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

CONSEIL CONSTITUTIONNEL

INTERVENTION VOLONTAIRE

AU SOUTIEN DE LA

QUESTION PRIORITAIRE DE CONSTITUTIONNALITÉ

ENREGISTRÉE SOUS LES N^{os} 2021-976 QPC ET 2021-977 QPC

POUR :

1°) **L'association « La Quadrature du Net » (LQDN)**, association soumise à la loi du 1er juillet 1901, dont le siège est sis 115, rue de Ménilmontant à Paris (75020), représentée par M. Bastien Le Querrec, membre du collège solidaire en exercice ;

2°) **L'association « Franciliens.net »**, association soumise à la loi du 1er juillet 1901, fournisseur d'accès à Internet déclaré à l'ARCEP sous le n^{o} 11-0005, dont le siège est sis 60, rue des Orteaux (75020), représentée par son président en exercice.

CONTRE : **Les II et III de l'article L. 34-1 du code des postes et des communications électroniques**

Table des matières

FAITS

1. L'association « La Quadrature du Net » (LQDN), première exposante, promeut et défend les libertés fondamentales dans l'environnement numérique. Elle est régulièrement amenée à défendre droits et libertés fondamentaux devant le Conseil d'État [1] et le Conseil constitutionnel français [2], ainsi que devant le juge de l'Union européenne [3].

2. L'association « Franciliens.net », seconde exposante, est un fournisseur d'accès à Internet (FAI) associatif qui a notamment pour buts, aux termes de l'article 2 de ses statuts constitutifs, « *la promotion et la défense des principes suivants : Usage éthique d'Internet, et notamment : usage non-commercial et usage à des fins d'éducation et de recherche* » ainsi que « *Le droit à la vie privée, notamment en ligne, la protection de la confidentialité des communications et du secret des correspondances et la protection des données personnelles* ». Elle a déjà été amenée à défendre les libertés fondamentales relatives à Internet devant le Conseil d'État [4] et devant le Conseil constitutionnel [5].

3. Par arrêts n^os^ 21-83.710 et 21-83.729 du 7 décembre 2021, la chambre criminelle de la Cour de cassation a renvoyé au Conseil constitutionnel la question prioritaire de constitutionnalité (QPC) suivante :

1. CE, 21 avril 2021, n^os^ 393099, 394922, 397844, 397851, 424717, 424718 ; CE, 13 avril 2021, n^o^ 439360, 440978, 441151, 442307, 442317, 442363, 443239 ; CE, 22 décembre 2020, n^o^ 446155 ; CE, ord., 4 janvier 2021, n^os^ 447970, 447972 et 447974 (trois affaires) ; CE, ord., 18 mai 2020, n^os^ 440442, 440445 ; CE, 16 octobre 2019, n^o^ 433069 ; CE, 18 octobre 2018, n^o^ 404996 ; CE, 26 juillet 2018, n^os^ 394924, 394922, et 393099 (trois affaires) ; CE, 21 juin 2018, n^o^ 411005 ; CE, 18 juin 2018, n^o^ 406083 ; CE, 25 octobre 2017, n^o^ 411005 ; CE, 17 mai 2017, n^o^ 405792 ; CE, 18 novembre 2016, n^o^ 393080 ; CE, 22 juillet 2016, n^o^ 394922 ; CE, 15 février 2016, n^o^ 389140 ; CE, 12 février 2016, n^o^ 388134 ; CE, ord., 27 janvier 2016, n^o^ 396220 ; CE, 9 septembre 2015, n^o^ 393079 ; CE, 5 juin 2015, n^o^ 388134.

2. Cons. const., 20 mai 2020, n^o^ 2020-841 QPC ; Cons. const., 3 avril 2020, n^o^ 2020-834 QPC ; Cons. const., 30 mars 2018, n^o^ 2018-696 QPC ; Cons. const., 2 février 2018, n^o^ 2017-687 QPC ; Cons. const., 15 décembre 2017, n^o^ 2017-692 QPC ; Cons. const., 4 août 2017, n^o^ 2017-648 QPC ; Cons. const., 21 juillet 2017, n^o^ 2017-646/647 QPC ; Cons. const., 2 décembre 2016, n^o^ 2016-600 QPC ; Cons. const., 21 octobre 2016, n^o^ 2016-590 QPC ; Cons. const., 24 juillet 2015, n^o^ 2015-478 QPC.

3. TUE, ord., 14 décembre 2020, aff. T-738/16 ; CJUE, 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18.

4. CE, 30 décembre 2021, *La Quadrature du Net et autres*, n^o^ 428028

5. Cons. const., 15 février 2019, n^o^ 2018-764 QPC ; Cons. const., 14 juin 2019, n^o^ 2019-789 QPC ; Cons. const., 20 mai 2020, n^o^ 2020-841 QPC.

