333*** *et la directive stratégique présidentielle n°28 (Presidential Policy directive 28) ».*

56. La Commission y décrit l'EO 12333 en ces termes :

« Le décret présidentiel définit les objectifs, les orientations principales, les missions et les responsabilités des activités de renseignement des États-Unis (y compris le rôle des diverses composantes de la communauté du renseignement) et ***établit le cadre général de la conduite des activités de renseignement*** *(en particulier, la nécessité de promulguer des règles procédurales propres). Conformément à l'article 3.2 de l'E.O. 12333, le président, assisté par le Conseil national de sécurité, et le DNI publient les* ***directives, procédures et orientations appropriées qui sont nécessaires à la mise en œuvre du décret****"»* (note de bas de page n° 59, p 13 de la décision attaquée*).*

57. Par ailleurs, dans une des lettres de recommandations de l'ODNI (annexe VI de la décision attaquée, p. 90), le conseiller général Riber Litt fait mention de ce décret lorsqu'il décrit le cadre juridique des États-Unis :

« Une mosaïque de lois et de politiques régissent la collecte de renseignements d'origine électromagnétique par les États-Unis, et notamment la constitution américaine, la loi sur la surveillance du renseignement étranger (50 U.S.C. § 1801 et suivants) (Foreign Intelligence Surveillance Act, FISA), ***le décret exécutif 12333 et ses procédures d'exécution****, l'orientation présidentielle et de nombreuses procédures et lignes directrices, approuvées par la Cour FISA et le procureur général, qui établissent des règles supplémentaires limitant la collecte, la conservation, l'utilisation et la diffusion de renseignements étrangers. »*

58. Ainsi, l'étude de ce texte pour évaluer l'adéquation du droit des États-Unis en matière de traitement des données transférées ne saurait être valablement écartée. Alors qu'il est manifeste que ce texte constitue une partie importante de la source de renseignement des États-Unis et nécessite d'être pris en compte dans l'analyse du constat d'adéquation, les États-Unis n'en font pas état dans leur mémoire, afin de restreindre le débat et d'écarter l'étude de la collecte en vrac permise par l'EO 12333.

59. Cependant, cette omission est grave dans la mesure où l'application de ce texte concerne directement les transferts du Bouclier et, de surcroit, permet une collecte de donnée à caractère généralisé par les États-Unis.

60. Il convient ainsi d'établir que l'EO 12333, contrairement à ce qui est allégué, entre bel et bien dans le champ du constat d'adéquation qui doit être dressé par la Commission, avant d'étudier l'ingérence dans les droits fondamentaux des citoyens européens induite par son régime.

3.2.1.1.1 Le champ d'application de l'EO 12333

61. Dans la décision attaquée, si la Commission constate l'existence de l'EO 12333, elle ne fait nullement état des débats relatifs à l'étendue de son champ application ni de ses liens avec les transferts permis par le Bouclier.

62. Pourtant, ce point a retenu l'attention d'une pluralité d'acteurs lors de l'examen annuel de révision du Bouclier et a suscité de vives inquiétudes. En effet, dans son document de travail joint au rapport de révision annuelle en date du 18 octobre 2017, la Commission décrivait :

« Dans leurs contributions envoyées à la Commission en vue de préparer l'examen de révision annuelle, des organisations non gouvernementales ont fait part de leurs inquiétudes en ce qui concerne la collecte de renseignement électromagnétique par l'EO 12333. Lors de la révision annuelle, la Commission a dès lors demandé des clarifications supplémentaires auprès des autorités américaines sur ce point, et particulièrement sur sa pertinence dans le cadre du Privacy Shield. » [7]

7 Traduction libre de : "*In their submissions sent to the Commission in preparation of the annual review, NGOs have raised concerns with respect to signals intelligence collection under Executive Order (E.O.) 12333. At the Annual Joint Review, the Commission therefore asked the U.S. authorities for further clarifications on this point, especially its relevance for the Privacy Shield. The U.S. authorities (ODNI/DoJ) confirmed that the collection of personal data for national security purposes from companies that have received such data under the Privacy Shield framework can only take place based on FISA or one of the statutory bases for NSLs, in line with the Commission's findings*" (Partie 4.2.1.2., p 23 du document de travail). Disponible à l'adresse : http://ec.europa.eu/newsroom/document.cfm?doc_id=47799.

63. Consécutivement, le groupe des autorités de contrôle européennes de l'Article 29 (ci-après le G29) précise dans son rapport en date du 28 novembre 2017 (pièce n° B.1 citée dans le mémoire en réplique du 23 janvier 2018) :

«Lors de l'examen de révision, les autorités des États-Unis ont souligné que l'EO 12333 ne pourrait pas être utilisé comme fondement d'une collecte de données à l'intérieur du territoire des États-Unis et qu'ils considéraient que la collecte permise par ce texte ne rentrait pas dans le champ du Privacy Shield.»[8]

64. Or, de telles déclarations sont manifestement erronées et empêchent d'établir correctement le constat d'adéquation requis par le droit de l'Union européenne.

3.2.1.1.1.1 Les transferts rentrant dans le champ d'application de l'EO 12333

65. L'EO 12333 est le fondement principal sur lequel la National Security Agency (NSA) recueille des informations à des fins de renseignement extérieur. Il permet au gouvernement d'entreprendre, avec une grande latitude, la surveillance des citoyens américains et étrangers.

