Recours en annulation (263 TFUE) contre la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016

I Parties

Parties requérantes :

La Quadrature du Net, association située au 60 rue des Orteaux, 75020 Paris, France

French Data Network, association située au 16 rue de Cachy, 80090 Amiens, France

Fédération FDN, association située au 16 rue de Cachy, 80090 Amiens, France

Représentant :

Hugo Roy, avocat au Barreau de Paris, P. 445

1 rue Paul Baudry, 75008 Paris, France

Partie défenderesse :

Commission européenne

II Objet

Demande d'annulation (telle que prévue par l'article 263 du traité sur le fonctionnement de l'Union européenne) de la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis.

III Conclusions

Les parties requérantes concluent à ce qu'il plaise au Tribunal :
- de déclarer la décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 contraire aux articles 7, 8 et 47 de la Charte des droits fondamentaux de l'Union européenne ;
- de prononcer l'annulation de cette décision.

IV Moyens et arguments

1 Recevabilité

1. Tout d'abord, l'activité des parties requérantes implique que leurs membres et employés soient actifs sur Internet et usent des services et logiciels développés par des entreprises ayant adhéré au Privacy Shield, telles que Microsoft et Google [1].

2. Ainsi, la décision attaquée permet le transfert par ces entreprises des données personnelles de ces personnes vers les États-Unis et leur soumission au droit de cet État, notamment en matière de surveillance. La situation juridique de ces individus en est donc nécessairement et directement modifiée de façon automatique et sans que d'autres règles intermédiaires n'aient à être adoptées (ordonnance rendue dans l'affaire *Northern Ireland Department of Agriculture and Rural Development c. Commission*, C-248/12 P, point 21). Les parties requérantes, représentant leur membres et employés, ont intérêt à agir de ce seul fait.

3. Par ailleurs, les parties requérantes sont engagées en France dans une procédure devant le Conseil d'État (affaires n° 394922, 394924, 394925 et 397851) contestant la conformité au droit de l'Union européenne du droit français encadrant les activités de surveillance. À cette occasion, les parties requérantes reprochent au droit français l'absence de garanties faisant aussi défaut au droit des États-Unis. En reconnaissant que le droit des États-Unis offre, en dépit de l'absence de ces garanties, une protection des droits et libertés fondamentaux équivalente à celle offerte par le droit de l'Union européenne, la décision attaquée met en péril le succès des moyens invoqués dans cette procédure française.

4. Pour chacun de ces motifs, l'intérêt à agir des associations requérantes ne fait aucun doute.

2 Premier moyen tiré du caractère généralisé des collectes autorisées par la réglementation des États-Unis

5. Dans sa décision du 6 octobre 2015 dans l'affaire C-362/14 (décision Schrems), la Cour de justice de l'Union européenne (CJUE) considère que la réglementation d'un État présente un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti dans l'Union européenne si et seulement si elle ne porte pas « atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte » (point 94 de la décision). La CJUE précise qu' « une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme

1. `https://europe.googleblog.com/2016/07/eu-us-privacy-shield-restoring-faith-in.html`

portant » une telle atteinte (même point 94 de la décision).

6. Or, la décision attaquée constate que :
   - « les composantes de la communauté du renseignement [des États-Unis] doivent parfois collecter des renseignements d'origine électromagnétique *en vrac* dans certaines circonstances, par exemple pour détecter et évaluer les nouvelles menaces ou les menaces émergentes » (considérant 72) ;
   - « lorsque la communauté du renseignement [des États-Unis] ne peut pas utiliser des identifiants spécifiques pour cibler la collecte, elle s'efforcera de réduire "autant que possible" le champ de la collecte » (considérant 73) ;
   - « la priorité est clairement donnée à une collecte ciblée, tandis que la collecte en vrac est limitée aux situations (exceptionnelles) dans lesquelles une collecte ciblée n'est pas possible pour des raisons techniques ou opérationnelles » (considérant 76).
7. Ces trois constats suffisent à révéler que tant la réglementation que la pratique des services de renseignement des États-Unis permettent « aux autorités publiques d'accéder de manière généralisée » (ici dite « en vrac », par opposition à « ciblée ») « au contenu de communications électroniques » (voir point 94 de la décision Schrems).

8. Ainsi, la réglementation des États-Unis « 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 » (voir point 94 de la décision Schrems), et comme ne pouvant présenter un niveau de protection des droits fondamentaux substantiellement équivalent à celui garanti dans l'Union. En tirant une conclusion contraire du constat auquel elle opère pourtant, la décision attaquée viole la Charte et doit être annulée de ce fait.

