Conservation des données de connexion, comment le Conseil d'État a sauvé la majorité des enquêtes judiciaires

Matthieu Audibert

▶ **To cite this version:**

Matthieu Audibert. Conservation des données de connexion, comment le Conseil d'État a sauvé la majorité des enquêtes judiciaires. Veille juridique, 2021, 96, pp.16-25. hal-03251929

HAL Id: hal-03251929
https://hal.science/hal-03251929v1

Submitted on 7 Jun 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Droit de l'espace numérique

Capitaine Matthieu AUDIBERT

Conservation des données de connexion
Comment le Conseil d'État a sauvé la majorité des enquêtes judiciaires

Conseil d'État, French Data Network et autres, 21 avril 2021, n° 3930922

La décision rendue le 21 avril 2021 par le Conseil d'État est certainement l'une des plus importantes de ces dernières années. Rendue en Assemblée du contentieux[1], elle vient clore (temporairement ?) un chapitre ouvert depuis 2014 s'agissant de la question ô combien sensible de l'équilibre entre protection de la vie privée et recherche et poursuite des auteurs d'infractions pénales.

Depuis 2014, la Cour de justice de l'Union européenne (CJUE) poursuit l'encadrement des dispositifs juridiques liés à la conservation et à l'accès, à des fins pénales, aux données de localisation et de trafic (données de connexion) des utilisateurs[2]. En effet, au travers de ses différents arrêts[3], la CJUE a posé plusieurs

1. Formation de jugement la plus solennelle du Conseil d'État et réservée aux affaires les plus importantes.

2. AUDIBERT, Matthieu. La conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ? [en ligne] *La veille juridique du Centre de recherche de l'École des officiers de la gendarmerie nationale*, mars 2021, p. 16-35. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/veille-juridique/mars-2021

3. Arrêt du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., C-293/12 et C-

grands principes qui mettaient à mal le régime juridique français de conservation des données de connexion[4] au regard de la Charte des droits fondamentaux de l'UE. Le droit français prévoit ainsi un cadre juridique précis organisant la conservation généralisée et indifférenciée des données techniques de connexion et des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne[5]. Ces données sont conservées pendant une année[6].

Par ailleurs, il convient de souligner que l'arrêt Quadrature du Net rendu le 6 octobre 2020 par la CJUE faisait suite à plusieurs questions préjudicielles posées par le Conseil[7].

Que nous apporte cette décision ?

594/12 ; arrêt du 21 décembre 2016, Tele2 Sverige, C-203/15 et C-698/15 ; arrêt du 6 octobre 2020, La Quadrature du Net e.a. contre Premier ministre e.a., C-511/18, C-512/18 et C-520/18 ; arrêt du 2 mars 2021, Prokuratuur, C-746/18.

4. LASSALLE, Maxime. Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE. *Recueil Dalloz*, 2021, p. 406.

5. AUDIBERT, Matthieu. La conservation des données, le droit français et la Cour de justice de l'Union européenne, quelles conséquences pour les enquêtes judiciaires ? [en ligne] *La veille juridique du Centre de recherche de l'École des officiers de la gendarmerie nationale*, novembre 2020, p. 15-29. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/veille-juridique/novembre-2020

6. Article L. 34-1 III du Code des postes et des communications électroniques. Article 6 II de la loi n° 2004-575 du 21 juin 2004, loi pour la confiance dans l'économie numérique (LCEN).

7. Conseil d'État, 26 juillet 2018, n° 394922, 397844 et 397851.

Droit de l'espace numérique

Particulièrement sensible à maintenir le régime juridique actuel, le Gouvernement demandait au Conseil d'État de déclencher un contrôle « *ultra vires* ». De quoi s'agit-il ?
Le Gouvernement invitait ainsi le Conseil à contrôler puis à constater que la CJUE avait dépassé les limites de ses compétences avec celles relevant des États membres au regard des traités. Ce faisant, le Conseil était invité à écarter la jurisprudence de la CJUE, ce qui aurait constitué un bouleversement majeur dans l'ordre juridique communautaire. Ce type de contrôle a déjà été mis en œuvre en Allemagne[8].