66. S'il est certes vrai que la surveillance permise en application de l'EO 12333 est largement conduite en dehors du territoire des États-Unis, il est tout aussi vrai que certaines collectes sont effectuées sur le sol de cet État. En effet, en application de l'"International Transit Switch Collection" (ITSC) par "l'Autorité de transit", les autorités des États-Unis collectent le trafic circulant dans **les câbles qui traversent le territoire et dont l'origine ou la fin se situe dans un pays étranger** (voir § 51 du rapport de l'ACLU, pièce B.3, notamment la note de bas de page n°56 p. 21, ainsi que son annexe n°53, pièce B.56).

67. Ainsi, il a pu être démontré que la NSA interceptait des informations directement dans les câbles de fibre optique, au niveau des « points de congestion » hors du territoire, c'est à dire des jonctions par lesquelles passent de vastes quantités de communications (§ 62 p. 26 et annexe n°66 du rapport de l'ACLU, pièce B.3 et B.69).

---

8 Traduction libre de : "*During the Joint Review, the U.S. authorities underlined that Executive Order 12333 could not be used as a basis for collection of data inside the U.S. territory and that they consider that collection of data under this Executive Order falls outside the scope of the Privacy Shield*" (partie 1.2, page 16 de l'avis).

3.2.1.1.1.2 Les transferts rentrant dans le champ d'application du Bouclier

68. Dans son mémoire, le gouvernement des États-Unis prétend que seul *l'accès* aux données, sur requête des services de renseignements adressée aux entreprises membres du Bouclier de Protection, serait concerné par les mesures du Bouclier (point 25 de leur mémoire).

69. Il exclurait ainsi l'application de l'EO 12333 du champ du Bouclier. Or, une telle assertion est résolument contraire à ce que prévoit la directive 95/46.

70. En effet, *en droit*, au point 75 de l'arrêt Schrems, la Cour de justice rappelle que « lors de l'examen du niveau de protection offert par un pays tiers, la Commission est tenue d'apprécier le contenu des règles applicables dans ce pays résultant de la législation interne ou des engagements internationaux de celui-ci ainsi que la pratique visant à assurer le respect de ces règles, cette institution devant, conformément à l'article 25, paragraphe 2, de la directive 95/46, prendre en compte **toutes les circonstances relatives à un transfert de données à caractère personnel** vers un pays tiers» (CJUE, gde ch., 6 oct. 2015, *Schrems*,C-362/14, § 75).

71. Ainsi, un transfert de données à caractère personnel ne peut être réduit à la seule demande d'accès par un service de renseignement d'une donnée détenue par une entreprise américaine mais, à l'inverse, inclut toutes les étapes depuis l'émission de cette donnée dans un État de l'Union européenne jusqu'à sa réception par l'entreprise américaine. Ce processus prend donc en compte le transit de cette donnée.

72. **En l'espèce**, de telles affirmations ne sont en rien contredites par la Commission dans ses constatations. À l'inverse, la décision d'adéquation tend à les corroborer. Précisément, au considérant 75 de la décision attaquée, concernant les limitations en matière de collecte, la Commission énonce que :

« Ces restrictions sont particulièrement appropriées pour les données à caractère personnel transférées dans le cadre du bouclier de protection des données UE-États-Unis, ***en particulier dans le cas où la collecte de données à caractère personnel devrait intervenir à l'extérieur des États-Unis, notamment lors de leur transit sur les câbles transatlantiques de l'Union vers les États-Unis.*** *»*

73. Dans la lettre de l'ODNI, cette pratique n'est pas davantage niée par le directeur général qui affirme que :

« En outre, 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 les exigences de la PPD-28 »* (Annexe VI, p 2).

74. Par ailleurs, dans son document de travail joint au rapport de révision annuelle, la Commission renvoie directement à ces affirmations de l'ODNI[9].

75. Enfin, dans son rapport rendu lors de l'examen annuel, le G29 reprenait sa position antérieure et affirmait clairement que le transfert de données devait prendre en compte l'étape ou la donnée était "en chemin" vers un pays :

*« Le G29 considère que l'analyse des lois du pays tiers pour lequel l'adéquation est considérée, ne devrait pas être limitée aux lois et à la pratique autorisant la surveillance **à l'intérieur de ses frontières physiques**, mais devrait aussi inclure une analyse des fondements légaux dans ce pays tiers qui permettent la mise en œuvre d'une surveillance **en dehors du territoire, pour autant que des données provenant de l'UE sont concernées**. Tel qu'il a déjà été souligné dans la précédente opinion, "Il devrait être clair que les principes du Privacy Shield vont s'appliquer à partir du moment où le transfert a lieu", ce qui implique d'inclure **les données qui sont en chemin ("on its way") vers ce pays** [mis en gras dans le texte d'origine]. C'est pourquoi le G29, dans son avis de l'année dernière, analyse l'Executive Order 12333 et la Presidential Policy directive (PPD 28), ce qui est d'autant plus important dans ce contexte puisqu'ils assurent les seules garanties et limites à la collecte et au traitement des données collectées en dehors des États-Unis dès lors que les limitations du FISA ou d'autres textes spécifiques ne s'appliquent pas ».*[10]

76. **En conclusion**, l'affirmation du gouvernement des États-Unis selon laquelle « l'article 25(1) de la Directive 25/46 ne réglemente pas - et ne saurait réglementer - le flux de données au niveau mondial, en fonction de l'éventualité que le pays de destination, ou tout autre gouvernement, puisse souhaiter acquérir des données à des fins de renseignement lorsque les données se trouvent en dehors de son territoire » est radicalement erronée, voire mensongère.