« *L'article L. 34-1, II et III, du code des postes et des communications électroniques, dans sa version en vigueur du 20 décembre 2013 au 31 juillet 2021, qui autorise pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, la conservation généralisée et indifférenciée pendant un an des données à caractère personnel prévues à l'article R. 10-13 du même code, sans réserver une telle conservation aux infractions les plus graves ni la soumettre à l'autorisation et au contrôle d'une autorité ou juridiction indépendante, contrevient-il au droit au respect de la vie privée garanti par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 et à l'article 34 de la Constitution ?* »

4. Ces arrêts ont été rendus aux motifs que :

« *4. La question posée présente un caractère sérieux. En effet, l'article L. 34-1, III, du code des postes et des télécommunications électroniques, dans sa version en vigueur du 20 décembre 2013 au 31 juillet 2021, permet de différer, pour une durée maximale d'un an, les opérations tendant à l'effacement ou à l'anonymisation de certaines catégories de données de connexion, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, dans le but de permettre la mise à disposition de l'autorité judiciaire.*

5. Or, ces dispositions sont susceptibles de constituer une atteinte excessive aux droits et libertés protégés par l'article 2 de la Déclaration des droits de l'homme et du citoyen, du fait que la conservation des données de connexion et leur accès ne sont pas réservés aux infractions les plus graves et ne sont pas soumises à l'autorisation ou au contrôle d'une juridiction ou d'une autorité administrative indépendante dont les décisions présentent un caractère contraignant. »

5. Ces arrêts ont été respectivement enregistrés, par le greffe du Conseil constitutionnel, le 10 décembre 2021, sous les n^{os} 2021-976 QPC et 2021-977 QPC.

6. Ce sont les instances auxquelles les exposantes souhaitent intervenir.

DISCUSSION

I. Sur la recevabilité de la présente intervention

7. D'emblée, il convient de relever que les associations exposantes sont bien recevables à intervenir.

8. Aux termes de l'alinéa 2 de l'article 6 du règlement intérieur sur la procédure suivie devant le Conseil constitutionnel pour les questions prioritaires de constitutionnalité :

> « *Lorsqu'une personne justifiant d'un intérêt spécial adresse des observations en intervention relatives à une question prioritaire de constitutionnalité avant la date fixée en application du troisième alinéa de l'article 1er et mentionnée sur le site internet du Conseil constitutionnel, celui-ci décide que l'ensemble des pièces de la procédure lui est adressé et que ces observations sont transmises aux parties et autorités mentionnées à l'article 1er. Il leur est imparti un délai pour y répondre. En cas d'urgence, le président du Conseil constitutionnel ordonne cette transmission.* »

9. L'objet statutaire de La Quadrature du Net est la défense des droits fondamentaux dans l'environnement numérique. À ce titre, l'association intervient dans les débats français et européens relatifs à ces enjeux, notamment en développant des analyses juridiques, en proposant et en évaluant des amendements au cours des procédures législatives. Elle promeut également auprès des citoyens des outils leur permettant d'assurer un meilleur contrôle de l'impact du numérique sur leur vie, et des ateliers de formation. En outre, elle est déjà intervenue, à plusieurs reprises, devant le Conseil constitutionnel dans des affaires ayant trait aux droits et libertés dans l'espace numérique.

10. L'objet statutaire de Franciliens.net est la promotion d'un « *usage éthique d'Internet* », du « *droit à la vie privée, notamment en ligne* », de « *la protection de la confidentialité des communications et du secret des correspondances et la protec-*

tion des données personnelles », ainsi que la promotion de la « *liberté d'expression et d'accès à l'information ainsi que la lutte contre la censure* » (article 2 des statuts de Franciliens.net). Cet objet statutaire est notamment mis en œuvre par la fourniture d'un accès Internet aux membres de l'association. Elle a ainsi vu son intérêt à agir reconnu dans un recours concernant des obligations de surveillance pesant sur les opérateurs de télécommunication (*cf.* CE, 30 décembre 2021, *La Quadrature du Net et autres*, n° 428028). Le Conseil constitutionnel a également reconnu qu'elle avait un intérêt spécial à intervenir dans une affaire concernant le droit de communication des données de connexion aux agents des douanes (*cf.* Cons. const., 15 février 2019, n° 2018-764 QPC) ou aux organismes de la sécurité sociale (*cf* Cons. const., 14 juin 2019, n° 2019-789 QPC).

11. Or, les dispositions faisant l'objet des présentes QPC affectent directement les droits et libertés défendus par les exposantes.