Toutefois, le Conseil a refusé le contrôle « *ultra vires* » demandé par le Gouvernement et a ainsi évité la guerre des juges[9]. Il s'est en revanche appuyé sur le droit constitutionnel français puis sur l'arrêt Quadrature du Net pour contourner certains principes dégagés par la CJUE dans ses différents arrêts, un bel exercice d'équilibrisme[10].

À cet effet, le Conseil introduit sa décision en affirmant avec solennité la primauté de la Constitution[11]. Elle est la norme suprême en droit national. Le Conseil en tire comme conséquence qu'il lui

8. JOOP, Olivier. Guerre des cours ou dialogue de sourds ? L'arrêt de la Cour constitutionnelle fédérale allemande relative au programme PSPP de la Banque centrale européenne, *RTD Eur.*, 2021, p. 110.
9. DE MONTECLER, Marie-Christine. Conservation des données : la guerre des juges n'aura pas lieu. *Dalloz Actualité*, avril 2021.
10. REES, Marc. Comment le Conseil d'État a sauvé la conservation des données de connexion [en ligne]. NextINpact, 22 avril 2021. Disponible sur : https://www.nextinpact.com/article/45613/comment-conseil-detat-a-sauve-conservation-donnees-connexion
11. Point 4.

revient de vérifier que l'application du droit communautaire ne remet pas en cause des exigences constitutionnelles qui ne seraient pas garanties de façon équivalente par le droit de l'Union.

Il s'agit en réalité d'une forme de clause de sauvegarde fondée sur la primauté de la Constitution dans la hiérarchie des normes. Ainsi, quand il est reproché à un acte réglementaire de ne pas respecter le droit de l'Union, alors le moyen soulevé en défense peut être écarté lorsque son acceptation aurait pour conséquence de bloquer une garantie constitutionnelle inexistante dans le droit communautaire[12]. Dans ce cas, le Conseil va alors contrôler la conformité du texte réglementaire non au droit communautaire, mais directement à la Constitution[13].

Dans son mémoire, le Gouvernement invoquait ainsi la sauvegarde des intérêts fondamentaux de la nation, la prévention des atteintes à l'ordre public, les atteintes à la sécurité des personnes et des biens, la lutte contre le terrorisme, ainsi que la recherche des auteurs d'infractions pénales[14]. Celles-ci « constituent des objectifs de valeur constitutionnelle, nécessaires à la sauvegarde de droits et de principes de même valeur, qui doivent être conciliés avec l'exercice des libertés constitutionnellement garanties, au nombre desquelles figurent la liberté individuelle, la liberté d'aller et venir et le respect de la vie privée[15] ».

12. Point 5.
13. Points 5 à 8.
14. Point 9.
15. *Ibidem*.

Néanmoins, et c'est toute l'habilité remarquable de cette décision, le Conseil d'État ne met pas en œuvre cette clause de sauvegarde, certainement pour ne pas ouvrir un front avec la CJUE.

En effet, il va s'appuyer sur l'arrêt Quadrature du Net pour, *in fine*, préserver la conservation et l'utilisation des données de connexion dans le cadre de la majorité des enquêtes judiciaires.

Dans son arrêt Quadrature du Net[16], la CJUE énonce que la conservation généralisée et indifférenciée des données de connexion est permise au titre de la sécurité nationale.

Ainsi, le Conseil relève que « le droit de l'Union européenne permet d'imposer aux opérateurs la conservation généralisée et indifférenciée des données de trafic et de localisation autres que les adresses IP aux seules fins de sauvegarde de la sécurité nationale lorsqu'un État est confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, sur injonction d'une autorité publique, soumise à un contrôle effectif d'une juridiction ou d'une autorité administrative indépendante, chargée notamment de vérifier la réalité de la menace, pour une période limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace [17]».