---

[9] Voir la note de bas de page n° 77, p. 23 du document de travail précité, disponible à l'adresse : http://ec.europa.eu/newsroom/document.cfm?doc_id=47799

10 Traduction libre de "*The WP29 is of the view that the analysis of the laws of the third-country for which adequacy is considered, should not be limited to the law and practice allowing for surveillance within that country's physical borders, but should also include an analysis of the legal grounds in that third country's law which enable it to conduct surveillance outside its territory as far as EU data are concerned. As already underlined in its previous opinion,"it should be clear that the Privacy Shield Principles will apply from the moment the data transfer takes place", which means including as regards **data "on its way" to that country** (mis en gras dans le texte d'origine). This is why the WP29, in the same opinion of last year, analysed the Executive Order 12333 and the Presidential Policy Directive 28 (PPD-28), which is all the more important in this context as it provides for the only safeguards and limits to the collection and use of data collected outside the U.S. as the limitations of FISA or other more specific U.S. law do not apply.* " p. 16 du rapport.

77. En effet, si les données en transit vers ou depuis les États-Unis entrent bel et bien dans le champ d'application de la décision contestée, ce « flux de données au niveau mondial » dans lequel les États-Unis pourraient collecter des informations relatives au renseignement ne saurait être écarté du champ de la directive 95/46 et donc du constat d'équivalence.

78. Ainsi, **dès lors que les services de renseignement des États-Unis utilisent l'Executive Order 12333 afin d'intercepter des informations** au niveau des câbles transatlantiques, par lesquels transitent des données transférées dans le cadre du Bouclier, **ce texte doit être pris en compte dans l'analyse du constat d'adéquation.**

79. Partant, il convient d'étudier les garanties prévues par ce texte, et de les comparer aux exigences d'adéquation requises par la directive 95/46, telles qu'exposées dans les précédentes écritures des requérantes (v. mémoire en réplique du 23 janvier 2018, §§ 3 à 12).

3.2.1.1.2 Le régime fixé par l'EO 12333 : Une collecte généralisée

80. **En droit**, 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 au droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte » (CJUE, gde ch., 6 oct. 2015, *Schrems*, C-362/14, § 94).

81. Ainsi, 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 (*Digital Rights Ireland*, C-293/12, C-594/12, point 57 cité au point 93 de l'arrêt *Schrems*, précité).

82. 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).

83. Or, **en l'espèce,** l'Executive Order, ainsi que les réglementations qui l'accompagnent, prévoient des limitations insuffisantes dans le cadre des collectes, et ce, à deux titres.

84. **En premier lieu**, la collecte mise en œuvre sur le fondement de l'EO 12333 s'applique à toutes les communications transitant entre les États-Unis et les États membres de l'Union européenne.

85. Comme il a été démontré ci-dessus, l'EO 12333 permet aux services de renseignement états-uniens d'intercepter des communications au niveau des câbles transatlantiques. Cela signifie que toutes les données en transit depuis les territoires des États membres peuvent être collectées à cet endroit.

86. Contrairement au FISA qui sera analysé ci-après, il n'existe aucun contrôle préalable à la collecte, les services de renseignement ne nécessitant alors pas d'autorisation judiciaire avant de mettre en œuvre une mesure de surveillance.

87. Il est dès lors manifeste que, par son champ d'application extrêmement large, l'EO 12333 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic.

88. **En second lieu**, les motifs prévus par la loi justifiant la collecte ne sont pas assez précis pour opérer une différenciation, limitation ou exception entre les données collectées.

89. L'EO 12333 a pour objectif général de donner aux services de renseignement la compétence de recueillir des informations relatives aux « politiques étrangères, de défense et économiques » des États-Unis, et particulièrement la lutte contre le terrorisme, l'espionnage et la prolifération des armes de destruction massive (voir §1.1 de l'EO 12333 en annexe B.5).

90. La Presidential Policy Directve n^{o} 28 (ci après « PPD 28 »), une directive présidentielle adoptée par le Président Barack Obama en janvier 2014 prévoit des principes généraux s'appliquant à la surveillance en matière de renseignement et notamment dans le cadre de l'EO 12333 (voir rapport de l'ACLU, § 63 p. 27, pièce B.3).

91. **Surtout**, il permet au gouvernement d'utiliser un type de collecte dite « en vrac ».

92. Pour rappel, la collecte en vrac est définie 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).

93. Cette définition laisse clairement transparaître que le nombre de cibles est quasiment illimité mais aussi que ces cibles ne sont pas nécessairement choisies grâce à des critères de différenciation, ouvrant ainsi la voie à une collecte généralisée.

94. Les constatations de la Commission sur le cadre permettant de cibler la collecte ne parviennent pas à démentir cette observation. Selon les observations de l'ODNI, la collecte en vrac serait ciblée au moins de deux façons :

« Premièrement, cette collecte portera toujours sur des objectifs liés au renseignement extérieur (..) et sera toujours focalisée sur les communications qui présentent un tel lien. (…) Deuxièmement, (…) les filtres et autres moyens techniques utilisés seront conçus de manière à cibler la collecte "aussi précisément que possible"» (Considérant 73 de la décision attaquée).