12. **Premièrement**, en prévoyant une obligation de conservation généralisée et indifférenciée des données de connexion, et un accès large sans contrôle par une juridiction ou une autorité administrative indépendante, les dispositions faisant l'objet de la présente QPC portent une atteinte manifestement disproportionnée au droit à la vie privée, à la protection des données personnelles et à la liberté d'expression, sur Internet et au-delà, que les associations exposantes se sont données pour mission de protéger.

13. **Deuxièmement**, La Quadrature du Net était requérante dans un recours contestant différents décrets pris en application des dispositions faisant l'objet de la présente QPC (*cf.* CE, Ass., 21 avril 2021, *French Data Network et autres*, n^{os} 393099, 394922, 397844, 397851, 424717 et 424718). Elle a, dans le cadre de ce recours, été à l'origine de l'arrêt de la Cour de Justice de l'Union européenne (CJUE) du 6 octobre 2020 (*cf.* CJUE, gr. ch., *La Quadrature du Net e. a.*, aff. C-511/18, C-512/18 et C-520/18) qui a rappelé certaines conditions pour qu'une obligation de conservation de données de connexion soit conforme au droit primaire de l'Union européenne, notamment la Charte des droits fondamentaux. La CJUE y a notamment réitéré l'interdiction d'une telle obligation généralisée et indifférenciée. Bien que les moyens tirés de la méconnaissance du droit de l'Union sont inopérants devant le Conseil constitutionnel, l'association La Quadrature du Net a un intérêt spécial à présenter dans le cadre de cette intervention le raisonnement qui a conduit la CJUE à poser de telles conditions strictes pour que le droit à la vie

privée, à la protection des données personnelles et à la liberté d'expression – tous trois protégés tant par la Constitution que par la Charte des droits fondamentaux de l'Union européenne – soient respectés. Par cette intervention, le Conseil pourra utilement s'inspirer des exigences européennes, tout comme il a pu le faire dans sa décision n° 2021-952 QPC du 3 décembre 2021, *M. Omar Y. [Réquisition de données informatiques par le procureur de la République dans le cadre d'une enquête préliminaire]*, en matière d'accès aux données de connexion.

14. **Troisièmement**, l'association Franciliens.net étant un FAI, c'est-à-dire un opérateur de communications électroniques, elle est elle-même soumise à l'obligation de conservation des données de connexion permise par les dispositions faisant l'objet de la présente QPC, bien que l'article L. 34-1 du code des postes et des communications électronique a été réécrit depuis. Ces dispositions, dans leur formulation ancienne ou actuelle, vont frontalement à l'encontre des intérêts qu'elle s'est donnée pour mission de défendre, puisqu'elles portent une atteinte manifestement disproportionnée au droit à la vie privée et à la liberté d'expression sur Internet, que Franciliens.net se doit d'assurer à ses membres et abonnés, ainsi qu'à leurs correspondants.

15. **En conclusion**, l'objet statutaire des associations exposantes ainsi que les actions, notamment juridictionnelles, qu'elles ont entreprises ces dernières années pour défendre leur objet, caractérisent un intérêt spécial justifiant leur intervention dans la présente QPC et démontrant la recevabilité des observations suivantes, adressées, en outre, dans le délai requis.

II. Sur les dispositions litigieuses

16. Les dispositions présentement contestées sont celles des II et III de l'article L. 34-1 du code des postes et des communications électroniques, qui s'applique au traitement des données personnelles dans le cadre de la fourniture au public de services de communications électroniques et notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification, dans leur version issue de la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense de la sécurité nationale. Aux termes de ces dispositions :

« II. – Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI.

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

III. – Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs. »

17. En édictant les dispositions litigieuses, le législateur a porté une atteinte

manifestement disproportionnée au droit au respect de la vie privée, au droit à la protection des données personnelles et au secret des correspondances, protégés par l'article 2 de la Déclaration de 1789, ainsi qu'au droit à la liberté d'expression, protégé par l'article 11 de la Déclaration. Par conséquent, il a manifestement rompu l'équilibre entre ces droits constitutionnels et l'objectif de sauvegarde de l'ordre public et de prévention des infractions.

III. Sur la conservation généralisée des données de connexion

18. Les dispositions faisant l'objet de la présente QPC imposent aux opérateurs de communications électroniques de conserver les données de connexion et de localisation liées à l'ensemble de leurs utilisateurs pendant un an.

19. Pour mémoire, la liste de ces données est dressée à l'article R. 10-13 du code des postes et des communication électronique, dans sa version applicable en l'espèce, issue du décret n° 2012-436 du 30 mars 2012 et antérieure au décret n° 2021-1361 du 20 octobre 2021, qui dispose que :

> « *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.

