ALEXIS FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris
5, rue Daunou - 75002 PARIS
Tél. 01.53.63.33.10 - Fax 01.45.48.90.09
afoc@afocavocat.eu

COUR DE JUSTICE

DE

L'UNION EUROPÉENNE

OBSERVATIONS SUR

DES QUESTIONS PRÉJUDICIELLES

AFFAIRES JOINTES

C-511/18 et C-512/18

POUR : Center for Democracy and Technology (CDT) (C-511/18 et C-512/18)

CONTRE : 1°) Le Premier ministre (France)
2°) Le Garde des Sceaux, ministre de la justice (France)
3°) Le ministre de l'intérieur (France)
4°) La ministre des armées (France)

EN PRESENCE DE : 1°) La Quadrature du Net
2°) La Fédération des fournisseurs d'accès à Internet associatifs
3°) igwan.net
4°) French Data Network
5°) Privacy International

FAITS

1. *Center for Democracy and Technology* (CDT), exposante, est une organisation non gouvernementale qui promeut les droits et libertés fondamentaux en ligne et en engagée pour la recherche de solutions prospectives et techniquement solides en réponse aux défis les plus pressants auxquels sont confrontés les utilisateurs de technologies de communications électroniques.

2. Depuis sa constitution, il y a près de 25 ans, CDT a joué un rôle de premier plan dans l'élaboration de politiques, de pratiques et de normes afin de permettre aux individus de s'approprier avec efficacité les technologies. Basée à Washington DC (Etats-Unis), CDT est un organisme caritatif agréé, enregistré aux Etats-Unis et disposant de bureaux à Bruxelles. CDT soutient activement le développement rigoureux de lois et de normes européennes respectueuses des droits de l'homme dans les domaines de la vie privée et de la liberté d'expression.

3. CDT est intervenue à plusieurs reprises devant la Cour européenne des droits de l'homme (CEDH), notamment dans un recours concernant l'accès gouvernemental aux données privées (*cf.* Cour EDH, 12 janvier 2016, *Szabo et Vissy c. Hongrie*, n° 37138/14) et, plus récemment, dans l'affaire *Big Brother Watch & Others* (*cf.* Cour EDH, 13 septembre 2018, n° 58170/13, 62322/14 et 24960/15), concernant les pratiques de surveillance du Royaume-Uni.

4. CDT est intervenue, devant le Conseil d'Etat français, dans l'instance n° 393099 tendant à l'annulation, pour excès de pouvoir, de la décision implicite de rejet résultant du silence gardé par le Premier ministre sur la demande présentée par La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs et French Data Network, tendant à l'abrogation de l'article R. 10-13 du code des postes et des communications électroniques et du décret n° 2011-219 du 25 février 2011.

5. Dans ses décisions n° 393099 et n° 394922, 394925, 397844 et 397851 du 26 juillet 2018, le Conseil d'Etat français a posé une série de questions préjudicielles à la Cour de justice de l'Union européenne.

6. Ces questions préjudicielles ont été enregistrées par le greffe de la Cour de justice de l'Union européenne (ci-après « la Cour ») sous les n° C-511/18 et C-512/18 qui ont été jointes. La Cour a invité CDT à présenter ses observations sur ces questions.

7. Le présent mémoire constitue les observations de CDT sur ces questions.

DISCUSSION

8. Dans un premier temps, CDT rappellera, d'une part, les lignes de force des régimes français en cause au principal (I) et, d'autre part, les principes essentiels de droit de l'Union dégagés par la Cour dans sa jurisprudence, à propos des question préjudicielles en question (II).

9. Dans un second temps, CDT détaillera le cadre juridique applicable aux Etats-Unis où il n'existe aucune obligation de rétention généralisée et indifférenciée des données de connexion, ni aucun régime de surveillance de masse sur le territoire des Etats-Unis, afin de montrer que, contrairement à ce que la manière dont les questions posées par le Conseil d'Etat laisse entendre, ce type d'atteintes graves dans les libertés fondamentales des citoyens de l'Union n'est pas nécessaire pour assurer la sûreté, ni pour assurer la sécurité nationale, ni pour lutter contre le terrorisme ou la criminalité grave (III).

I.- Les régimes en cause au principal

10. Sur les questions relatives à la conservation généralisée des données de connexion de droit commun

11. Les régimes en cause au principal sont notamment constitués, d'une part, des articles L. 34-1 et R. 10-13 du code des postes et des communications électroniques (CPCE)[1], qui s'appliquent aux opérateurs de communications électroniques (fournisseurs de réseaux ou de services de communications électroniques) et concernent de très nombreuses données de trafic et de localisation et, d'autre part, du décret n° 2011-219, pris en application de l'article 6, II de la loi pour la confiance dans l'économie numérique et s'applique aux personnes visées à l'article 6, I, 1 et 2 de cette loi (les fournisseurs d'accès et les hébergeurs) et concerne des données identifiantes, y compris des données relatives au trafic.

12. Il est prévu, en particulier, d'une part, que les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne sont tenues de conserver l'identifiant de la connexion, l'identifiant attribué à l'abonné, l'identifiant du terminal utilisé pour la connexion, les dates et heure de début et de fin de la connexion, les caractéristiques de la ligne de l'abonné ; d'autre part, les personnes qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des

[1] Article R. 10-13 du CPCE : « *I. – En application du III de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :*
a) Les informations permettant d'identifier l'utilisateur ;
b) Les données relatives aux équipements terminaux de communication utilisés ;
c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
e) Les données permettant d'identifier le ou les destinataires de la communication.
II. – Pour les activités de téléphonie l'opérateur conserve les données mentionnées au II et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.
III. – La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement. (…) »

destinataires de ces services sont tenues de conserver l'identifiant de la connexion à l'origine de la communication, l'identifiant attribué par le système d'information au contenu, objet de l'opération, les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus, la nature de l'opération, les date et heure de l'opération, l'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni.