95. En effet, *d'une part*, la définition du renseignement extérieur est **particulièrement large**. Le paragraphe 3.5 (e) de l'EO 12333 la définit ainsi :

« [une] information relative aux capacités, intentions ou activités de gouvernements étrangers ou de leur démembrements, organisations étrangères, personnes étrangères ou les terroristes internationaux »[11].

96. *D'autre part*, les règles de ciblage ne sont pas suffisamment précises. Au considérant 70 de la décision attaquée, la Commission constatait que :

« l'élaboration et le choix des sélecteurs appropriés sont effectués au sein du cadre des priorités de contrôle du renseignement national (National Intelligence Priorities Framework, NIPF); ce cadre général garantit que les priorités en matière de renseignement sont fixées par des décideurs politiques de haut niveau et sont régulièrement réexaminées afin de rester adaptées aux menaces réelles pour la sécurité nationale et en tenant compte

---

11 « [*I]nformation relating to the capabilities, intentions, or activities of foreign governments or elements therof, foreign organizations, foreign persons, or international terrorists* », qui englobe des citoyens autres que des États-Unis, sans lien avec une menace de sécurité nationale.

des risques potentiels, y compris les risques d'atteinte à la vie privée. Sur cette base, les agents des différents services élaborent et établissent des règles spécifiques de sélection qui doivent collecter des renseignements extérieurs répondant aux priorités. Les règles de sélection, aussi appelées «sélecteurs», doivent être régulièrement réexaminées afin de voir si elles continuent de fournir des renseignements pertinents au regard des priorités.»

97. Selon le directeur du renseignement national, « *les priorités du NIPF sont formulées à un* ***niveau de généralité relativement élevé*** » (Lettre de l'ODNI, Annexe VI, p 4).

98. Dans la pratique, ce cadre de priorité s'étend à un champ large et extensible. Il a ainsi pu être qualifié de « matrice d'une surveillance généralisée », en raison de la latitude qu'il offre aux analystes des services pour fixer les cibles et pays ciblés par les mesures de renseignement (v. § 59 et les annexes 58, 59 et 60 du rapport de l'ACLU, p. 24, pièces B.3, B.61, B.62, B.63).

99. Aussi, une fois les données collectées, l'application de l'EO 12333 permet-elle la pratique dite de « recherche en vrac ». Cette technique permet à la NSA de chercher des informations de renseignement dans les communications interceptées grâce à une large gamme de mots clés. Ainsi, les données et contenus des communications de la population mondiale peuvent faire l'objet d'une surveillance en temps réel. Dans le cadre de l'EO 12333, les sélecteurs utilisés ne sont pas associés à des cibles en particulier, mais peuvent viser des noms de villes ou de partis politiques (§57 du rapport de l'ACLU, p. 23, pièce B.3).

100. L'EO 12333 est utilisé par le gouvernement des États-Unis pour entreprendre une collecte de données de citoyens de leur État mais aussi de ressortissants étrangers. Celles-ci ont mené à la collecte quotidienne de milliards de géolocalisation de téléphone et de 200 millions de messages textes (§61, p. 25, et annexes 61 et 62 du rapport de l'ACLU, pièces B.3; B.64 et B.65).

101. **En conclusion**, l'injonction de l'ODNI de cibler « aussi précisément que possible » une collecte dont la finalité est extrêmement étendue est bien trop laconique. L'objectif de ciblage poursuivi par cette injonction est alors vidé de toute effectivité. La collecte en vrac 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 »*. De plus, l'objectif poursuivi est trop large pour que soit opéré *« toute différenciation, limitation ou exception »* quant aux données collectées.

102. Ainsi, la collecte en vrac permise par l'EO 12333 doit nécessairement être qualifiée de collecte généralisée au regard des critères posées par la CJUE et, par suite, comme portant atteinte au contenu essentiel au droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte de l'Union.

3.2.1.2 La section 702 du FISA

103. Dans la partie 1.2 de son mémoire, le gouvernement des États-Unis présente les lois états-uniennes supposées interdire la collecte en vrac. Son analyse se concentre exclusivement sur les 'Lettres de sécurité nationale' (National Security Letter ou NSL) et le FISA. Parmi les dispositions qu'il évoque, seule l'analyse de la section 702 relative aux mesures de renseignement concernant les citoyens non américains est pertinente dans le cadre de la décision attaquée. En effet, celle-ci concerne les données des ressortissants de l'Union dans la mesure où elle autorise les services de renseignement des États-Unis à intercepter des communications *à l'intérieur* du territoire grâce à la coopération de fournisseurs d'accès. De plus, si cette collecte n'est techniquement pas qualifiée de « en vrac », le large nombre de cibles et la faiblesse des limitations des moyens de ciblage en font néanmoins une collecte indifférenciée au regard du droit de l'Union européenne.