IV. – Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale. »

20. Dans son arrêt rendu le 6 octobre 2020 (*cf.* CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e. a.*, préc.), la CJUE a consolidé sa jurisprudence, déjà bien établie, relative à l'illégalité de tels régimes de conservation généralisée de données de connexion déjà définie dans l'arrêt *Digital Rights Ireland* (*cf.* CJUE, gr. ch., 8 avril 2014, *Digital Rights Ireland et autres*, aff. C-293/12, C-594/12, pt. 62) puis précisée dans son arrêt *Tele2* (*cf.* CJUE, grd. ch., 21 décembre 2016, *Tele2 Sverige*, aff. C-203/15).

21. Dans cet arrêt, la Cour a conclu à l'incompatibilité manifeste entre les droits fondamentaux garantis par le droit primaire de l'Union européenne – notamment le droit à la vie privée, à la protection des données personnelles et à la libertés d'expression, garantis par la Charte – et le régime de conservation généralisé et indifférencié des données de connexion et de localisation, imposé par le droit interne aux opérateurs de communications électroniques ainsi qu'aux hébergeurs.

22. Pour des raisons analogues, les dispositions faisant l'objet de la présente QPC, qui obligent les opérateurs de communications électroniques à conserver, de manière généralisée et indifférenciée, l'ensemble des données de connexion de leurs utilisateurs, sont manifestement contraire aux droits et libertés que la Constitution garantit. Si les moyens tirés de la méconnaissance du droit de l'Union sont inopérants en matière de contrôle constitutionnel, le Conseil a ici l'occasion de s'inspirer du contrôle opéré par la grande chambre de la CJUE dans son arrêt du 6 octobre 2020 précité, notamment parce que la grande chambre de la Cour a réalisé son contrôle à l'aune du droit à la vie privée, du droit à la protection des données per-

sonnelles et du droit à la liberté d'expression, tous trois protégés à la fois par la Charte des droits fondamentaux et par la Déclaration de 1789.

23. La conservation généralisée et indifférenciée des données de connexion imposée aux opérateurs de communications électroniques par les dispositions faisant l'objet de la présente QPC est manifestement contraire aux droits et libertés que la Constitution garantit – notamment le droit à la vie privée, le droit à la protection des données personnelles, le secret des correspondances et la liberté d'expression – en ce qu'elle repose sur des finalités de collecte manifestement trop étendues (A) et n'est justifiée par aucune nécessité (B).

A. S'agissant des finalités manifestement excessives

24. **En premier lieu**, les dispositions faisant l'objet de la présente QPC imposent un régime de conservation généralisée pour des finalités outrepassant largement celles qui sont strictement nécessaires, seules conformes aux droits et libertés que la Constitution garantit.

25. **En droit**, les droits et libertés que la Constitution garantit exigent que toute mesure de surveillance réponde à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi (*cf.*, *mutatis mutandis*, CJUE, *Tele2 Sverige*, préc., pt. 110). Ces conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné (*cf.*, *mutatis mutandis*, CJUE, *Tele2 Sverige*, préc., pt. 110).

26. Ainsi, la grande chambre de la Cour de justice a pu considérer qu'une réglementation nationale prévoyant une conservation permanente, généralisée et indifférenciée des données de connexion « *excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée dans une société démocratique* » même lorsque en vue de lutter contre la criminalité grave (*cf.* CJUE, *Tele2 Sverige*, préc., pt. 107).

27. Cette solution est reprise par la grande chambre de la Cour dans son arrêt du 6 octobre 2020 précité : une conservation des données de connexion ne peut être mise en œuvre par les opérateurs de communications électroniques sur

l'ensemble de leurs utilisateurs que s'« *il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave* […] *pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible* » (*cf.* CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, aff. C-511/18, pt. 137).

28. Ces menaces demeurent exceptionnelles en ce qu'elles « *se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique* » (même arrêt, pt. 136).

29. La Cour insiste : « *eu égard à la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte* [droit à la vie privée et droit à la protection des données personnelles] *résultant d'une telle mesure de conservation généralisée et indifférenciée des données, il importe d'assurer que le recours à celle-ci soit effectivement limité aux situations dans lesquelles il existe une menace grave pour la sécurité nationale* » (même arrêt, pt. 139). Cette exigence ne connaît qu'un unique relâchement : la conservation « *des seules adresses IP attribuées à la source d'une connexion* » qui, elle et elle seule, est permise pour lutter contre la criminalité grave en plus des atteintes à la sécurité nationale (*cf.* CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, préc., pts. 155 et 156).