13. Ces deux séries de personnes doivent en outre conserver les information fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte, à savoir, au moment de la création du compte, l'identifiant de cette connexion, les nom et prénom ou la raison sociale, les adresses postales associées, les pseudonymes utilisés, les adresses de courrier électronique ou de compte associés, les numéros de téléphone, le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour. Enfin, ces deux séries de personnes doivent encore conservé, lorsque la souscription du contrat ou du compte est payante, les informations relatives au type de paiement utilisé, la référence du paiement, le montant, ainsi que la date et l'heure de la transaction.

14. Il s'en infère que les régimes français de conservation de données de trafic, de localisation et d'autres données afférentes aux communications électroniques imposent la conservation d'un ensemble de données très nettement plus large que le régime suédois en cause dans l'affaire *Tele2* et ce pour une durée d'un an, soit double à la durée prévue par le régime suédois dans cette affaire.

15. **Sur les questions relatives au renseignement de masse**

16. Les données de connexion susceptibles d'être recueillies dans le cadre des techniques de renseignement sont encore plus importantes dès lors qu'au-delà de ces données conservées « de droit commun », le 2° du I de l'article R. 851-5 du code de la sécurité intérieure (CSI)[2] y ajoute les données techniques permettant de localiser les équipements terminaux, celles relatives à l'accès de ces équipements aux réseaux ou aux services de communication au public en ligne, celles relatives à l'acheminement des communications électroniques par les réseaux, celles relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne et celles relatives aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels.

---

[2] Article R. 851-5 du CSI : « *I.-Les informations ou documents mentionnés à l'article L. 851-1 sont, à l'exclusion du contenu des correspondances échangées ou des informations consultées :*
1° Ceux énumérés aux articles R. 10-13 et R. 10-14 du code des postes et des communications électroniques et à l'article 1er du décret n° 2011-219 du 25 février 2011 modifié relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne ;
2° Les données techniques autres que celles mentionnées au 1° :
a) Permettant de localiser les équipements terminaux ;
b) Relatives à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne ;
c) Relatives à l'acheminement des communications électroniques par les réseaux ;
d) Relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne ;
e) Relatives aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels.
II.- Seuls les informations et documents mentionnés au 1° du I peuvent être recueillis en application de l'article L. 851-1. Ce recueil a lieu en temps différé.
Les informations énumérées au 2° du I ne peuvent être recueillies qu'en application des articles L. 851-2 et L. 851-3 dans les conditions et limites prévues par ces articles et sous réserve de l'application de l'article R. 851-9. »

17. Les mesures de surveillance prévues par les régimes en cause sont susceptibles d'être mise en œuvre pour de très larges finalités, dépassant de très loin la lutte contre la criminalité grave et selon des techniques particulièrement attentatoires aux droits fondamentaux protégés par la Charte.

18. Le contrôle de la mise en œuvre des techniques de renseignement n'étant soumis qu'à un simple avis de la Commission nationale de contrôle des techniques de renseignement (CNCTR), qui ne lie pas le Premier ministre (*cf.* articles L. 821-3 et L. 821-4 du CSI) et qui n'est pas nécessaire en cas d'urgence (*cf.* article L. 821-5 du CSI).

19. En outre, le contentieux de la mise en œuvre des techniques de renseignement n'est pas conforme au droit de l'Union européenne, dès lors qu'il ne prévoit aucune information, à aucun moment, de la personne faisant l'objet d'une mesure de surveillance, qu'il exclut, tout au long de la procédure pré-contentieuse et contentieuse, tout contradictoire et qu'en matière de surveillance internationale aucun recours n'est prévu, ainsi que l'ont reconnu tant le Conseil constitutionnel (*cf.* Cons. const., 26 novembre 2015, *Loi renseignement*, décision n° 2015-722 DC, cons. 18) que la formation spécialisée du Conseil d'Etat (*cf.* CE, formation spécialisée, 19 octobre 2016, n° 397623, aux Tables). Ce dernier ayant précisé, en outre, qu'un recours pour excès de pouvoir était insusceptible d'être formé à l'encontre du défaut de saisine du Conseil d'Etat par le président de la CNCTR (*cf.* CE, formation spécialisée, 20 juin 2018, *Sophie in't Veld*, n° 404012).

II.- Le droit de l'Union s'oppose, d'une part, à un régime généralisé et indifférencié de conservation des données de connexion et, d'autre part, à un régime de surveillance de masse, telles que ceux en cause au principal

20. D'emblée, il ne fait aucun doute qu'un régime de conservation généralisée et indifférenciée des données de connexion, de même qu'un système de surveillance de masse et de renseignement automatisé et non ciblé tel que celui mis en place en France, « comporte le risque de saper, voire de détruire, la démocratie au motif de la défendre » (*cf.* Cour EDH, 6 septembre 1978, *Klass et autres c. Allemagne*, req. n° 5029/71, §§ 49-50 ; Cour EDH, 4 mai 2000, *Rotaru c. Roumanie*, req. n° 28341/95, §. 49).