3.2.1.2.1 Le champ d'application de la section 702 du FISA

104. Le FISA est un acte adopté en 1978 afin de donner un cadre aux activités de renseignement dont l'application serait contrôlée par une cour spécialisée : la Cour de Surveillance du Renseignement Étranger (*Foreign Intelligence Surveillance Court*, ci-après "Cour FISA"). A l'origine, le FISA exigeait que le gouvernement obtienne une autorisation individuelle de la Cour FISA avant de mettre en œuvre une technique de surveillance électronique sur le sol américain. Pour obtenir une telle autorisation, le gouvernement devait expliquer et décrire en détail la cible faisant l'objet de ces mesures de surveillance ainsi que la technique spécifique de communication à surveiller. La Cour FISA pouvait octroyer cette autorisation de surveillance s'il apparaissait notamment, qu'il existait *« une raison probable de croire que la cible [était] une puissance étrangère ou un agent d'une puissance étrangère »* et que *« chacun des équipements ou lieux où la surveillance électronique [était] conduite ou utilisée, ou d[evait] être utilisée, par une puissance étrangère ou un agent étranger »* (voir §25 et 26 du rapport de l'ACLU, p. 9, pièce B.3).

105. L'adoption en 2008 de la section 702 a significativement affaibli cette pratique. En effet, les amendements introduits (voir 50 U.S.C §1881a, annexe nº 3 du rapport de l'ALCU, pièce B.6) ont permis au gouvernement de pouvoir intercepter les communications internationales de citoyens américains sans autorisation individuelle, grâce à certaines entreprises – tels que des fournisseurs d'accès à internet et de télécommunications – à l'intérieur des États-Unis. De cette manière, **si la surveillance cible le sol américain, elle balaye toutefois un spectre beaucoup plus large que celle mise en œuvre traditionnellement par le FISA**. Ainsi, la section 702 permet au gouvernement d'intercepter des communications échangées entre des personnes se trouvant à l'intérieur des États-Unis et des personnes situées à l'étranger. Dans la décision d'adéquation, le directeur du renseignement national la décrit en ces termes : (Lettre de l'ODNI, annexe VI, p 8) :

« Elle autorise l'obtention de renseignements étrangers via le ciblage de ressortissants non américains se trouvant en dehors du territoire des États-Unis, avec l'assistance obligatoire des fournisseurs de services de communications électroniques américains. La section 702

autorise le procureur général et le DNI — deux responsables gouvernementaux nommés par le Président et approuvés par le Sénat — à soumettre des certifications annuelles à la Cour FISA. Ces certifications identifient des catégories spécifiques de renseignements étrangers à collecter, telles que des renseignements en rapport avec le contre-terrorisme ou les armes de destruction massive, qui doivent relever ***des catégories de renseignement étranger définies par la FISA****. »*

106. Les définitions auxquelles renvoient la lettre de l'ODNI démontrent ainsi que la section 702 autorise l'interception de communications dès lors qu'au moins un des interlocuteurs est un citoyen non américain à l'étranger afin d'obtenir des informations de « renseignement étranger »[12], et que cela constitue un « objectif important »[13] de la surveillance (voir §31 du rapport de l'ACLU, pièce B.3).

107. Au regard de la définition du 50 U.S.C §1801 (e) définissant le renseignement extérieur, le champ d'application de la surveillance mise en œuvre sous la section 702 est très large et peut avoir de nombreuses autres finalités que le seul contre-terrorisme et peut inclure, entre autres, toute information concernant les affaires extérieures des États-Unis.[14]

108. De plus, la section 702 autorise une surveillance qui n'est pas fondée sur le critère de « cause probable ». Le gouvernement n'a pas à démontrer que la cible des mesures est un agent d'une puissance étrangère, exerce une activité criminelle ou est liée même de manière lointaine avec le terrorisme. **La section 702 permet plutôt de cibler *n'importe quel* citoyen non américain situé hors des États-Unis pour obtenir des informations de renseignement extérieur**. (voir §34 du rapport de l'ACLU, p 13, pièce B.3). Ainsi, le cadre juridique s'appliquant à la définition du "renseignement extérieur" en tant que finalité de la collecte de données est d'une telle souplesse qu'il permet l'interception de données d'un très

---

12 voir 50 U.S.C. §1881 a(a), définissant le champ d'application de la section par le "ciblage de personnes présumées être situés hors des États-Unis pour obtenir des informations de renseignement étranger". Traduction libre de "*the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information*".

13 voir 50 U.S.C. §1881 a(g)(2)(A)(v) qui définit les critères d'obtention d'une autorisation de la FISC, notamment qu'un "objectif important de la collecte est d'obtenir des informations de renseignement extérieur". Traduction libre de "*a significant purpose of the acquisition is to obtain foreign intelligence information*".

14 Une information de renseignement extérieur ("f*oreign intelligence information*") est définie (en anglais) au §50 U.S.C §1801 (e) ainsi : " (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against— (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—(A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States.

grand nombre de communications de ressortissants de l'Union, sans que ceux-ci ne 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.

109. La collecte prévue par la section 702 concerne ainsi directement les ressortissants de l'Union européenne, dont les droits sont directement menacés par l'absence de garanties protectrices prévues par ce texte.

3.2.1.2.2 Le régime de la section 702 du FISA

110. **En droit**, tel qu'il a été exposé précédemment, la Cour de justice considère qu' « une réglementation permettant aux autorités publiques d'accéder de **manière généralisée** au contenu des communications électroniques doit être considérée comme portant atteinte au contenu essentiel au droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte » (CJUE, gde ch., 6 oct. 2015, *Schrems*, C-362/14, § 94).

111. Ainsi, 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 (*Digital Rights Ireland*, C-293/12, C-594/12, pt. 57 cité au pt. 93 de l'arrêt *Schrems*, précité).