30. Dès lors que les adresses IP constituent des données personnelles (*cf.* Cons. const., 10 juin 2009, *Loi favorisant la diffusion et la protection de la création sur internet*, n° 2009-580 DC, pt. 27 ; Civ. 1re, 3 novembre 2016, n° 15-22.595, Bull. civ. I, n° 206 ; Soc., 25 novembre 2020, n° 17-19.523, Bull. civ. V ; CJUE, 24 novembre 2011 *Scarlet Extended*, n° C-70/10, pt. 51 ; CJUE, 19 octobre 2016, *Breyer*, n° C-582/14, pt. 49 ; Cour EDH, 24 avril 2018, *Benedik c/ Slovénie, n° 62357/14, pts. 107 à 11*), leur conservation telle que définie dans ce cadre est néanmoins soumise à des exigences strictes, la Cour imposant que « *la durée de conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi* » et qu'une « *mesure de cette nature doit prévoir des conditions et des garanties strictes quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées* » (même arrêt, pt. 156).

31. En outre, la Cour de justice précise le cadre dans lequel les États membres peuvent, à titre strictement exceptionnel, recourir à une conservation généralisée et

indifférenciée des données de connexion qui doit, en toute hypothèse, être limitée dans le temps. C'est ainsi qu'une telle conservation ne peut être mise en œuvre que par une injonction *ad hoc* des autorités aux opérateurs, celle-ci ne pouvant jamais être permanente, mais toujours limitée à une durée strictement nécessaire (même arrêt, pt. 138).

32. En droit français, cette injonction devrait prendre la forme d'une décision individuelle qui doit être notifiée aux personnes concernées et non d'un acte réglementaire.

33. Seule l'hypothèse dans laquelle une menace, particulièrement grave, actuelle et tangible à la sécurité nationale persisterait permettrait de renouveler cette injonction, sans que la durée de chaque injonction ne dépasse un laps de temps prévisible de sorte que « *cette conservation ne saurait présenter un caractère systématique* » (même arrêt, pt. 138). En droit interne, cette situation véritablement exceptionnelle ne peut correspondre qu'à une situation d'état d'urgence « sécuritaire » au sens de la loi n° 55-385 du 3 avril 1955 relative à l'état d'urgence, ou aux hypothèses visées à l'article 16 de la Constitution.

34. **En l'espèce**, le III de l'article L. 34-1 du code des postes et des communications électroniques, dans sa version applicable à l'espèce, définit les finalités qui permettent au législateur d'imposer une obligation de conservation généralisée aux opérateurs de communications électroniques :

- la « *recherche, la poursuite et la constatation des infractions pénales en général* » ;
- un « *manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle* », c'est-à-dire l'identification par la Haute Autorité pour la diffusion des œuvres et la protection des droits sur Internet (Hadopi) [6] de personnes échouant à sécuriser leur accès à Internet ;
- « *les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal* ».

6. Devenue depuis le 1er janvier 2022 l'Autorité de régulation de la communication audiovisuelle et numérique (Arcom).

35. En application de cette disposition, l'article R. 10-13 du même code, dans sa version applicable à l'espèce, impose la conservation permanente des données de l'ensemble des utilisateurs de moyens de communications électroniques en France, applicable systématiquement, en toutes circonstances et en tous lieux, sans aucune garantie encadrant une telle collecte ou limitant l'exploitation des données conservées.

36. **Premièrement**, ces finalités sont particulièrement larges et ne répondent à aucun critère objectif permettant de limiter l'étendue de l'ingérence dans les droits et libertés que la Constitution garantit.

37. **Deuxièmement**, la conservation généralisée et indifférenciée imposée par les dispositions contestées n'est nullement circonscrite à un laps de temps limité et proportionné, mais demeure permanente. En outre, elle est imposée de manière générale et non subordonnée à l'intervention d'une injonction fondée sur l'existence d'une menace grave et précise à la sécurité nationale, et strictement encadrée. Au contraire, la conservation des données de connexion est mise en œuvre de manière générale et sur toute personne, sans aucun indice susceptible de laisser penser que le comportement des personnes concernées puisse avoir un lien, même indirect et lointain, avec une menace grave à la sécurité nationale, ou même avec la commission d'un crime ou d'un délit grave. Ce régime impose donc la conservation des données de connexion de l'ensemble de la population française, sans que cela réponde à une exigence de nécessité.