II.1.- Le présent litige s'inscrit pleinement dans le champ d'application de la Charte des droits fondamentaux de l'Union européenne (ci-après « la Charte »)

21. A titre liminaire, il convient de rappeler qu'un, tel que celui en cause au principal, qui impose à des fournisseurs de services de communications électroniques de conserver les données relatives au trafic et les données de localisation, relève du champ d'application de la directive 2002/58 du 12 juillet 2002. De même, relève également dudit champ d'application une réglementation nationale, comme dans l'affaire au principal, sur l'accès des autorités nationales aux données conservées par ces fournisseurs (*cf. mutatis mutandis*, CJUE, 21 décembre 2016, *Tele2 Sverige AB et autres*, n° C-203/15, C-698/15, EU:C:2016:970, ci-après « arrêt *Tele2* », pts. 75-81).

22. A cet égard, il est particulièrement curieux de relever que, dans sa décision n° 394922, 394925, 397844, 397851 du 26 juillet 2018 ayant renvoyé plusieurs des questions préjudicielles en cause, le Conseil d'Etat a cru pouvoir juger, au point 21 de sa décision, de manière frontalement contraire à la jurisprudence constante de la Cour, qu'il « résulte clairement de la directive du 12 juillet 2002 que ne relèvent pas de son champ les dispositions des articles L. 851-5 et L. 851-6, ainsi que celles des chapitres II, III et IV du titre V du livre VIII du code de la sécurité intérieure, dès lors qu'elles portent sur des techniques de recueil de renseignement qui sont directement mises en œuvre par l'Etat sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques. Dès lors, ces dispositions ne sauraient être regardées comme mettant en œuvre le droit de l'Union européenne et, par suite, les moyens tirés de la méconnaissance de la directive du 12 juillet 2002 interprétée à la lumière de la Charte des droits fondamentaux de l'Union européenne ne peuvent être utilement invoqués à leur encontre. »

23. Ce faisant le Conseil d'Etat a manifestement réduit le champ d'application du droit de l'Union européenne et l'a privé d'effet utile et d'effet direct en restreignant indument son invocabilité. La Cour pourra utilement saisir l'occasion présentée par cette affaire afin de rappeler sa propre interprétation, qui ne manquera pas d'être radicalement opposée à celle du Conseil d'Etat sur ce point.

II.2.- <u>La confidentialité des communications est un principe fondamental du droit de l'Union européenne, qui ne souffre que des exceptions limitées et interprétées strictement</u>

24. Le principe de confidentialité des communications instauré notamment par la directive 2002/58 implique, entre autres, ainsi qu'il ressort de l'article 5, §. 1er, deuxième phrase, de celle-ci, une interdiction faite, en principe, à toute autre personne que les utilisateurs de stocker, sans le consentement de ceux-ci, les données relatives au trafic afférentes aux communications électroniques. Font seuls l'objet d'exceptions les personnes légalement autorisées conformément à l'article 15, §. 1er, de cette directive et le stockage technique nécessaire à l'acheminement d'une communication (*cf.* arrêt *Tele2*, pt. 85 et CJUE, 29 janvier 2008, *Promusicae*, C-275/06, EU:C:2008:54, pt. 47).

25. Dit autrement, le système mis en place par la directive 2002/58 exige que la conservation des données relatives au trafic et à la localisation soit une exception très strictement encadrée et délimitée (*cf.* arrêt *Tele2*, pt. 104).

26. Le traitement et le stockage des données relatives au trafic ne sont autorisés que dans la mesure et pour la durée nécessaires à la facturation des services, à la commercialisation de ceux-ci et à la fourniture de services à valeur ajoutée (*cf.* arrêt *Tele2, in limine*, pt. 86 ; arrêt *Promusicae*, pts. 47 et 48). S'agissant, en particulier, de la facturation des services, un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement. Une fois cette durée expirée, les données ayant été traitées et stockées doivent être effacées ou rendues anonymes (*cf.* arrêt *Tele2*, pt. 86, *in medio*). S'agissant des données de localisation autres que les données relatives au trafic, l'article 9, §. 1er, de ladite directive prévoit que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés (*cf.* arrêt *Tele2*, pt. 86, *in fine*).

27. La présente affaire doit notamment s'interpréter à la lumière du principe de minimisation des données personnelles collectées et traitées, rappelé notamment par le considérant 30 de la directive 2002/58 (*cf.* arrêt *Tele2*, pt. 87).

28. Si l'article 15, §. 1er de la directive 2002/58 permet aux Etats membres de limiter la portée de l'obligation de principe d'assurer la confidentialité des communications et des données relatives au trafic y afférentes, il est, conformément à la jurisprudence constante de la Cour, d'interprétation stricte (*cf.* arrêt *Tele2*, pt. 89, *in limine* ; CJUE, 22 novembre 2012, *Probst*, C-119/12, EU:C:2012:748, pt. 23).

II.3.- L'ingérence que constitue la conservation généralisée et indifférenciée de l'ensemble des données de connexion est d'une vaste ampleur et doit être considérée comme particulièrement grave

29. La Cour a déjà jugé, en formation de grande chambre, que « les données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet (…) permettent, notamment, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée. » (*cf.* CJUE, 8 avril 2014, *Digital Rights Ireland*, n° C-293/12 et C-594/12, EU:C:2014:238, pt. 26 ; voir également, arrêt *Tele2*, pt. 96)

30. La Cour relevait très justement que « [c]es données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. » (arrêt *DRI*, pt. 27 ; arrêt *Tele2*, pt. 99, *in limine*). En particulier, ces données fournissent les moyens d'établir, ainsi que la Cour l'a jugé, à la suite de son avocat général, M. Henrik Saugmandsgaard Øe aux points 253, 254 et 257 à 259 des conclusions qu'il a prononcées sur l'arrêt *Tele2*, « le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications » (*cf.* arrêt *Tele2*, pt. 99, *in fine*).