112. **En l'espèce**, la section 702 du FISA n'est soumise qu'à une forme très limitée de contrôle juridictionnel, ce qui a pour effet de s'opposer à toute précision jurisprudentielle - pourtant nécessaire - dans la délimitation de la collecte. Dans la lettre de l'ODNI, le directeur du renseignement national poursuit sa description concernant les certifications annuelles de la Cour FISA :

« Les certifications doivent également inclure des procédures de «ciblage» et de « limitation » à examiner et approuver par la Cour FISA. Les procédures de ciblage servent à faire en sorte que la collecte ne soit effectuée que dans les limites prévues par la législation et selon la portée définie dans les certifications; les procédures de limitation, elles, visent à limiter l'ampleur de l'obtention, de la diffusion et de la conservation de données sur les ressortissants américains. »

113. **En premier lieu**, les procédures de ciblage prévues sont insuffisantes.

114. En effet, contrairement à la surveillance traditionnelle permise par le FISA, celle mise en œuvre sous la section 702 ne fait pas l'objet d'autorisations judiciaires individualisées. Le rôle de la Cour FISA y est étroitement circonscrit par le texte. Il consiste essentiellement à examiner ces procédures de ciblage qui constituent alors les seules garanties permettant de

limiter la collecte. Les dispositions de la section 702 exigent que les procédures de ciblage puissent permettre aux agents du gouvernement de « cibler des personnes dont il est raisonnable de penser qu'elles sont situées en dehors des États-Unis » et d'éviter « la collecte intentionnelle » de communications purement privées (50 U.S.C §1881a(d)). Il apparait donc clairement que les procédures de ciblage déterminent de manière trop générale les personnes susceptibles d'être ciblées par des mesures de surveillance ainsi que les techniques d'interceptions. En pratique, les procédures sont faibles et criblées d'exceptions (voir note de bas de page n° 23 au §33, p. 13 du rapport de l'ACLU, et ses annexes 32 et 33, pièces B.3 ; B.35 ; B.36).

115. Les procédures de ciblage pour le Federal Bureau of Investigation (FBI) et la NSA, récemment publiées par le gouvernement des États-Unis, donnent un large pouvoir aux autorités pour cibler les ressortissants étrangers situés hors du territoire étatsunien. Par exemple, la NSA doit « raisonnablement attester, en se fondant sur toutes les circonstances, que la cible est censée posséder, recevoir, et/ou **est susceptible** de communiquer des informations de renseignement extérieur concernant un pouvoir étranger ou un territoire étranger »(voir §42 , p. 18, et annexe 47 du rapport de l'ACLU, pièces B.3 ; B.50).[15]

116. Elles n'exigent pas non plus d'identifier auprès de la Cour FISA les « équipements, lieux, locaux ou propriétés » spécifiques où cette surveillance doit avoir lieu[16]. Ainsi, le gouvernement peut recourir à la surveillance au niveau de nœuds stratégiques de l'Internet, par lesquels passent les communications de millions de personnes, plutôt que des lignes téléphoniques ou adresses email individuelles (voir §35, p. 14, et l'annexe n° 36 du rapport de l'ACLU, pièces B.3 ; B.39).

117. **En second lieu**, la définition de renseignement étranger est si large qu'elle peut être interprétée de manière très extensive, ouvrant la collecte mise en œuvre sous la section 702 à un champ d'application très vaste.

118. Puisque la section 702 ne requiert la preuve d'aucune « cause probable », le gouvernement peut alors se contenter d'une simple autorisation de la Cour FISA pour intercepter un nombre incalculable de communications à chaque fois pendant l'année de sa validité. Il convient d'ajouter également que la mise en œuvre de la section 702 peut mener à une collecte « accidentelle » de communications de personnes non ciblées ou sans lien avec le renseignement extérieur. Cette pratique générant du contenu dit « inutile » par les analystes, pouvant concerner jusqu'à 9 personnes surveillées sur 10 (voir §41, p 17, et annexe 46 du rapport de l'ACLU, pièce B.3 ; B.49).

---

15 Traduction libre de "*reasonably assess, based on the totality of the circumstances, that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory*"

16 voir 50 U.S.C. §1881 a(g)(4) : e. Traduction libre de "*A certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition authorized under subsection (a) will be directed or conducted*."

119. Au considérant 81 de la décision attaquée, la Commission constate que l'article 702 du FISA « fournit la base pour deux importants programmes de renseignement menés par les agences américaines de renseignement (PRISM, UPSTREAM), des recherches sont effectuées de manière ciblée par le recours à différents critères de sélection qui identifient des moyens de communication spécifiques (…) mais non des mots clés ni même les noms des personnes ciblées » mais n'en tire aucune conclusions adaptée. D'abord, elle se focalise sur la recherche d'informations déjà collectées, sans examiner les limites de cette collecte -- ce qui est bien l'aspect le plus problématique de ces mesures. De plus, aussi bien les déclarations du gouvernement que les articles de presse ont démontré l'ampleur de ces deux programmes, notamment la capacité des services de renseignement à directement surveiller la **colonne vertébrale d'Internet** aux États-Unis, à savoir **l'infrastructure physique** qui transporte les communications de centaines de millions d'américains et de personnes à travers le monde, grâce à l'aide d'entreprises étatsuniennes (sur ce point, voir §§ 37 à 40, p. 14-17 du rapport de l'ACLU, pièce B.3).