38. **Troisièmement**, les dispositions faisant l'objet de la présente QPC prévoient la collecte généralisée et indifférenciée notamment des adresses IP, données personnelles, de l'ensemble de la population, pour une durée minimale d'une année, pour la recherche de l'ensemble des infractions pénales, même les plus triviales. Les données personnelles ainsi obtenues peuvent ensuite être utilisées dans le cadre d'enquêtes qui ne se rapportent ni à la sauvegarde de la sécurité nationale, ni à la lutte contre la criminalité grave, ni même à la prévention des menaces graves contre la sécurité publique. En outre, aucune garantie n'est prévue afin d'éviter les abus inhérents à l'utilisation de ces données personnelles par les autorités publiques.

39. Les rapports d'activité de la Hadopi sont par ailleurs éloquents quant à l'utilisation de ces données pour des infractions triviales et montrent sans équivoque possible que les dispositions contestées mettent en œuvre une conservation

généralisée, permanente et indifférenciée dont l'utilisation première est faite pour punir le défaut de sécurisation d'un accès à Internet utilisé pour télécharger des œuvres culturelles, qui ne constitue qu'une simple contravention. En 2011, 2012 et 2014, la Hadopi a eu accès à ces données 20 millions de fois, et encore plus en 2016 (*cf.* pièce n° 5, p. 43). Si par la suite une telle utilisation a baissé, cela n'est pas dû à une retenue de l'autorité face à la disproportion entre ces moyens attentatoires aux libertés et les finalités poursuivies, mais à une baisse de l'utilité de son action avec une augmentation des contournements mis en œuvre par les utilisateurs (*cf.* même pièce). Toutefois, même après quatre années de baisse, les saisines de la Hadopi représentent un nombre considérable (4,5 millions en 2020) et constituent incontestablement la première finalité que les dispositions contestées permettent de poursuivre.

40. **En conclusion**, les dispositions faisant l'objet de la présente QPC permettent la conservation des données de connexion de l'ensemble de la population, sans que les finalités poursuivies soient précisément définies et strictement limitées à la lutte contre la criminalité grave et à la protection de la sécurité nationale, en contradiction manifeste avec les exigences de la Constitution.

41. Les dispositions contestées mettent ainsi en œuvre un régime généralisé, indifférencié et permanent de conservation préventive des données de connexion contraire aux droits et libertés que la Constitution garantit et doivent être censurés de ce seul fait.

B. S'agissant du défaut de nécessité intrinsèque

42. **En deuxième lieu**, les dispositions faisant l'objet de la présente QPC souffrent d'un défaut manifeste de nécessité.

43. **En droit**, à l'instar de ce que juge la grande chambre de la Cour de justice de l'Union européenne, « *la protection du droit fondamental au respect de la vie privée exige* [...] *que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire* », de sorte qu'« *une réglementation prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport*

entre les données à conserver et l'objectif poursuivi » (*cf.* CJUE, 6 octobre 2020, *La Quadrature du Net e.a.*, préc., pts. 130 et 133).

44. **En l'espèce**, **premièrement**, il serait faux de prétendre que seul l'accès aux données traitées par les opérateurs permet d'analyser rétrospectivement les communications. En effet, d'autres techniques existantes et actuellement utilisées permettent d'obtenir des résultats analogues sans imposer une surveillance généralisée et permanente de l'ensemble de la population.

45. Par exemple, il est désormais courant, pour les services d'enquête, d'accéder aux données enregistrées sur le téléphone des personnes mises en cause. Une fois saisies, ces données suffisent largement pour analyser rétrospectivement les communications de la personne suspectée d'avoir commis un délit ou un crime sur plusieurs semaines, voire plusieurs mois. Si, en théorie, l'accès à ces données est conditionné au fait que la personne ne les a pas supprimées de son téléphone avant que celui-ci n'ait été saisi, en pratique, supprimer ses données efficacement et à une fréquence suffisante est une opération technique complexe et rarement constatée par les enquêteurs.

46. Au demeurant, il serait illusoire de croire que les dispositions contestées, bien que mettant en œuvre une conservation généralisée, permanente et indifférenciée des données de connexion et de localisation, seraient à l'abri de stratégies de contournement. Un grand nombre d'outils, quotidiennement utilisés par les entreprises et le grand public, comme le *Virtual Private Network* ou réseau privé virtuel (VPN), rendent inutile une telle conservation des données de connexion parce que celles-ci ne montreront alors jamais le réel destinataire de la communication, mais uniquement le fournisseur du service de VPN qui relaie la communication au destinataire réel. Le fournisseur de ce service peut également être de droit étranger et donc ne pas être soumis aux dispositions contestées et ne pas coopérer avec les services d'enquête français. En effet un tel service de VPN est légalement proposé par toutes sortes d'acteurs dans le monde entier, du particulier jusqu'aux multinationales telles qu'Apple. Ainsi les personnes y ayant recours, que cela soit pour les nombreuses applications légitimes ou dans la volonté de cacher des traces d'actes répréhensibles, rendent inutilisables les données de connexion collectées par les dispositions contestées, pour les finalités que ces dernières poursuivent. Cependant, les personnes qui ne se servent pas de tels outils continuent d'être soumises à une surveillance généralisée et permanente qui devient ainsi discriminante en ce qu'elle

s'applique plus lourdement aux internautes n'ayant pas les connaissances ou les moyens nécessaires pour y échapper.