31. Même si une telle réglementation n'autorise pas formellement la conservation du contenu d'une communication, la conservation des données relatives au trafic et des données de localisation a une incidence sur l'utilisation des moyens de communication électronique et, en conséquence, sur l'exercice par les utilisateurs de ces moyens de leur liberté d'expression, garantie à l'article 11 de la Charte (*cf.* arrêt *DRI*, pt. 28 ; arrêt *Tele2*, pt. 101).

32. Par suite, « [l]a conservation des données aux fins de leur accès éventuel par les autorités nationales compétentes (…) concerne de manière directe et spécifique la vie privée et, ainsi,

les droits garantis par l'article 7 de la Charte. En outre, une telle conservation des données relève également de l'article 8 de celle-ci en raison du fait qu'elle constitue un traitement des données à caractère personnel au sens de cet article et doit, ainsi, nécessairement satisfaire aux exigences de protection des données découlant de cet article » (arrêt *DRI*, pt. 29).

33. Etant précisé que l'obligation imposée aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte (*cf.* arrêt *DRI*, pt. 34).

34. En outre, « l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental », en sorte que « les règles relatives à l'accès des autorités nationales compétentes aux données sont également constitutifs d'une ingérence dans les droits garantis par l'article 7 de la Charte. » (arrêt *DRI*, pt. 35). De même, cet accès est constitutif d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte (*cf.* arrêt *DRI*, pt. 36).

35. Cette ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère, d'une vaste ampleur et doit être considérée comme particulièrement grave (*cf.* arrêt *DRI*, pt. 37 ; arrêt *Tele2*, pt. 100). En outre, la circonstance que la conservation des données soit effectuée sans que les utilisateurs des services en cause en soient informés est susceptible d'engendrer, dans l'esprit des personnes concernées, le sentiment que leur vie privée fait l'objet d'une surveillance constante (*cf.* arrêt *DRI*, pt. 37 ; arrêt *Tele2*, pt. 100, *in fine*).

36. Sur le fondement, notamment, de l'article 52, §. 1er, de la Charte, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit être prévue par la loi, respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui (*cf.* arrêt *DRI*, pt. 38). Ce principe général de proportionnalité est encore repris tant dans le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (RGPD) qui prévoit que les données collectées doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées » (*cf.* article 5, §. 1, c), que dans la directive 2016/680, qui prévoit que ces données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées » (*cf.* article 4, §. 1, c).

37. Partant, s'il est certes vrai que cette ingérence est éventuellement susceptible de répondre à un objectif d'intérêt général, il est tout aussi vrai qu'elle est radicalement disproportionnée aux objectifs poursuivis.

II.4.- L'ingérence de la législation nationale en cause au principal, non seulement, n'est pas nécessaire afin d'atteindre les objectifs poursuivis, mais encore, est radicalement disproportionnée

38. D'emblée, il convient de rappeler que le principe de proportionnalité exige, selon une jurisprudence constante de la Cour, que les actes portant une ingérence dans des droits fondamentaux soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs (*cf. mutatis mutandis*, arrêt *DRI*, pt. 46 ; arrêt *Schrems*, pt. 92 ; arrêt *Tele2*, pts. 96 et 116).

39. Au cas présent, compte tenu, d'une part, du rôle essentiel que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte, d'une part, un régime de rétention généralisée et indifférenciée des données et, d'autre part, un régime de surveillance de masse, tel que ceux en cause au principal, le pouvoir d'appréciation du législateur s'avère réduit de sorte qu'il convient de procéder à un contrôle strict (*cf.* arrêt *DRI*, pt. 48).

40. Il est certes vrai que les données qui doivent être conservées en application des régimes en cause au principal peuvent éventuellement être de nature à permettre aux autorités nationales compétentes en matière de poursuites pénales de disposer de possibilités supplémentaires d'élucidation des infractions graves, de sorte qu'elles peuvent donc constituer un instrument utile pour les enquêtes pénales

41. Toutefois, un tel objectif d'intérêt général, aussi important puisse-t-il être, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par les régimes en cause au principal, soit considérée comme nécessaire aux fins de ladite lutte (*cf. mutatis mutandis*, arrêt *DRI*, pt. 51).

42. La protection du droit fondamental au respect de la vie privée exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire (*cf.* CJUE, 26 juillet 2017, avis 1/15, pt. 140 ; arrêt *Tele2*, pts. 96 et 116 ; CJUE, 6 octobre 2015, *Schrems*, C-362/14, EU:C:2015:650, pt. 92 ; arrêt *DRI*, pt. 52 ; CJUE, 7 novembre 2013, *IPI*, C-473/12, EU:C:2013:715, pt. 39 et jurisprudence citée).

43. À cet égard, il convient de rappeler que la protection des données à caractère personnel, résultant de l'obligation explicitement prévue à l'article 8, §. 1er, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l'article 7 de celle-ci (*cf.* arrêt *DRI*, pt. 53).