120. **En conclusion**, les garanties prévues par la section 702 du FISA ne permettent pas de limiter la collecte si bien que celle-ci en acquiert un caractère généralisé. Les procédures ne permettent ni d'individualiser les mesures de surveillance, ni de les associer à un objectif précis. Tant les certifications annuelles que les procédures et définitions de ciblage sont imprégnées d'un niveau de généralité trop élevé pour que le cadre mis en place puisse suffire à limiter les ingérences engendrées par la collecte. Dès lors, la collecte mise en œuvre sur le fondement de la section 702 vise les communications d'un très large nombre de ressortissants de l'Union **sans qu'il soit possible de constater que celle-ci est soumise à des critères de « différenciation, limitation ou exception ».**

121. Ainsi, dès lors que les données personnelles des ressortissants de l'Union européenne sont transférées à des entreprises localisées aux États-Unis, celles-ci sont susceptibles d'être collectées par les services de renseignement aussi bien à l'extérieur du territoire, au niveau des câbles transatlantiques, qu'à l'intérieur du territoire sans que des garanties adaptées ne soient prévues pour en limiter la portée. Dès lors, un tel encadrement ne saurait constituer des garanties suffisantes dans le cadre d'un constat d'adéquation. À ce propos, les requérantes renvoient à leur mémoire en réplique.

122. Sur ce moyen, l'annulation est encourue.

3.2.2 En ce qui concerne l'exploitation des données collectées

123. Les parties intervenantes, notamment le gouvernement des États-Unis, font état de la réglementation supposée respecter le principe de limitation au strict nécessaire de l'exploitation de données (principe de minimisation).

124. Or, en l'espèce, il n'en est rien.

125. Sur ce moyen, les requérantes reprennent l'entièreté de leur argumentation développée dans leur réplique adressée à la Commission. Il apparait cependant nécessaire d'apporter des précisions factuelles quant aux deux types de collecte exposées ci-dessus, au regard des exigences posées par la jurisprudence de la CJUE. En effet, aucun des deux textes servant de fondement aux collectes ne limite lesdites exploitations des données collectées grâce à des critères objectifs ni ne restreint « 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. »

3.2.2.1 L'exploitation des données collectées sur le fondement de l'Executive Order 12333

126. Concernant l'EO 12333, la PPD 28 limite l'utilisation et la diffusion des données recueillies au moyen de la « collecte en vrac » fondée sur ce texte. Rappelons que cette collecte est mise en œuvre au niveau des câbles transatlantiques à l'extérieur du territoire des États-Unis, ce qui n'est en rien contesté par la Commission, qui constate l'application de cette directive au considérant 75 de la décision attaquée :

« *Comme l'ont confirmé les autorités américaines dans les observations de l'ODNI, les limitations et garanties prévues par ce bouclier, y compris celles énoncées dans la PPD-28, s'appliquent à ce type de collecte.* »

127. Or, il a été démontré que ces garanties ne sont pas effectives en pratique, tant les objectifs de cette directive sont formulés de façon vague (§§63 à 66 du mémoire en réplique). De plus, la rétention de données concernant des ressortissants étrangers a été conçue en fonction du seuil de protection des ressortissants des États-Unis. Or, il a été démontré la faiblesse de cette garantie tant la définition de « renseignement extérieur » est trop large (voir §§71 à 74 du rapport de l'ACLU, p. 30-31 pièce B.3) De plus, l'EO 12333 permet la conservation des données collectées pendant cinq ans, ou pour une période indéterminée si ces données sont chiffrées, sont liées à des exigences de renseignement extérieur, indiquent une menace sur une personne ou organisation ou sont relatives à la commission d'un crime, passé, en train d'être commis ou futur (voir rapport de l'ACLU §60, p. 25, pièce B.3).

128. Il est ainsi manifeste que, par leur manque de précision, de tels critères ne peuvent constituer des garanties objectivement fixées permettant de restreindre l'utilisation des données collectées.

3.2.2.2 En ce qui concerne l'exploitation justifiée par la cybersécurité

129. **En droit**, le principe de sécurité juridique constitue un principe général du droit communautaire depuis l'arrêt *Bosch* (affaire 13-61) du 6 avril 1962 de la Cour de justice des Communautés européennes (CJCE).

130.

En l'espèce, les parties intervenantes au soutien de la Commission européenne avancent que la surveillance qui n'est pas empêchée par la décision attaquée peut être justifiée par la protection de la cybersécurité. Le Royaume-Uni reconnaît que cet « objectif est nécessairement formulé en termes larges vu la nature variable et évolutive des menaces pour la cybersécurité. Cet élément ne le rend pas indûment "vague" » (point 20, page 7).

131. Il est crucial pour l'économie et la confiance européennes que des garanties solides soient attendues de la part des États-Unis. Si certaines notions ne peuvent être parfaitement précises, les droits fondamentaux avec lesquels elles sont en équilibre doivent être protégés par un arsenal adapté à la pratique. L'argument politique ou technologique ne doit pas être pouvoir être mis en balance avec les droits fondamentaux garantis par la Charte.

132. **En conclusion**, la finalité de cybersécurité est à la fois contraire au principe de sécurité juridique et aux exigences de précision des critères d'exploitation des données posées par la Cour de justice.