47. D'autres outils, plus rapides et efficaces que ceux permis par les dispositions contestées, sont à la disposition des enquêteurs. On peut par exemple citer un entretien de 2019, dans lequel la cheffe du pôle central d'analyse des traces technologiques de la police nationale expliquait, au sujet de l'outil fourni par la société Cellebrite, que : « *avec ce kiosque qui sera installé dans les commissariats de premier niveau, il suffira de brancher le téléphone et toutes les données seront extraites pendant la garde à vue : SMS, photos géolocalisées…* […] *L'an prochain, cent nouvelles machines seront installées en Île-de-France et dans le Sud. En tout, cinq cents machines doivent être installées d'ici 2024, pour un coût de quatre millions d'euros. Nous l'avons déjà testé lors du G7, pour traiter les téléphones des personnes gardées à vue, et les retours ont été très positifs* » (*cf.* pièce n° 6). En tout, l'État a conclu deux marchés publics pour déployer et maintenir ces kiosques, pour un coût total de 7 millions d'euros (*cf.* pièce n° 7).

48. Ainsi, les services d'investigation judiciaire, comme ceux de renseignement, disposent d'ores et déjà de moyens d'investigation efficaces, qui leur permettent aisément de se passer entièrement et de plus en plus facilement des données conservées de manière généralisée et indifférenciée par des opérateurs, afin d'analyser rétrospectivement les communications d'une personne. Ces outils sont utilisés de manière ciblée sur des dispositifs liés à des personnes mises en cause. Plus rapides et efficaces que les dispositifs ayant recours aux dispositions contestées, ces outils sont plus respectueux des libertés fondamentales de l'ensemble de la population car ils n'opèrent pas de manière généralisée et permanente.

49. **Deuxièmement**, il est tout aussi faux de prétendre qu'il faudrait contraindre les opérateurs pour que ceux-ci conservent des données exploitables par l'administration.

50. Au contraire, au fil des années, les usages d'Internet croissent et se diversifient, en engendrant une quantité toujours plus importante de données de communication. Les utilisateurs ont recours à de plus en plus de services différents (messageries instantanées, email, réseaux sociaux, etc.) qui collectent et conservent volontairement des données pour leurs propres besoins, notamment techniques ou de facturation. Ainsi, entre 2017 et 2019, la proportion de la population française

qui « *échange des messages via des applications* » est passée de 43 % à 62 % et celle qui « *téléphone via des applications* » de 31 % à 51 % (*cf.* pièce n° 8, page 114). La multiplication du nombre d'intermédiaires auprès de qui l'administration peut obtenir des données de connexion diminue mécaniquement la nécessité de s'assurer que ceux-ci conservent le plus longtemps possible les données qu'ils exploitent. Par ailleurs, les données conservées par ces intermédiaires identifient de manière plus directe et immédiate les utilisateurs que ne le font les données des opérateurs de télécommunications.

51. Ainsi, les services d'enquête judiciaire comme ceux de renseignement ont de moins en moins besoin de contraindre les intermédiaires pour que ceux-ci conservent des données de communication utiles à leurs enquêtes. *A contrario*, les opérateurs de télécommunication sont donc tenus de conserver des données de moins en moins utiles.

52. **Troisièmement**, s'il est certes vrai qu'une conservation généralisée et indifférenciée de l'ensemble des données de connexion de la population est susceptible, dans certains cas et dans les limites exposées *supra*, de présenter une utilité pour les services de police, il est tout aussi vrai qu'une telle conservation n'est pas nécessaire à l'accomplissement des missions de police.

53. D'abord, la situation a largement évolué depuis 2018, tel que le constate la Commission nationale de contrôle des techniques de renseignement (CNCTR) deux années plus tard, en juin 2020, dans son 4e rapport d'activité (*cf.* pièce n° 9). Elle détaille le fait que le nombre de demandes d'accès aux données de connexion a baissé de 20 % au cours des deux dernières années observées (passant de 48 000 à 40 000), tandis que les autres techniques de renseignement continuent de croître à des taux importants (de 8 800 à 12 500 pour les interceptions, de 3 700 à 7 600 pour la géolocalisation et de 9 300 à 13 700 pour les « *autres techniques* »).