44. Ainsi, afin d'être conforme au droit de l'Union européenne et, en particulier à la directive du 12 juillet 2002 lue à la lumière de la Charte et à la directive du 8 juin 2000, lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, §. 1er, de la Charte, les régimes en cause au principal auraient dû prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant un minimum d'exigences de sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus ainsi

que contre tout accès et toute utilisation illicites de ces données (*cf.* arrêt *DRI*, pt. 54 ; par analogie, en ce qui concerne l'article 8 de la Convention EDH : Cour EDH, 1er juillet 2008, *Liberty et autres c. Royaume-Uni*, n° 58243/00, §§. 62 et 63 ; Cour EDH, 1er juillet 2008, *Rotaru c. Roumanie [GC]*, n° 28341/95, §§. 57 à 59 ; arrêt *S. et Marper c. Royaume-Uni*, préc., §. 99).

45. La nécessité de disposer de telles garanties est d'autant plus importante lorsque, comme le prévoit les régimes en cause au principal, les données à caractère personnel sont soumises à un traitement automatique et qu'il existe un risque important d'accès illicite à ces données (*cf.* arrêt *DRI*, pt. 55 ; par analogie, en ce qui concerne l'article 8 de la Convention EDH : arrêt *S. et Marper c. Royaume-Uni*, préc., §. 103 ; Cour EDH, 18 avril 2013, *M. K. c. France*, n° 19522/09, §. 35).

46. L'ingérence que comporte les régimes en cause au principal est très loin d'être limitée au strict nécessaire, dès lors, notamment que ces régimes imposent la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à l'internet, le courrier électronique par Internet, la téléphonie par l'internet ainsi que l'ensemble des données de connexion conservées par les hébergeurs. Ainsi, elle vise tous les moyens de communication électronique dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne de chacun. En outre, ces régimes couvrent tous les abonnés et utilisateurs inscrits. Ils comportent donc une ingérence dans les droits fondamentaux de la totalité des utilisateurs de ses services, peu importe leur nationalité (*cf.* arrêt *DRI*, pt. 56).

47. **D'abord**, les régimes en cause au principal couvrent de manière généralisée, la totalité des utilisateurs de l'ensemble des moyens de communication électronique, ainsi que la totalité des données relatives au trafic sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre les infractions graves (*cf.* arrêt *DRI*, pt. 57).

48. D'une part, ces régimes concernent 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. Ils s'appliquent 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, ils ne prévoient aucune exception, de sorte qu'ils s'appliquent même à des personnes dont les communications sont soumises au secret professionnel (*cf.* arrêt *DRI*, pts. 58 ; arrêt *Tele2*, pt. 105).

49. D'autre part, alors même que la justification affichée de ces régimes est la lutte contre la criminalité grave, il est particulièrement étonnant de relever que ces régimes ne requièrent aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. En particulier, ils ne sont pas limités 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 (*cf.* arrêt *DRI*, pt. 59 ; arrêt *Tele2*, pt. 106, qui résume ce triptyque, de manière générique, sous l'angle de « *la lutte contre la criminalité* »).

50. **Ensuite**, à cette absence générale et caractérisée de limites s'ajoute le fait que les régimes en cause au principal ne prévoient aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence (*cf.* arrêt *DRI*, pt. 60).

51. En particulier, ces régimes ne prévoient aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi. Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante au sens du droit de l'Union européenne, 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 intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales (*cf.* arrêt *DRI*, pt. 62).

52. **Enfin**, s'agissant de la durée de conservation des données, les régimes en cause au principal imposent la conservation de celles-ci pendant une période d'un an sans que soit opérée une quelconque distinction entre les catégories de données en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées (*cf.* arrêt *DRI*, pt. 63).

53. Cette très longue durée de conservation est fixée de manière totalement arbitraire sans être fondée sur des critères objectifs afin de garantir, notamment, que celle-ci soit limitée au strict nécessaire (*cf.* arrêt *DRI*, pt. 64).

54. Il s'en infère que les régimes en cause au principal ne prévoient pas de règles suffisamment claires et précises susceptible de venir limiter utilement la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est donc de constater que ces régimes comportent une ingérence dans ces droits fondamentaux d'une très vaste ampleur et d'une gravité particulière sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle soit effectivement limitée au strict nécessaire (*cf.* arrêt *DRI*, pt. 65).

55. De surcroît, les régimes en cause au principal ne prévoient pas les garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicite de ces données. En effet, ces régimes ne prévoient pas de règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée par ces régimes, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, destinées notamment à garantir la pleine intégrité et confidentialité des données en cause (*cf.* arrêt *DRI*, pt. 66).

56. En particulier, les régimes en cause ne prévoient pas les conditions dans lesquelles les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données conservées, de manière à limiter strictement cet accès aux objectifs visés à l'article 15, §. 1er de la directive 2002/58, ni des conditions

matérielles et procédurales suffisamment précises régissant cet accès (*cf.* arrêt *DRI*, pt. 61 ; arrêt *Tele2*, pt. 118). Ils ne prévoient pas plus des conditions matérielles et procédurales suffisamment précises régissant l'utilisation de ces données (*cf.* avis 1/15, p. 192).

57. Du reste, les régimes en cause n'imposent pas aux autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé d'informer les personnes concernées, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités (*cf.* arrêt *Tele2*, pt. 121, *in limine*), alors même que cette information est nécessaire afin de permettre aux personnes concernées d'exercer, notamment, le droit de recours, explicitement prévu à l'article 15, §. 2, de la directive 2002/58, lu en combinaison avec l'article 22 de la directive 95/46, en cas de violation de leurs droits (*cf.* avis 1/15, pt. 220 ; arrêt *Tele2*, pt. 121, *in fine* ; arrêt *Schrems*, pt. 95 ; CJUE, 7 mai 2009, *Rijkeboer*, n° C-553/07, EU:C:2009:293, pt. 52). En effet, « la question de la notification *a posteriori* de mesures de surveillance est indissolublement liée à celle de l'effectivité des recours judiciaires et donc à l'existence de garanties effectives contre les abus des pouvoirs de surveillance. La personne concernée ne peut guère, en principe, contester rétrospectivement devant la justice la légalité des mesures prises à son insu, sauf si on l'avise de celles-ci » (*cf.* Cour EDH, 4 décembre 2015, *Zakharov c/ Russie*, n° 47143/06, §. 234).