3 Deuxième moyen tiré de l'absence de limitation au stricte nécessaire des exploitations autorisées par la réglementation des États-Unis

9. Dans l'arrêt Schrems, la Cour de justice a également considéré que « n'est pas limitée au strict nécessaire une réglementation » qui ne prévoit aucun « *critère objectif* » permettant de *délimiter l'utilisation ultérieure* des données collectées à « des *fins précises, strictement restreintes et susceptibles de justifier l'ingérence* » que comporte telle utilisation (point 93 de la décision Schrems).

10. Or, la décision attaquée se contente de constater que la réglementation des États-Unis prévoit, à l'article 2 de la PPD-28, que, « dans les cas où les États-Unis jugent nécessaire de recueillir des renseignements d'origine électromagnétique en vrac » - et dans ces cas seulement -, l'utilisation des renseignements collectés est limitée à « une liste spécifique de six motifs ». Ces motifs concernent « les menaces liées à l'espionnage, au terrorisme et aux armes de destruction massive, les menaces pour la cybersécurité,

ainsi que les menaces contre les forces armées ou le personnel de l'armée et les menaces criminelles transnationales liées aux cinq autres motifs » (considérant 74).

11. D'une part, la limitation d'une mesure de surveillance à un motif aussi vague et général que la lutte contre les « menaces pour la cybersécurité » ne saurait être considérée être un critère objectif permettant de limiter telle ingérence à « des *fins précises, strictement restreintes et susceptibles de [la] justifier* ».

12. D'autre part, la décision attaquée ne constate aucune limitation apportée à l'exploitation des données collectées de façon ciblée, l'article 2 de la PPD-28 ne concernant que la collecte « en vrac ». Pourtant, la décision attaquée reconnaît à de nombreuses reprises que les États-Unis ne collectent pas systématiquement des données « en vrac » mais le font aussi de façon « ciblée ». Dès lors, la décision attaquée échoue à constater que la réglementation des États-Unis prévoit le moindre « *critère objectif* » permettant de *délimiter l'utilisation ultérieure* des données collectées » de façon ciblée tout en reconnaissant l'existence d'une telle collecte.

13. Pour ces deux raisons, la décision attaquée viole la Charte, devant être annulée de ce fait, lorsqu'elle constate que, en dépit de ces manquements, le bouclier de protection des données UE-États-Unis assure une protection substantiellement équivalente à celle garantie au sein de l'Union.

4 Troisième moyen tiré de l'absence de recours effectif prévu par la réglementation des États-Unis

14. Dans sa décision Schrems, la CJUE a considéré que « 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 » (point 95).

15. Aux considérants 91 à 124 de la décision attaquée, la Commission présente le système de protection mis en place aux États-Unis. Jusqu'au considérant 104, la Commission expose les mécanismes de contrôle opérés sur les services de renseignement au sein du pouvoir exécutif et par le pouvoir législatif. Si l'ensemble de ces moyens de supervision sont importants et peuvent in abstracto compléter un contrôle juridictionnel ou *a posteriori* effectif, la Cour n'en a pas moins imposé l'existence d'un contrôle juridictionnel effectif et c'est sur l'existence de ce dernier qu'il convient désormais de se focaliser.

16. Tout d'abord, il importe de préciser que le FISC et la suite de recours auxquels ses décisions peuvent ouvrir ne sont aucunement constitutifs d'un quelconque droit au recours juridictionnel effectif tel que l'entend la CJUE puisqu'il ne s'agit que de faire valider des programmes et non pas de permettre à des individus de se plaindre de l'existence d'une surveillance illé-

gale sur leur personne. Comme l'établit la Commission : « 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 » (considérant 109). Ce n'est que la décision de certification et non la décision de surveillance individualisée qui peut faire l'objet d'un recours.

17. Ensuite, la Commission européenne reconnaît elle-même que la protection juridictionnelle, quand bien même serait-elle existante, *quod non*, n'est souvent pas effective : « 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. De plus, même lorsque des possibilités de recours juridictionnel existent en principe pour des personnes non américaines, comme par exemple pour la surveillance FISA, 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).

18. Enfin, l'insistance de la Commission sur le médiateur pour considérer que le dispositif américain de contrôle est conforme aux exigences posées par la Cour révèle l'absence de conformité du système juridictionnel américain à l'exigence de voies de recours effectives. Le médiateur, tel que décrit aux points 116 à 123 ainsi qu'à l'annexe II de la décision attaquée, n'est en effet autre qu'un membre de l'administration désigné comme un « coordinateur chevronné (niveau de sous-secrétaire) au département d'État » (sic). Le fait qu'il s'appuie sur des organes dits « indépendants » n'est en aucune mesure suffisant pour le considérer comme une entité juridictionnelle indépendante garante d'une protection juridictionnelle effective au sens où l'entend la Cour.

19. L'indépendance et l'impartialité de ce médiateur vis-à-vis de l'exécutif américain a d'ailleurs été vivement remise en question par Mme O'Reilly, médiatrice européenne, dans sa lettre du 22 février 2014 à la commissaire européenne Mme Jourova (Annexe A. 2). Cette lettre dénonce un mécanisme ne remplissant pas les qualités attendues d'un médiateur en droit international.

20. Ainsi, le Tribunal doit constater l'absence de contrôle juridictionnel effectif prévu par la réglementation des États-Unis et que, dès lors, la décision attaquée viole la Charte, qui doit donc être annulée de ce fait, lorsqu'elle constate que, en dépit de ce manquement, le bouclier de protection des données UE-États-Unis assure une protection substantiellement équivalente à celle garantie au sein de l'Union.

5 Quatrième moyen tiré de l'absence de contrôle indépendant prévu par la réglementation des États-Unis

21. Dans sa décision Digital Rights Ireland (affaire C-293/12 et C-594/12, 8 avril 2014), la CJUE a conclu que « l'accès aux données conservées par les autorités nationales compétentes [doit être] 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 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 » (point 62).

22. Étant rappelé qu'au sujet de la directive 95/46/CE la CJUE a déjà jugé que l'« indépendance fonctionnelle ne suffit pas, à elle seule, à préserver ladite autorité de contrôle de toute influence extérieure » (CJUE, Commission c. Autriche, C-614/10, point 42).

23. Au considérant 95 de la décision attaquée, la Commission présente les autorités de contrôle des activités américaines de surveillance dans les termes suivants : « De multiples niveaux de supervision ont été instaurés à cet égard, 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). Le personnel de toutes les agences chargé du respect de la conformité participe au bon déroulement de ces fonctions de surveillance ». Néanmoins, au considérant 96, la Commission reconnaît elle-même que « Selon l'appréciation des autorités nationales de protection des données, le contrôle interne exercé par les délégués à la protection des libertés civiles ou de la vie privée peut être considéré comme "assez solide", bien que, de leur point de vue, ces délégués ne jouissent pas du degré d'indépendance requis. »

24. À l'évidence, la Commission a considéré de manière manifestement erronée, dans la décision attaquée, qu'en dépit de ces substantiels manquements, le bouclier de protection des données UE-États-Unis assurerait une protection substantiellement équivalente à celle garantie au sein de l'Union.

25. À tous égards, la décision attaquée viole manifestement la Charte, et doit donc être annulée de ce fait.

V Bordereau des annexes

A. 1. Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 (pages 1 à 112) – décision attaquée – annexe non citée dans la requête

A. 2. Lettre de Mme O'Reilly du 22 février 2014 à la commissaire européenne Mme Jourova (pages 113 et 114) – annexe citée à la page 5 et au paragraphe 19 de la requête

A. 3. Document certifiant que Hugo Roy est habilité à exercer devant les juridictions françaises (pages 115 à 117) – annexe non citée dans la requête

A. 4. Statuts de l'association La Quadrature Du Net (pages 118 à 128) – annexe non citée dans la requête
A. 5. Extrait du registre d'association concernant l'association La Quadrature Du Net (page 129) – annexe non citée dans la requête
A. 6. Mandat de l'association La Quadrature Du Net (page 130) – annexe non citée dans la requête
A. 7. Décision du bureau de l'association La Quadrature Du Net (page 131) – annexe non citée dans la requête

A. 8. Statuts de l'association French Data Network (pages 132 et 133) – annexe non citée dans la requête
A. 9. Extrait du registre d'association concernant l'association French Data Network (page 134) – annexe non citée dans la requête
A. 10. Mandat de l'association French Data Network (page 135) – annexe non citée dans la requête
A. 11. Décision du bureau de l'association French Data Network (page 136) – annexe non citée dans la requête

A. 12. Statuts de l'association Fédération FDN (pages 137 à 140) – annexe non citée dans la requête
A. 13. Extrait du registre d'association concernant l'association Fédération FDN (page 141) – annexe non citée dans la requête
A. 14. Mandat de l'association Fédération FDN (page 142) – annexe non citée dans la requête
A. 15. Décision du bureau de l'association Fédération FDN (page 143) – annexe non citée dans la requête