

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

SECONDES OBSERVATIONS

POUR : 1°) L'association « La Quadrature du Net » (LQDN);
 2°) L'association « Franciliens.net ».

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

Table des matières

Faits	3
Discussion	4
I Sur l'atteinte grave créée par la conservation des données de connexion	4
II Sur l'application de l'arrêt <i>La Quadrature du Net e. a.</i> en droit constitutionnel belge	6
III Sur l'accès aux données de connexion en l'absence de contrôle par une autorité administrative indépendante ou une juridiction	6
IV Sur la conservation rapide des données de connexion (« <i>quick freeze</i> »)	8
Bordereau des productions	10

FAITS

1. Par un mémoire enregistré le 3 janvier 2022, les associations La Quadrature du Net et Franciliens.net, exposantes, ont demandé à intervenir au soutien d'une question prioritaire de constitutionnalité (QPC) relative à la conservation généralisée et indifférenciée des données de connexion et enregistrée dans les affaires n^{os} 2021-976 QPC et 2021-977 QPC.

2. Elles ont rappelé le contrôle exercé par la Cour de Justice de l'Union européenne (CJUE), notamment dans sa jurisprudence *La Quadrature du Net e. a.* (cf. CJUE, gr. ch., 6 octobre 2020, aff. C-511/18, C-512/18 et C-520/18), en matière de conservation des données de connexion, invitant le Conseil constitutionnel à s'inspirer de ce contrôle opéré notamment au regard du droit à la vie privée, du droit à la protection des données personnelles et du droit à la liberté d'expression, tous trois protégés par la Charte des droits fondamentaux de l'UE et par la Déclaration de 1789.

3. Le 6 janvier 2022, le greffe du Conseil constitutionnel a transmis aux exposantes les mémoires produits dans les affaires n^{os} 2021-976 QPC et 2021-977 QPC, et les a invité à produire leurs éventuelles nouvelles observations d'ici au 18 janvier 2022 à 18 heures.

4. Par les présentes observations, les exposantes souhaitent compléter leurs écritures du 3 janvier dernier, ainsi que répondre aux premières observations du Premier ministre datées du même jour. Ces nouvelles observations ne remettent pas en cause les moyens précédemment articulés, que les exposantes réitèrent expressément.

DISCUSSION

I. Sur l'atteinte grave créée par la conservation des données de connexion

5. À titre liminaire, il est essentiel de rappeler l'importance que revêt la protection des données de connexion, notamment en limitant de manière stricte leurs possibilités de conservation. Une telle obligation de conservation – qu'elle soit généralisée ou ciblée – porte en effet intrinsèquement atteinte au droit à la vie privée, au droit à la protection des données personnelles, au droit au secret des correspondances et au droit à la liberté d'expression, protégés par les articles 2 et 11 de la Déclaration de 1789.

6. Les données de connexion révèlent ce qui entoure une communication. Elles permettent d'indiquer l'emplacement d'une communication (antenne téléphonique ou point de livraison d'une connexion internet fixe) et divulguent le graphe social d'une personne, c'est-à-dire les contacts avec qui elle est régulièrement en communication.

7. Ainsi, un certain nombre d'informations peuvent être déduites de l'analyse des seules données de connexion, alors même que le contenu des correspondances n'est pas étudié. En effet, si une personne communique régulièrement avec un avocat, un journaliste ou un médecin, on peut en déduire certaines informations. Par exemple, si un journaliste publie un article sur la base d'une source qu'il tient à garder secrète, il est assez facile de retrouver ladite source par l'étude des données de connexion, notamment en recherchant des communications avec un nouveau contact précédant la publication de l'article. Ce faisant, il n'est pas nécessaire de connaître le contenu exact de la communication pour pouvoir en déduire suffisamment d'informations, et donc porter une atteinte au secret des correspondances malgré l'absence d'analyse de leur contenu.

8. La CJUE ne se trompait pas non plus quant à son analyse de la sensibilité des données de connexion, puisqu'elle relevait que « *la conservation des données relatives au trafic et des données de localisation constitue, par elle-même, [...] une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection*

*des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, sans qu'il importe de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence » (cf. CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e. a.*, préc., pt. 115). Elle poursuit en relevant de la même manière que « les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent 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. En particulier, ces données fournissent les moyens d'établir 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. même arrêt, pt. 117).*

9. Par ailleurs, la conservation des données de connexion peut dissuader les citoyens d'user de leur droit à la liberté d'expression. La CJUE a relevé que la conservation généralisée et indifférenciée des données de connexion « est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de celle-ci » (cf. même arrêt, pt. 118). Le Conseil constitutionnel a lui-même relevé qu'une mesure de surveillance peut constituer une atteinte au droit à la liberté d'expression (cf. Const. const., 27 décembre 2019, *Loi de finances pour 2020*, n° 2019-796 DC, pt. 81).

II. Sur l'application de l'arrêt *La Quadrature du Net e. a.* en droit constitutionnel belge

10. **En premier lieu**, la Cour constitutionnelle de Belgique a, par un arrêt n° 57/2021 du 22 avril 2021, appliqué en droit interne belge la décision *La Quadrature du Net e. a.* de la CJUE, ce qui l'a logiquement amené à annuler les articles 2, b), 3 à 11 et 14 de la loi belge du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (*cf.* pièce n° 11, §§ B.15 à B.20), avec effet immédiat (*cf.* pièce n° 11, § B.24.3).

11. Elle a notamment estimé qu'une obligation généralisée et indifférenciée de conservation des données de connexion, telle que prévue par la loi belge déférée au contrôle de la Cour constitutionnelle, portait une atteinte disproportionnée au droit à la vie privée, au droit à la protection des données personnelles et au droit à la liberté d'expression (*cf.* pièce n° 11, § B.15 al. 2).

12. Pour en arriver à cette conclusion, la Cour constitutionnelle belge opère un contrôle la loi belge au regard du droit à la vie privée, du droit à la protection des données personnelles et du droit à la liberté d'expression, tous trois également protégés par la Déclaration de 1789 (*cf.* observations du 3 janvier 2022, pt. 22).

III. Sur l'accès aux données de connexion en l'absence de contrôle par une autorité administrative indépendante ou une juridiction

13. **En deuxième lieu**, le Conseil constitutionnel pourra également utilement s'inspirer de la décision *Prokuratuur* de la CJUE (*cf.* CJUE, gr. ch., 2 mars 2021, *Prokuratuur*, aff. C-746/18) en ce qui concerne les règles nécessaires en matière d'accès aux données de connexion, et conclure à l'inconstitutionnalité des dispositions faisant l'objet de la présente QPC en ce qui concerne leur accès.

14. En effet, une obligation de conservation des données de connexion vise à permettre *in fine* leur accès : la conservation ne se conçoit **que** parce qu'est prévu l'accès ultérieurement, contrairement à ce que tente vainement de soutenir le Premier ministre dans ses observations. Partant, les conditions d'accès – notamment

le contrôle indépendant des conditions d'accès et de la gravité de l'acte réprimé justifiant l'accès – doivent être envisagées en même temps que les obligations de conservations.

15. Dans son arrêt *Prokuratuur*, la grande chambre de la CJUE a précisé les conditions nécessaires pour que l'accès aux données de connexion soit conforme aux droits fondamentaux, en particulier les conditions d'indépendance que doivent remplir les autorités judiciaires et administratives qui contrôlent la licéité des accès. La CJUE exige que l'accès aux données de connexion fasse l'objet d'un contrôle par une autorité indépendante (cf. CJUE, 2 mars 2021, *Prokuratuur*, préc., pts. 46 et s.). Elle a notamment précisé que, lorsque le contrôle n'est pas effectué par une juridiction mais par une autorité administrative, celle-ci doit avoir « *la qualité de tiers par rapport à celle qui demande l'accès aux données* », afin de pouvoir être qualifiée d'indépendante (cf. même arrêt, pt. 54).

16. **En droit**, les articles 2 et 11 de la Déclaration de 1789 garantissent notamment le droit à la vie privée, le droit à la protection des données personnelles, le secret des correspondances, ainsi que le droit à la liberté d'expression.

17. Dans sa décision *M. Omar Y. [Réquisition de données informatiques par le procureur de la République dans le cadre d'une enquête préliminaire]* (cf. Cons. const., 3 décembre 2021, n° 2021-952 QPC), le Conseil constitutionnel a estimé que l'article 77-1-1 du code de procédure pénale dans sa rédaction résultant de la loi 24 décembre 2020, et 77-1-2 du même code dans sa rédaction résultant de la loi du 23 mars 2019, en ce qu'ils permettent l'accès à des données de connexion ou d'autres données contenues dans des traitements informatisés en ne prévoyant pas de garanties suffisantes, portaient, dès lors, une atteinte disproportionnée au droit à la vie privée.

18. En particulier, le Conseil constitutionnel a relevé que « *l'autorisation du procureur de la République, magistrat de l'ordre judiciaire auquel il revient, en application de l'article 39-3 du code de procédure pénale, de contrôler la légalité des moyens mis en œuvre par les enquêteurs et la proportionnalité des actes d'investigation au regard de la nature et de la gravité des faits* », n'est pas une garantie suffisante (cf. même arrêt, pt. 13).

19. **En l'espèce**, dans ses décisions de renvoi, la Cour de cassation a bien souligné l'absence de contrôle indépendant au moment de l'accès aux données de connexion. Elle relevait ainsi que « [l']accès [n'est] pas [...] [soumis] à l'autorisation ou au contrôle d'une juridiction ou d'une autorité administrative indépendante dont les décisions présentent un caractère contraignant. » (cf. décision de renvoi, pt. 5)

20. Au cas présent, force est de constater qu'aucune disposition législative – ni les dispositions faisant l'objet de la présente QPC, ni d'autres dispositions spéciales – ne prévoit de mécanisme de contrôle indépendant, ni par une autorité administrative indépendante, ni par une juridiction.

21. **Il en résulte que** les dispositions faisant l'objet de la présente QPC, en ne prévoyant pas que l'accès aux données de connexion soit subordonné au contrôle par une juridiction ou par une autorité administrative indépendante, porte une atteinte manifestement disproportionnée au droit à la vie privée, au droit à la protection des données personnelles, au secret des correspondances et au droit à la liberté d'expression.

IV. Sur la conservation rapide des données de connexion (« quick freeze »)

22. **En troisième lieu**, il est important de relever que la conservation généralisée et indifférenciée des données de connexion n'est pas nécessaire à la poursuite de l'objectif de recherche des auteurs d'infraction, notamment en raison de la possibilité de conserver ces données de manière ciblée par la technique de « conservation rapide » (en anglais « *quick freeze* »).

23. La technique de la « conservation rapide » consiste pour les autorités publiques, en absence d'obligation de conservation généralisée et indifférenciée des données de connexion, à, tout de même, pouvoir imposer aux intermédiaires techniques de conserver les données à venir ou celles qui ont été conservées temporairement pour des finalités de facturation d'un service (pouvoir démontrer à un abonné qu'il a bien passé les communications facturées) ou de protection d'une infrastructure informatique (pour se prémunir d'une attaque informatique en analysant le trafic réseau passé).

24. En pratique, les données de connexion sont régulièrement conservées pendant plusieurs semaines, voire plusieurs mois, de manière ciblée, par les intermédiaires techniques. Une « conservation rapide » consiste donc, par le biais d'une injonction, à exiger d'un opérateur technique qu'il conserve, pour une nouvelle finalité de recherche des auteurs d'infraction, les données à venir ou celles qu'il aurait traitées et conservées pour une finalité différente.

25. La CJUE mentionne également cette possibilité de « conservation rapide » aux points 160 et suivants de sa décision *La Quadrature du Net e. a.*, notamment en visant explicitement l'article 16 de la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (cf. CJUE, gr. ch., 6 octobre 2020, *La Quadrature du Net e. a.*, préc., pt. 162). Cet article précise déjà que les États membres se donnent les moyens « d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique ».

26. **Il en résulte que** les dispositions faisant l'objet de la présente QPC sont manifestement disproportionnées en ce qu'elles ne sont pas nécessaires à la poursuite de l'objectif recherche des auteurs d'infraction.

PAR CES MOTIFS, les associations La Quadrature du Net et Franciliens.net, exposantes, persistent dans leurs précédentes conclusions.

Fait à Paris, le 18 janvier 2022

Alexis FITZJEAN Ó COBHTHAIGH
Avocat au Barreau de Paris

BORDEREAU DES PRODUCTIONS

Pièces produites avec les observations du 3 janvier 2022 :

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 Rimbart, « 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, 4^e 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.

Nouvelle pièce :

Pièce n° 11 : Cour constitutionnelle belge, 22 avril 2021, n° 57/2021.