3.2.2.3 L'exploitation des données collectées sur le fondement de la section 702 du FISA

133. La collecte ciblée mise en œuvre sur le fondement de la section 702 du FISA est supposée être limitée par des procédures de limitation (ou minimisation). Celles-ci sont conçues pour limiter l'acquisition et la conservation, et interdire la diffusion d'information non publiques concernant des **ressortissants des États-Unis** sans leur consentement, en balance avec la nécessité, pour les États-Unis, d'obtenir, produire et diffuser des informations de **renseignement extérieur** 17 (50 U.S.C §1801(h) à laquelle renvoie la section 702 du FISA). D'une part, ces procédures ne concernent pas explicitement les ressortissants étrangers, qui ne font donc l'objet d'aucun texte spécifique. D'autre part, la définition du renseignement extérieur telle qu'elle est formulée dans le FISA, exposée précédemment, n'est pas suffisamment précise pour limiter les pouvoirs des services de renseignement :

134. En effet, la publication des procédures de minimisation de la NSA, du FBI, de la Central Intelligence Agency (CIA) et du Centre National de l'Antiterrorisme démontre que celles-ci fournissent au gouvernement un large pouvoir pour conserver, analyser et exploiter les données collectées. Par exemple, ces agences peuvent conserver des communications de manière indéterminée si celles-ci sont chiffrées ou s'il apparait qu'elles contiennent des informations de renseignement extérieur. Le gouvernement peut ainsi conserver dans ses bases de données des centaines de milliers de communications collectées sur le fondement de la section 702, même si les données qui ne font pas parties de ces catégories. Pendant cette période de conservation, ces communications peuvent être consultées et demandées

17 Traduction libre de "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information"

par des analystes pour des enquêtes criminelles mais également de renseignement (voir §43, p. 18, et annexe 48 du rapport de l'ACLU, pièces B.3 et B.51).

135. **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 fins précises, strictement restreintes et susceptibles de justifier l'ingérence ».

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

137. À cet égard, encore, la censure est acquise.

3.2.3 En ce qui concerne l'existence et les modalités de recours effectif

138. Les parties intervenantes soutiennent que la décision contestée permet aux ressortissants de l'Union européenne de disposer de recours effectifs pour contester toute violation de leur droit à la vie privée.

139. Les parties requérantes réitèrent entièrement l'argumentation qu'elles ont développée dans le mémoire en réplique à la Commission du 23 janvier 2018 (§§73 à 108). Elles se borneront, au cas présent, à ajouter que la majorité des recours, non seulement sont inadéquats, inadaptés et *in fine* défaillants, mais encore qu'ils ne s'appliquent qu'à une violation dans le cadre d'une collecte de données fondées sur la section 702 du FISA.

140. En effet, la Commission constate au considérant 115 de la décision attaquée :

« *Alors que les personnes physiques, notamment les personnes concernées de l'Union européenne, disposent donc d'un certain nombre de voies de recours lorsqu'elles ont fait l'objet d'une surveillance (électronique) illégale à des fins de sécurité nationale, il est également clair qu'au moins quelques bases juridiques pouvant être utilisées par les services de renseignement américains (comme l'E.O. 12333)* ***ne sont pas couvertes*** ».

141. Dès lors, il n'est pas douteux que toute collecte de données au niveau des câbles transatlantiques, mise en œuvre sur le fondement de l'EO 12333, ne peut être contestée en cas de violation. Or, cette collecte concerne potentiellement **tous les transferts** de données entre l'Union européenne et les États-Unis.

142. En ne tenant pas compte cette très grave possibilité, la Commission n'a pas tiré les conclusions qui s'imposaient pour son constat d'adéquation.

143. A tous égards, l'annulation est encourue.

3.2.4 En ce qui concerne l'existence d'un contrôle indépendant

144. Les parties intervenantes soutiennent que la réglementation des États-Unis prévoit qu'il existe un contrôle indépendant permettant de limiter l'accès aux données conservées par les autorités nationales compétentes, ainsi que leur utilisation, à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi.

145. Sur ce moyen, les parties requérantes réitèrent, à nouveau, l'entière argumentation qu'elles ont développée dans le mémoire en réplique à la Commission du 23 janvier 2018 (§§109 à 132). Il convient néanmoins de préciser que le contrôle judiciaire effectué par la Cour FISA quant aux certifications annuelles ne concerne que la collecte sur le fondement de la section 702 FISA (§§124 à 131 de la réplique). Dès lors, les données collectées "en vrac" sur le fondement de l'EO 12333 ne sont soumises à aucune forme de contrôle judiciaire qui limiterait l'accès et leur utilisation par les services de renseignement des États-Unis.

146. Compte tenu de l'ampleur de la collecte en vrac, le contrôle existant ne peut qu'être qualifié que de parcellaire, voire anecdotique. Il est dès lors impossible de constater l'existence de tout contrôle indépendant au regard des exigences de la CJUE, entraînant une atteinte disproportionnée aux droits fondamentaux des citoyens de l'Union européenne.

147. A tous égards, l'annulation est inévitable.

148. **Enfin**, pour le surplus des remarques de l'intervention, les requérantes considèrent qu'il s'agit essentiellement d'observations au soutien d'arguments formulés par la Commission. Les requérantes renvoient donc à leur mémoire en réplique à cet égard.

* * *

149. **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.

A Paris, le 13 mars 2018

Pour La Quadrature du Net, la Fédération FDN et French Data Network

Me Alexis Fitzjean Ó Cobhthaigh
Avocat au Barreau de Paris

***