58. Pour mémoire, la Cour a été conduite, après avoir invalidé la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (*cf.* arrêt *DRI*, préc.), à dire, pour droit :

- d'une part, que « *L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique*. » et,

- d'autre part, que « *L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union.* »

59. Cette jurisprudence a été encore confirmée par l'avis 1/15 du 26 juillet 2017 dans lequel la Cour a notamment exigé, à propos de l'accord *Passengers Name Records (PNR)* en négociation entre le Canada et l'Union européenne, d'une part, que la conservation des données des dossiers passagers après leur départ du Canada soit strictement limitée à celles des passagers à l'égard desquels il existe des éléments objectifs permettant de considérer qu'ils pourraient présenter un risque en termes de lutte contre le terrorisme et la criminalité transnationale grave et, d'autre part, qu'il soit prévu un droit à l'information individuelle des passagers aériens en cas d'utilisation des données des dossiers passagers les concernant pendant leur séjour au Canda et après leur départ de ce pays, ainsi qu'en cas de divulgation de ces données par l'autorité canadienne compétente à d'autres autorités nationales ou à des particuliers et que ces règles soient garanties par une autorité de contrôle indépendante.

60. **En l'espèce**, les régimes français en cause au principal prévoient une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de la totalité des abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, et obligent les fournisseurs de services de communications électroniques à conserver ces données de manière systématique et continue, et ce sans aucune exception (*cf. mutatis mutandis*, arrêt *Tele2*, pt. 97).

61. Ces régimes excèdent donc les limites du strict nécessaire et ne sauraient être considérés comme étant justifiés, dans une société démocratique, ainsi que l'exige l'article 15, §. 1er, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, §. 1er, de la Charte (*cf. mutatis mutandis*, arrêt *Tele2*, pt. 107).

62. Ces régimes prévoient également une surveillance de masse et un système de renseignement non ciblé, sans autorisation préalable par un juge ou par une autorité administrative indépendante, ni aucune notification des mesures de surveillance mise en œuvre et sans aucun recours effectif, contraire, notamment, à la directive du 12 juillet 2002 et aux articles 5, §1, c, du RGPD et 4, §1, c de la directive 2016/680, lu à la lumière de la Charte.

63. Cela est d'autant plus vrai que nombre d'Etats, à l'instar des Etats-Unis, écartent toute obligation de conservation généralisée et indifférenciée des données de connexion à la charge des opérateurs de communications électroniques, ainsi que toute surveillance de masse sur leur propre territoire (III).

III.- <u>Le droit des Etats-Unis prohibe toute surveillance de masse sur le territoire des Etats-Unis et exclut toute conservation généralisée des données de connexion</u>

64. La manière dont les présentes questions préjudicielles ont été posées cherche à laisser entendre que des régimes particulièrement attentatoires aux droits fondamentaux des citoyens de l'Union européenne, seraient « nécessaires » compte tenu des risques actuels auxquels les Etats membres de l'Union seraient confrontés.

65. Il n'en est rien.

66. L'expérience des Etats-Unis montre qu'une obligation générale et indifférenciée de conservation des données n'est pas nécessaire pour assurer la sécurité publique, y compris

pour lutter efficacement contre le terrorisme, pas plus qu'un régime autorisation une surveillance massive et indifférenciée.

67. En effet, aux Etats-Unis le droit positif ne prévoit aucune obligation, à la charge des opérateurs de communications électroniques, de conserver les données de connexion.

68. La Cour Suprême des Etats-Unis a d'ailleurs récemment jugé que l'accès aux données relatives à la localisation d'un téléphone portable est subordonné à l'obtention d'un mandat en bonne et due forme, justifiant d'une « *probable cause* » (qui est en quelque sorte un standard servant à définir l'encadrement des arrestations et des fouilles par les forces de police) plutôt qu'à une simple ordonnance judiciaire rendu sur le fondement du *Stored Communications Act* qui se borne à exiger de démontrer l'existence d'un « *reasonable grounds* » (grossièrement traduit par « motifs raisonnables ») (*cf.* SCOTUS, 22 juin 2018, *Carpenter v. US*, n° 16-402).[3]

69. Au lieu d'une rétention massive et généralisée, le Congrès des Etats-Unis a octroyé aux forces de l'ordre une procédure leur permettant de demander aux fournisseurs de communications électroniques de conserver les données d'une personne spécifiquement ciblée jusqu'à 90 jours, avec la possibilité de renouveler cette période de conservation[4]. Une ordonnance judiciaire ou une autre procédure judiciaire, en fonction de la nature des données, est nécessaire pour permettre aux forces de l'ordre de contraindre la communication des données recherchées.