54. Ensuite, la quasi-totalité des attentats terroristes déjoués ces dernières années sont le fait d'interventions et d'actions humaines, et non le résultat de techniques de renseignement (*cf.* pièce n° 10).

55. Ici encore, les faits montrent que l'obligation de conservation généralisée est de moins en moins utile au fur et à mesure que les années passent, les services

de renseignement diversifiant leurs approches et techniques.

56. Il n'a jamais été démontré que les informations tirées de l'exploitation des données issues d'une surveillance permanente, généralisée et indifférenciée de la population ne sauraient être fournies par d'autres techniques d'enquêtes ou d'autres sources de preuve moins attentatoires aux droits constitutionnellement protégés.

57. La prétendue nécessité de ce dispositif de conservation généralisée et indifférenciée des données de connexion est directement contredite par un examen historique et géographique.

58. D'une part, la conservation généralisée et indifférenciée des données de connexion n'est née qu'au tout début des années 2000, à l'occasion d'un effet d'aubaine dû aux évolutions technologiques. La facilité technologique avec laquelle cette surveillance est mise en place induit à la présenter, à tort, comme acceptable. Pour saisir pleinement les enjeux de cette question, il est intéressant de transposer les règles gouvernant la conservation généralisée et indifférenciée des données de connexion à la période antérieure à l'invention et la diffusion massive des téléphones portables et des accès à Internet : la conservation généralisée et indifférenciée des données de connexion se serait ainsi traduite par un suivi des déplacements de l'ensemble de la population (qui aurait été matériellement impossible sans la téléphonie mobile) mais également par une surveillance de toutes les correspondances postales, par l'établissement d'un registre recensant l'ensemble des courriers et colis échangés, leurs expéditeurs et leurs destinataires, leurs poids, leurs formes, leurs caractéristiques principales, leurs fréquences, etc. Une telle surveillance est l'apanage des régimes autoritaires et n'a pas sa place dans un État de droit. Dès lors qu'une telle surveillance n'a pas sa place dans le monde « matériel », elle ne peut pas être tolérée non plus dans le monde « immatériel ».

59. D'autre part, l'acharnement du gouvernement à alléguer de la nécessité de ce dispositif est immédiatement contredite par la simple constatation que d'autres États arrivent parfaitement à assurer leurs missions de police sans un tel dispositif. L'exemple le plus parlant est celui des États-Unis d'Amérique. Le droit étasunien, difficilement qualifiable de laxiste en matière de surveillance, n'impose en effet aucunement un régime de conservation généralisée et indifférenciée des données de connexion, comme l'ONG Center for Democracy and Technology (CDT), intervenante devant la CJUE, l'a d'ailleurs rappelé à la Cour.

60. **Il en résulte que** l'obligation de conservation généralisée, permanente et indifférenciée des données de connexion porte une atteinte manifestement disproportionnée aux droits constitutionnellement protégés en ce qu'elle manque cruellement de nécessité.

61. À tous égards, la censure immédiate est inévitable.

PAR CES MOTIFS, les associations La Quadrature du Net et Franciliens.net, exposantes, concluent qu'il plaise au Conseil constitutionnel de :

ADMETTRE leur intervention dans les présentes instances ;

DÉCLARER contraire à la Constitution les dispositions des II et III de l'article L. 34-1 du code des postes et des communications électroniques, dans leur version en vigueur du 20 décembre 2013 au 31 juillet 2021, avec effet immédiat.

Fait à Paris, le 3 janvier 2022

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

Pièce n° 1 : Statuts de La Quadrature du Net ;

Pièce n° 2 : Statuts de Franciliens.net ;

Pièce n° 3 : Pouvoir spécial de La Quadrature du Net ;

Pièce n° 4 : Pouvoir spécial de Franciliens.net ;

Pièce n° 5 : Rapport d'activité de la Hadopi pour 2020 ;

Pièce n° 6 : Émilie Massemin et Isabelle Rimbert, « Nous avons visité Milipol, le salon de la répression », *Reporterre*, 21 novembre 2019 ;

Pièce n° 7 : Christophe-Cécil Garnier, « Bientôt dans presque tous les commissariats, un logiciel pour fouiller dans vos portables », *Streetpress*, 20 janvier 2020 ;

Pièce n° 8 : ARCEP, Baromètre du numérique, 2019 ;

Pièce n° 9 : CNCTR, 4e rapport d'activité, pour l'année 2019 ;

Pièce n° 10 : Jacques Follorou, « 58 des 59 attentats déjoués depuis six ans l'ont été grâce au renseignement humain », *Le Monde*, 15 octobre 2019.