Ce faisant, le Conseil juge illégale l'obligation de conservation

16. Arrêt du 6 octobre 2020, La Quadrature du Net e.a. contre Premier ministre e.a., C-511/18, C-512/18 et C-520/18, points 134 à 139.
17. Point 31.

généralisée et indifférenciée des données de connexion (hormis les données peu sensibles : état civil, adresse IP, comptes et paiements) pour les besoins liés à la poursuite des infractions pénales. Il rappelle ainsi que le droit de l'Union s'oppose à ce que soit imposée aux opérateurs la conservation généralisée et indifférenciée des données de trafic et de localisation autres que les adresses IP, y compris aux fins de lutte contre la criminalité grave.

Néanmoins, il relève que cette conservation généralisée et indifférenciée aujourd'hui imposée aux opérateurs par le droit français est bien justifiée par une menace pour la sécurité nationale, comme cela est requis par la CJUE[18]. Il relève notamment « que la France est confrontée à une menace pour sa sécurité nationale (…). Cette menace est non seulement prévisible mais aussi actuelle. Cette menace procède d'abord de la persistance d'un risque terroriste élevé, ainsi qu'en témoigne notamment le fait que sont survenues sur le sol national au cours de l'année 2020 six attaques abouties ayant causé sept morts et onze blessés. Deux nouveaux attentats ont déjà été déjoués en 2021. Le plan Vigipirate a été mis en œuvre au niveau "Urgence attentat" entre le 29 octobre 2020 et le 4 mars 2021 puis au niveau "Sécurité renforcée - risque attentat" depuis le 5 mars 2021, attestant d'un niveau de menace terroriste durablement élevé sur le territoire[19]. »

Il impose à ce sujet au gouvernement de procéder, sous le contrôle du juge administratif, à un réexamen périodique de l'existence d'une

18. Points 42 à 46.
19. Point 44.

telle menace[20].

Pour la poursuite des infractions pénales, le CE énonce que la solution suggérée par la CJUE dans son arrêt Quadrature du Net de « conservation ciblée[21] » en amont des données n'est ni matériellement possible, ni opérationnellement efficace[22]. En effet, il n'est pas possible de prédéterminer les personnes qui seront impliquées dans une infraction pénale qui n'a pas encore été commise ou le lieu où elle sera commise[23].

Pour contourner les infaisabilités opérationnelles des solutions proposées par la CJUE, le Conseil suggère de recourir à la méthode de « conservation rapide » autorisée par le droit européen[24]. Celle-ci peut s'appuyer sur le stock de données conservées de façon généralisée et indifférenciée pour les besoins de la sécurité nationale et peut être utilisée pour la poursuite des infractions pénales[25]. Autrement dit, le critère lié à la sécurité nationale devient le support juridique autorisant l'accès en judiciaire à ces données, sous deux réserves.

Tout d'abord, cette conservation rapide et cet accès ne peuvent être autorisés que dans le cadre de la criminalité grave. Cela implique de

20. Points 31 et 46.
21. Point 54.
22. Point 57.
23. Point 54.
24. Points 55 et 56. Cette méthode de « conservation rapide » est prévue par la Convention du Conseil de l'Europe sur la cybercriminalité dite Convention de Budapest du 23 novembre 2001 (articles 16 et 17) à laquelle la France est partie.
25. Point 57.

prévoir un seuil de gravité en excluant *de facto* les contraventions et certains délits pour lesquels les enquêteurs ne pourront plus requérir les opérateurs, les crimes étant nécessairement graves. En outre, selon la jurisprudence de la CJUE, cet accès ne pourra être autorisé que par une autorité administrative indépendante ou un juge indépendant qui doit avoir la qualité d'un tiers par rapport aux enquêteurs[26]. Ce juge ne doit pas être impliqué dans la conduite des investigations et doit avoir une position de neutralité vis-à-vis des parties à la procédure pénale[27].

Le recours au critère lié à la sécurité nationale permet donc de sauvegarder l'accès aux données de connexion dans le cadre des enquêtes judiciaires. Pour autant, cette solution ne peut être que temporaire. Le Conseil rappelle, en effet, que l'existence et la persistance de cette menace liée à la sécurité nationale doivent faire l'objet d'un examen périodique sous le contrôle du juge administratif[28]. Si cette menace liée à la sécurité nationale disparaît, la conservation des données à ce titre et l'accès pour les enquêtes judiciaires disparaîtront.
En réalité, cette solution permet certainement de conserver, en partie, le régime actuel, pour avancer sur le projet de règlement E-evidence[29].

---

26. CJUE, 2 mars 2021, aff. C-746/18, Prokuratuur.

27. AUDIBERT, Matthieu. La conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ? [en ligne] *La veille juridique du Centre de recherche de l'École des officiers de la gendarmerie nationale*, mars 2021, p. 16-35. Disponible sur : https://www.gendarmerie.interieur.gouv.fr/crgn/publications/veille-juridique/mars-2021

28. Point 31.

29. CONSEIL EUROPÉEN, Un meilleur accès aux preuves électroniques pour lutter

Droit de l'espace numérique

À court terme, le Conseil d'État enjoint le Gouvernement à procéder à l'abrogation du dispositif réglementaire[30] de conservation des métadonnées dans un délai de six mois[31]. À moyen et long terme, des modifications substantielles de notre procédure pénale doivent également être envisagées.

Ces modifications concerneront vraisemblablement cinq articles du Code de procédure pénale.
S'agissant de l'accès aux métadonnées conservées au titre de la sécurité nationale, il faudra envisager de modifier les articles 60-1, 77-1-1 et 99-3 du Code de procédure.
Au titre du principe de proportionnalité[32], cette obligation de conservation n'est imposée aux opérateurs que « pour les besoins de la recherche, de la constatation et de la poursuite d'infractions pénales susceptibles de présenter un degré de gravité suffisant pour justifier l'ingérence dans les droits protégés » par la Charte des droits fondamentaux de l'Union. Le Conseil d'État précise que « seules de telles infractions [peuvent] légalement justifier l'accès des services d'enquêtes aux données conservées par les opérateurs[33] ». Or, les articles précités prévoient actuellement la

---

contre la criminalité [en ligne]. Dernière mise à jour le 20 octobre 2020. Disponible sur : https://www.consilium.europa.eu/fr/policies/e-evidence/

30. Article R. 10-13 du Code des postes et des communications électroniques. Décret n° 2011-219 du 25 février 2011 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.

31. Point 46.

32. Points 39 et 57.

33. *Ibid.*

possibilité pour les services d'enquêtes d'accéder à ces données pour l'ensemble des contraventions, délits et crimes.

Cette possibilité est en contradiction avec la position du Conseil d'État qui subordonne l'accès aux « données nécessaires à la poursuite et à la recherche des auteurs d'infractions pénales dont la gravité le justifie[34]».

Enfin, il sera certainement nécessaire de modifier l'article 60-2 du Code de procédure pénale pour actualiser la méthode dite de « conservation rapide » des données, laquelle n'est actuellement prévue que pour « le contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs[35] ».

Après le Conseil d'État, la position de la Chambre criminelle de la Cour de cassation, qui va certainement être amenée à se prononcer sur ces questions, devra être examinée avec la plus grande attention.

En effet, au regard de l'arrêt de la CJUE Prokuratuur du 2 mars 2021, quelle est l'autorité qui doit préalablement autoriser cet accès ? Au regard de son positionnement, quelle place pour le procureur de la République ? Le juge d'instruction peut-il voir ses pouvoirs d'enquête menacés ? Enfin, les juges des libertés et de la détention doivent-ils être cette autorité ?

34. Point 57.
35. Article 60-2 alinéa 2 du Code de procédure pénale.