70. Il convient de relever que le Congrès des Etats-Unis a eu l'opportunité de mettre en place un tel régime d'obligation de conservation généralisée et indifférenciée des données de connexion en 2011, mais la loi proposée n'a pas réussie à obtenir suffisamment de supporteurs afin d'entrainer un vote à la *House of Representatives* (une des deux chambres du Congrès). Cette proposition a reçu l'opposition frontale de l'ancien président du *full Committee, representative* James Sensenbrenner, expliquant que la proposition de créer une obligation de conservation généralisée des données de connexion devrait être relégué dans la « poubelle de l'histoire » et que « cette proposition de loi va à l'encontre du droit à la vie privée des personnes utilisant Internet pour des milliers de buts licites »[5].

71. De même, aux Etats-Unis, la surveillance et le renseignement sur le territoire national doivent être ciblés et non généralisés, sur le fondement de la loi étatsunienne sur la

[3] https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf : « As with GPE information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through themhis « familial, political, professional, religious, and sexual associations. » *Id.*, at 415 (opinion of SOTOMAYOR, J.). These location records « hold for many Americans the « privacies of life ». *Riley*, 573 U. S., at (slip op., at 28) (quoting *Boyd*, 116 U. S., at 630). And like GPS monitoring, cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense. In fact, historical cell-site records present even greater privacy concerns than the GPC monitoring of a vehicle we considered in *Jones*. Unlike the bugged container in *Knotts* ot the car in *Jones*, a cell phone –almost a « feature of human anatomy », *Riley*, 573 U. S., at (slip op., at 9) tracks nearly exactly the movements of its owner.
(…)
Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may –in the Government's view- call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance. »

[4] 18 USC §2703(f).

[5] https://judiciary.house.gov/_files/hearings/printers/112th/112-60_67309.PDF at 2.

surveillance internationale (*i.e. Foreign Intelligence Surveillance Act*) (FISA). Cela est valable, dans le cadre du renseignement étranger, peu importe l'objectif poursuivi, y compris lorsqu'il s'agit de sécurité nationale, de sécurité publique ou de lutte contre le terrorisme perpétué par des organisations étrangères. La mesure de surveillance du contenu d'une communication ne peut être autorisée, en application du FISA, que lorsqu'une « *probable cause* » démontrant que la mesure de surveillance cible un pouvoir étranger (tel qu'un gouvernement ou une organisation terroriste étrangère) ou un agent d'un pouvoir étranger[6].

72. Une telle demande de surveillance, sur le fondement du FISA, doit être formée devant un juge spécifique (*i.e. Foreign Intelligence Surveillance Court*) (FISC) et doit contenir : 1) un exposé des motifs conduisant à penser que la cible de la surveillance est un pouvoir étranger ou un agent d'un pouvoir étranger, 2) une attestation que l'information recherchée est réputée revêtir un caractère étranger et que cette information ne peut être raisonnablement obtenue par des techniques de renseignement conventionnelles, 3) un exposé détaillant l'ensemble des précédentes demandes concernant la cible, 4) une description détaillée de la nature de l'information recherchée et du type de communications ou activités sujette à surveillance, 5) la durée de la surveillance projetée, 6) la question de savoir si l'introduction dans une propriété privée est nécessaire et, 7) des propositions afin de minimiser l'acquisition, l'utilisation et la rétention des informations nécessaires concernant des citoyens ou habitants des Etats-Unis non consentants.

73. Le IV^{ème} Amendement de la Constitution des Etats-Unis exige que les mesures de surveillance mise en œuvre par les forces de l'ordre soient ciblées. En matière d'enquêtes pénales, les forces de l'ordre sont également soumises à la loi sur la vie privée en matière de communications électroniques (*i.e. Electronic Communications Privacy Act*) (ECPA) lorsqu'ils souhaitent surveiller des communications ou des données relatives aux communications (dates, en-tête, notamment l'expéditeur et le destinataire d'un message).

74. Sur le fondement du *Wiretap Act*, les forces de l'ordre doivent être préalablement autorisées par un juge avant d'intercepter le contenu d'une communication[7]. La demande n'est susceptible d'être autorisée qu'après un examen complet des faits susceptible de justifier qu'une telle autorisation judiciaire soit délivrée, incluant notamment les détails relatifs à une infraction en cause (qui doit être un crime sérieux tel que la corruption ou le terrorisme), une description et localisation des équipements visés par la mesure de surveillance demandée, une description du type de communications visées par les mesures d'interception et l'identité de la personne ayant commis le crime, si elle est connue, et une explication complète et détaillée que d'autres procédures d'enquête ont été tentées en vain ou les motifs expliquant pourquoi elles seraient manifestement vouées à l'échec. La mesure de surveillance demandée n'est autorisée que si un juge estime qu'il existe de solides et sérieux indices (« *probable cause* ») d'autoriser cette demande. Etant précisé que ces mesures de surveillance ne sont susceptibles d'être autorisées que lorsqu'elles concernent un individu et une enquête, en particulier.

75. De même, afin d'accéder au contenu d'une communication ciblée, un mandat garantissant les standards de protection du IV^{ème} Amendement de la Constitution des Etats-Unis est

[6] 50 USC Section 1805(a).
[7] 18 U.S.C. § 2518

requis, délivré par une décision de justice[8]. Si les données de trafic ou les informations relatives à un abonnement sont recherchées elles n'en doivent pas moins être préalablement autorisées par un mandat, une décision de justice[9] ou une assignation. Ici encore, la demande doit être ciblée.

76. En 2013, Edward Snowden, un contractant de la *National Security Agency* (NSA) a révélé, notamment, que la NSA recevait les données relatives à l'ensemble des appels téléphoniques émis à l'intérieur du territoire des Etats-Unis. CDT[10], parmi plusieurs autres organisations, le *US Privacy and Civil Liberties Oversight Board*[11], et au moins une juridiction, ont tous considéré que cette surveillance de masse de l'ensemble des données relatives aux appels téléphoniques était illégale et inconstitutionnelle.

77. En 2015, le Congrès des Etats-Unis a adopté le *USA Freemdom Act*[12] afin, spécifiquement, d'interdire sans équivoque toute mesure de surveillance généralisée à l'intérieur des Etats-Unis. Les Sections 102, 201 et 501 interdisent expressément l'ensemble des mesures de surveillance massive[13]. Dans tous les cas, cette législation impose que des discriminants suffisamment précis soient utilisés préalablement à la mise en place de toute mesure de recueil de renseignements.

78. En revanche, la surveillance massive et généralisée, de même que le renseignement non ciblé, sont exercés à l'extérieur du territoire des Etats-Unis et, concernant le cas des câbles transatlantiques de télécommunications, jusqu'au point d'interconnexion entre ces derniers et le territoire national, au détriment du reste du monde et, en particulier, des citoyens de l'Union et de leurs droits fondamentaux.

79. Malgré le fait que seul les enquêtes criminelles et le renseignement ciblés sont permis sur le territoire des Etats-Unis et qu'aucune loi n'impose aux opérateurs de communications électroniques de conserver les données de connexion, les Etats-Unis dispose d'un système pénal robuste et d'une sécurité nationale solide. Cela démontre bien qu'un régime rendant obligatoire la conservation généralisée et indifférenciée des données de connexion, pas plus qu'un régime de surveillance de masse, ne sont nécessaires afin d'assurer la sécurité ou de lutter contre la criminalité grave.

80. Enfin, CDT s'associe expressément aux observations déposées dans la présente affaire devant la Cour par les associations françaises « La Quadrature du Net », la « Fédération des fournisseurs d'accès à Internet associatifs » et « igwan.net ».

---

[8] *United States v. Warshak*, 631 F.3d 266 (2010).
[9] 18 U.S.C. § 2703 (c)
[10] August 1, 2013 Statement for the Record at Privacy and Civil Liberties Oversight Board Hearings on Surveillance Programs, https://www.cdt.org/files/pdfs/CDT-PCLOB-Statement-for-the-Record.pdf
[11] https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf
[12] https://www.gpo.gov/fdsys/pkg/PLAW-114publ23/html/PLAW-114publ23.htm.
[13] Section 102 of the law, entitled « Prohibition of bulk collection of tangible things », prohibits bulk collection under Section 215 of the USA PATRIOT Act, which governs collection of stored metadata for intelligence purposes. Section 201 of the law, entitled « Prohibition of bulk collection » outlaws bulk collection of metadata domestically in real time. Section 501 of the law, entitled « Prohibition of bulk collection » outlaws the use of National Security Letters to obtain stored metadata domestically in intelligence investigations. In each case, the USA FREEDOM Act precludes bulk collection by requiring that a « specific selection term » or selector be used as the basis for the collection.

PAR CES MOTIFS, et s'associant à ceux exposés par la Fédération des fournisseurs d'accès à Internet associatifs, igwan.net et La Quadrature du Net, ainsi qu'à leurs conclusions, CDT conclut à ce qu'il plaise à la Cour de justice de l'Union européenne de dire pour droit :

1) Une obligation de conservation généralisée et indifférenciée, imposée aux opérateurs de télécommunications sur le fondement des dispositions de l'article 15 de la directive du 12 juillet 2002, doit nécessairement être regardée, peu importe le contexte, comme une ingérence dans les droits protégés par la Charte qu'aucun motif d'aucune sorte ne saurait justifier (première question transmise dans l'affaire C-511/18 et première question transmise dans l'affaire C-512/18).

2) Les dispositions de la directive du 8 juin 2000, lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, §1er, de la Charte des droits fondamentaux de l'Union européenne et de la directive du 12 juillet 2002, prohibent radicalement à un État membre de l'Union européenne d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services qu'elles fournissent, peu importe l'objectif poursuivi (seconde question transmise dans l'affaire C-512/18).

3) La directive du 12 juillet 2002 lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, du règlement 2016/679 et de la directive 2016/680, prohibe des dispositions nationales qui permettent de réaliser des mesures de renseignement pour des finalités non limitées par un critère objectif ou visant à lutter contre des infractions ne relevant pas de la criminalité grave, qui permettent la collecte de données non nécessaires à la poursuites des finalités prévues, qui ne limitent pas par des critères objectifs au strict nécessaire les agents pouvant réaliser ces mesures, qui n'encadrent pas l'utilisation ultérieure des données collectées ou qui ne soumettent à aucun contrôle indépendant effectif la collecte, l'utilisation et les transferts des données (deuxième question transmise dans l'affaire C-511/18).

4) La directive du 12 juillet 2002, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, du règlement 2016/679 et de la directive 2016/680, subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à, d'une part, une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes et, d'autre part, à la possibilité de contester de façon effective devant une juridiction, pour toute personne et sans exception, toute mesure de recueil, d'exploitation et de transfert de renseignements (troisième question transmise dans l'affaire C-511/18).

BORDEREAU DES ANNEXES PRODUITES

Pièce n° 1 : Requête en intervention de CDT devant le Conseil d'Etat français ;

Pièce n° 2 : Conclusions de M. Edouard Crépey, rapporteur public du Conseil d'Etat, prononcées lors de la séance publique du 11 juillet 2018 des 10ème et 9ème chambres réunies, sur les affaires *La Quadrature du Net et autres*, n° 393099, 394924, 394922, 394844 et 397851.

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris