ANALYSES ET DOSSIERS JURIDIQUES

French Data Network et autres

Chronologie, explication et méthode de commentaire de l’arrêt du 21 avril 2021

Florent HAAS | FH Droit

Dossier de septembre 2026

Révision éditoriale du 6 novembre 2026

Table des matières

1. L’objet du litige 2

2. Les acteurs et les requêtes 2

3. La chronologie de l’affaire 3

4. Le renvoi préjudiciel de 2018 4

5. La réponse de la Cour de justice en 2020 5

6. La méthode du Conseil d’État en 2021 5

7. L’application aux données de connexion 7

8. Le dispositif et ses effets 9

9. La portée jurisprudentielle 9

10. Une méthode de commentaire 10

L’arrêt d’Assemblée *French Data Network et autres* permet de comprendre comment le juge administratif articule le droit de l’Union européenne et les exigences constitutionnelles françaises. Le litige porte sur la conservation des données de connexion et leur utilisation par les services de renseignement. Son intérêt dépasse toutefois ce domaine : le Conseil d’État y précise une méthode de contrôle qui assure le plein effet du droit de l’Union tout en préservant, dans des conditions strictes, les garanties constitutionnelles[1].

Ce dossier suit le parcours de l’affaire : origine des recours, renvoi préjudiciel de 2018, réponse de la Cour de justice de l’Union européenne en 2020, raisonnement du Conseil d’État en 2021 et conséquences concrètes de sa décision. Il présente l’arrêt dans son contexte historique ; il ne prétend pas décrire l’ensemble du droit des données de connexion en vigueur aujourd’hui.

1. Conseil d’État, Assemblée, 21 avril 2021, *French Data Network et autres*, nos 393099, 394922, 397844, 397851, 424717 et 424718, publié au Recueil Lebon : décision intégrale ; analyse officielle.

1. L’objet du litige

Le droit français imposait aux opérateurs de communications électroniques, aux fournisseurs d’accès et aux hébergeurs de conserver pendant un an plusieurs catégories de données de connexion. Des associations, puis les sociétés Free et Free Mobile, soutenaient que cette conservation généralisée et indifférenciée méconnaissait le droit de l’Union.

Le litige concerne principalement les données qui retracent l’environnement technique d’une communication : identité, adresse IP, trafic, localisation, caractéristiques de connexion, compte et certains paiements. Il ne porte pas sur le contenu même des communications. Cette distinction ne diminue pas l’enjeu de protection : une agrégation de données techniques peut révéler de nombreux aspects de la vie privée[2].

Deux opérations doivent être distinguées. La **conservation** impose aux opérateurs de garder des données. L’**accès** permet ensuite aux autorités de les consulter ou de les exploiter. La légalité de la première ne suffit pas à établir celle du second : chaque opération doit répondre à ses propres conditions et garanties.

Le Conseil d’État doit ainsi articuler la protection de la vie privée et des données personnelles avec la sécurité nationale et la lutte contre la criminalité. Cette conciliation mobilise notamment l’article 15, paragraphe 1, de la directive du 12 juillet 2002 sur la vie privée et les communications électroniques, les articles 7, 8, 11 et 52 de la Charte des droits fondamentaux, l’article 4, paragraphe 2, du traité sur l’Union européenne et l’article 88-1 de la Constitution française[3].

2. Les acteurs et les requêtes

La décision du 21 avril 2021 joint six requêtes soulevant des questions communes. Certaines attaquent directement des décrets ; d’autres contestent le refus du Premier ministre d’abroger des dispositions réglementaires. Cette différence explique une partie du dispositif[4].

Requête	Requérants	Objet principal	Type de recours
393099	French Data Network, La Quadrature du Net et FFDN	Refus d’abroger l’article R. 10-13 du code des postes et des communications électroniques et le décret du 25 février 2011	Recours contre un refus implicite d’abrogation
394922	La Quadrature du Net, French Data Network et FFDN	Décret du 28 septembre 2015	Recours direct

2. Même décision, présentation des requêtes, point 1 et développements relatifs aux catégories de données : texte intégral.
3. Même décision, points 3 et suivants pour la hiérarchie des normes et cadre juridique européen : texte intégral. Les textes européens sont analysés à travers leur interprétation applicable au litige.
4. Même décision, procédure et points 1 et 2 : texte intégral. FFDN désigne la Fédération des fournisseurs d’accès à Internet associatifs.

Requête	Requérants	Objet principal	Type de recours
397844	Igwan.net	Décret du 11 décembre 2015	Recours direct
397851	La Quadrature du Net, French Data Network et FFDN	Décret du 29 janvier 2016	Recours direct
424717	Free Mobile	Refus d'abroger l'article R. 10-13 du même code	Recours contre un refus implicite d'abrogation
424718	Free	Refus d'abroger l'article R. 10-13 du même code	Recours contre un refus implicite d'abrogation

La requête n° 394925 figurait dans le renvoi préjudiciel du 26 juillet 2018. Elle n'est cependant pas tranchée par l'arrêt d'Assemblée du 21 avril 2021 : le Conseil d'État statue séparément sur cette branche du contentieux le 14 octobre 2021[5].

3. La chronologie de l'affaire

La succession des textes nationaux, des recours et des décisions européennes explique la durée de la procédure. Le renvoi à la Cour de justice constitue une étape du règlement du litige, après laquelle le Conseil d'État reprend l'examen des questions demeurées ouvertes[6].

Date	Étape
12 juillet 2002	Adoption de la directive 2002/58/CE sur la vie privée et les communications électroniques.
25 février 2011	Adoption du décret relatif aux données permettant d'identifier les auteurs de contenus en ligne. L'article R. 10-13 du code des postes et des communications électroniques impose parallèlement la conservation de données techniques.
24 juillet 2015	Adoption de la loi relative au renseignement, qui crée ou réorganise plusieurs techniques de recueil.
1er septembre 2015	Enregistrement de la requête n° 393099 contre le refus d'abroger les dispositions relatives à la conservation.
Septembre 2015 à janvier 2016	Adoption des décrets des 28 septembre, 1er octobre et 11 décembre 2015, puis du 29 janvier 2016, donnant lieu à plusieurs recours.
22 juillet 2016	Transmission au Conseil constitutionnel d'une question prioritaire de constitutionnalité sur l'article L. 811-5 du code de la sécurité intérieure.
21 octobre 2016	Déclaration d'inconstitutionnalité de cet article, avec effet différé[7].

5. Conseil d'État, 14 octobre 2021, n° 394925 : décision intégrale.
6. Pour les actes attaqués, les dates de saisine et le déroulement des renvois : Conseil d'État, 26 juillet 2018, n° 393099 et nos 394922 et autres ; décision d'Assemblée du 21 avril 2021, procédure et point 1.
7. Conseil constitutionnel, décision n° 2016-590 QPC du 21 octobre 2016 : décision intégrale.

Date	Étape
21 décembre 2016	Arrêt *Tele2 Sverige* de la Cour de justice sur la conservation généralisée et indifférenciée des données de trafic et de localisation[8].
26 juillet 2018	Renvois préjudiciels du Conseil d'État et sursis à statuer sur les questions européennes.
5 octobre 2018	Saisine du Conseil d'État par Free Mobile et Free.
6 octobre 2020	Arrêt de la Cour de justice *La Quadrature du Net et autres*, répondant aux questions françaises et belges.
16 avril 2021	Séance publique devant l'Assemblée du contentieux du Conseil d'État.
21 avril 2021	Décision *French Data Network et autres*.
30 juillet 2021	Adoption de la loi relative à la prévention d'actes de terrorisme et au renseignement, qui adapte notamment le cadre juridique[9].
14 octobre 2021	Décision distincte sur la requête n° 394925 relative au contentieux des techniques de renseignement.

4. Le renvoi préjudiciel de 2018

Le Conseil d'État est compétent pour trancher les recours nationaux. L'interprétation uniforme du droit de l'Union appartient toutefois à la Cour de justice. Les requérants invoquant la directive de 2002, la Charte des droits fondamentaux et la jurisprudence européenne, les difficultés d'interprétation conduisent le Conseil d'État à utiliser le renvoi préjudiciel prévu à l'article 267 du traité sur le fonctionnement de l'Union européenne[10].

Les questions portent principalement sur quatre sujets : la possibilité d'une conservation généralisée face à des menaces graves et persistantes pour la sécurité nationale ; le recueil en temps réel de données concernant certaines personnes ; l'information ultérieure des personnes surveillées lorsque celle-ci ne compromet plus les missions des autorités ; enfin, la conservation des données permettant d'identifier l'auteur d'un contenu en ligne.

Le renvoi organise une répartition des rôles. La Cour de justice précise le sens du droit européen ; le Conseil d'État applique ensuite cette interprétation au litige national. En 2018, le juge français ne se dessaisit donc pas définitivement de l'affaire : il suspend son jugement sur les questions européennes et conserve la responsabilité de la décision finale.

8. Cour de justice de l'Union européenne, grande chambre, 21 décembre 2016, *Tele2 Sverige*, affaires jointes C-203/15 et C-698/15 : arrêt intégral.
9. Loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement : texte officiel. Cette étape est postérieure à l'arrêt commenté.
10. Conseil d'État, 26 juillet 2018, *French Data Network et autres*, n° 393099, et *La Quadrature du Net et autres*, nos 394922 et autres, motifs et questions du dispositif.

5. La réponse de la Cour de justice en 2020

Dans l'arrêt *La Quadrature du Net et autres* du 6 octobre 2020, la Cour de justice maintient une exigence élevée de protection. La conservation générale et indifférenciée des données de trafic et de localisation constitue une ingérence particulièrement grave dans la vie privée et la protection des données. Elle ne peut devenir un instrument permanent disponible pour toute finalité de police ou de justice[11].

La sauvegarde de la sécurité nationale

La Cour admet une conservation généralisée et indifférenciée lorsque l'État fait face à une menace grave pour la sécurité nationale, réelle et actuelle ou prévisible. Cette possibilité demeure limitée au strict nécessaire. Elle doit être soumise à un contrôle effectif et à un réexamen de la persistance de la menace.

La lutte contre la criminalité grave

Pour la criminalité grave et la prévention des menaces graves contre la sécurité publique, la Cour distingue plusieurs instruments : conservation ciblée, conservation de certaines catégories de données dans les conditions qu'elle précise et conservation rapide de données déjà disponibles. Les adresses IP ne suivent pas exactement le même régime que l'ensemble des données de trafic et de localisation.

Les garanties d'accès aux données

Pour plusieurs formes d'accès ou de recueil, la Cour impose un contrôle préalable par une juridiction ou une autorité administrative indépendante disposant d'un pouvoir contraignant, sous réserve des urgences dûment justifiées. La seule présence d'un organe consultatif ne répond donc pas nécessairement à cette exigence.

La question soumise au Conseil d'État devient alors plus précise : l'application de ce cadre européen prive-t-elle certaines exigences constitutionnelles françaises de garanties effectives ? La réponse suppose une méthode, puis un examen concret de chaque régime.

6. La méthode du Conseil d'État en 2021

Le plein effet du droit de l'Union

Le Conseil d'État rappelle d'abord que le respect du droit de l'Union résulte des traités et de l'article 88-1 de la Constitution. Le juge national doit assurer sa primauté, son unité et son effectivité. Il laisse au besoin inappliquée une norme contraire, qu'il s'agisse notamment d'une loi ou d'un acte administratif[12].

11. Cour de justice de l'Union européenne, grande chambre, 6 octobre 2020, *La Quadrature du Net et autres*, affaires jointes C-511/18, C-512/18 et C-520/18 : dossier officiel de l'affaire et arrêt, spécialement dispositif sur la conservation, le recueil et les garanties de contrôle.
12. Conseil d'État, Assemblée, 21 avril 2021, précité, points 3 et 4 : décision intégrale.

La place de la Constitution dans l'ordre interne

L'intégration de l'ordre juridique de l'Union n'efface pas la place de la Constitution au sommet de l'ordre juridique interne. Cette affirmation s'inscrit dans le prolongement de l'arrêt *Sarran, Levacher et autres*, rendu le 30 octobre 1998. Le Conseil d'État y avait précisé que la supériorité des engagements internationaux *« ne s'applique pas, dans l'ordre interne, aux dispositions de nature constitutionnelle »*[13].

La recherche d'une interprétation compatible

Avant d'envisager un conflit, le juge administratif recherche une lecture de l'interprétation donnée par la Cour de justice qui soit compatible avec les exigences constitutionnelles. Cette démarche reste limitée par ce que les énonciations de l'arrêt européen permettent : elle n'autorise pas à réécrire sa portée[14].

La recherche d'une protection européenne équivalente

Le Conseil d'État reprend la méthode de l'arrêt *Société Arcelor Atlantique et Lorraine et autres*, rendu le 8 février 2007. Le juge recherche une règle européenne qui *« garantit par son application l'effectivité du respect de la disposition ou du principe constitutionnel invoqué »*. L'équivalence s'apprécie au regard de la nature et de la portée de la garantie, telles qu'elles sont interprétées par le juge de l'Union[15].

Dans la configuration *Arcelor*, le requérant invoque la Constitution contre un acte transposant directement une directive. Dans *French Data Network*, l'État invoque une exigence constitutionnelle pour défendre une norme nationale critiquée au regard du droit de l'Union. L'outil de comparaison est proche, mais la position procédurale de l'argument constitutionnel change.

Les conséquences de l'existence d'une protection équivalente

Lorsqu'une protection européenne équivalente existe, le contrôle se déploie sur le terrain du droit de l'Union. Dans le contrôle d'un acte de transposition, le juge examine la conformité de la directive au principe européen correspondant. Une difficulté sérieuse peut imposer un renvoi préjudiciel. Dans la configuration où l'État défend la norme nationale, l'existence d'une protection équivalente conduit à écarter son argument constitutionnel, avant de tirer les conséquences du moyen européen[16].

13. Conseil d'État, Assemblée, 30 octobre 1998, *Sarran, Levacher et autres*, nos 200286 et 200287 : décision intégrale, considérant relatif à l'article 55 de la Constitution. Le texte ne comporte pas de numérotation des considérants.
14. Conseil d'État, Assemblée, 21 avril 2021, précité, point 5 : décision intégrale.
15. Conseil d'État, Assemblée, 8 février 2007, *Société Arcelor Atlantique et Lorraine et autres*, n° 287110 : décision intégrale, considérant de principe relatif aux modalités du contrôle de constitutionnalité des actes de transposition. La citation reproduit un extrait de ce considérant non numéroté.
16. Conseil d'État, Assemblée, 21 avril 2021, précité, points 6 et 7 : décision intégrale.

Les conséquences de l'absence d'équivalence

L'absence de protection équivalente ne suffit pas à neutraliser le droit de l'Union. Le juge doit encore vérifier si l'éviction de la règle nationale priverait effectivement de garanties l'exigence constitutionnelle invoquée. Le point 5 indique alors que *« le juge administratif, saisi d'un moyen en ce sens, doit l'écarter dans la stricte mesure où le respect de la Constitution l'exige »*. La sauvegarde constitutionnelle dépend ainsi d'une privation établie de garanties et reste limitée à ce que leur préservation impose[17].

La méthode comporte donc deux filtres successifs : une comparaison des protections, puis un examen concret de la perte de garanties. Les confondre conduirait à transformer une réserve subsidiaire en dérogation générale.

Le refus du contrôle de la compétence de la Cour de justice

Le Premier ministre invitait le Conseil d'État à vérifier si la Cour de justice avait dépassé les compétences attribuées à l'Union. Le Conseil d'État refuse cette voie. Il ne se reconnaît pas le pouvoir de contrôler les décisions de la Cour ni de leur retirer leur force obligatoire pour un dépassement allégué de compétence. C'est le refus du contrôle dit *ultra vires*[18].

Question	Conséquence dans le raisonnement
La norme nationale est-elle contraire au droit de l'Union ?	Le juge examine le moyen européen, après un éventuel renvoi préjudiciel.
L'État invoque-t-il une exigence constitutionnelle avec les précisions nécessaires ?	Le juge recherche une protection européenne équivalente.
Une protection équivalente existe-t-elle ?	L'argument constitutionnel en défense ne permet pas de faire obstacle à l'application du droit de l'Union.
À défaut, l'éviction de la norme nationale priverait-elle l'exigence constitutionnelle de garanties effectives ?	Le juge peut écarter le moyen européen dans la seule mesure nécessaire à la sauvegarde de cette exigence.

7. L'application aux données de connexion

L'État invoque la sauvegarde des intérêts fondamentaux de la Nation, la prévention des atteintes à l'ordre public, la lutte contre le terrorisme et la recherche des auteurs d'infractions. Le Conseil d'État relève l'absence de protection européenne équivalente pour les exigences en cause. Il ne s'arrête cependant pas à ce constat : il examine ensuite si l'application du droit de l'Union les priverait concrètement de garanties[19].

17. Même décision, points 5 à 7 ; extrait cité au point 5 : texte intégral.
18. Même décision, point 8 : texte intégral.
19. Même décision, points 9 et 10 : texte intégral.

La conservation pour la sécurité nationale

À la date de sa décision, le Conseil d'État constate une menace grave et réelle pour la sécurité nationale. Il admet donc la conservation généralisée des données de trafic et de localisation pour cette finalité, dans le cadre tracé par la Cour de justice. En revanche, le droit français doit prévoir un réexamen périodique de la persistance de la menace[20].

La conservation pour la criminalité et l'ordre public

Le régime national ne peut imposer la conservation généralisée et indifférenciée des données de trafic et de localisation pour l'ensemble des finalités de recherche et de poursuite des infractions. Le raisonnement du Conseil d'État est cependant plus précis qu'un simple renvoi vers des solutions moins intrusives. Il relève les limites opérationnelles de la conservation ciblée et constate que les mécanismes alternatifs, pris isolément, ne suffisent pas à garantir les objectifs constitutionnels.

La combinaison des dispositifs lui permet de conclure autrement : à la date de l'arrêt, la menace justifie une conservation générale pour la sécurité nationale ; les données ainsi conservées peuvent ensuite faire l'objet d'une conservation rapide pour des infractions dont la gravité le justifie. Dans ces conditions, l'application du droit de l'Union ne prive pas les exigences constitutionnelles de garanties effectives. La solution reste liée à cette articulation et à l'état de la menace[21].

La distinction des catégories de données

L'intensité de l'ingérence dépend aussi des données concernées. L'identité civile, les coordonnées de contact et de paiement, les données relatives aux comptes et aux contrats ainsi que les adresses IP font l'objet de distinctions. Leur régime ne peut être déduit sans nuance de celui des données de trafic et de localisation, particulièrement révélatrices de la vie privée[22].

Le contrôle préalable du renseignement

Le Conseil d'État applique l'exigence européenne de contrôle préalable. L'avis de la Commission nationale de contrôle des techniques de renseignement n'était pas juridiquement contraignant. Pour les techniques visées, l'absence de contrôle préalable par une juridiction ou une autorité administrative indépendante dotée d'un pouvoir contraignant méconnaît donc le droit de l'Union, hors urgence dûment justifiée[23].

La Constitution ne permet ainsi pas de maintenir l'ensemble de la réglementation nationale. Le Conseil d'État applique les exigences européennes et censure plusieurs insuffisances. La réserve constitutionnelle demeure une garantie ultime, soumise à un examen concret.

20. Même décision, notamment point 44 et article 1er du dispositif : texte intégral.
21. Même décision, points 51 à 58, spécialement points 57 et 58, sur la combinaison des dispositifs et la situation à la date de l'arrêt : texte intégral.
22. Même décision, points 33 à 41, consacrés aux données d'identité, aux comptes, aux paiements et aux adresses IP : texte intégral.
23. Même décision, notamment points 74, 77, 80, 83 et 97 : texte intégral.

8. Le dispositif et ses effets

La décision combine des annulations partielles, une injonction et des rejets. Cette combinaison reflète la diversité des actes attaqués et des illégalités constatées[24].

Objet	Solution	Effet
Refus d'abroger l'article R. 10-13 et le décret du 25 février 2011	Annulation partielle concernant les finalités de conservation généralisée des données de trafic et de localisation et l'absence de réexamen périodique de la menace	Injonction au Premier ministre de procéder à l'abrogation nécessaire dans les six mois
Décrets des 11 décembre 2015 et 29 janvier 2016	Annulation partielle en tant qu'ils permettent certaines techniques sans contrôle préalable contraignant, hors urgence dûment justifiée	Mise en conformité avec l'exigence européenne de contrôle préalable
Requête n° 394922 contre le décret du 28 septembre 2015	Rejet	Maintien du décret sur les moyens restant en discussion
Autres conclusions	Rejet pour le surplus	Absence d'annulation générale du dispositif français

9. La portée jurisprudentielle

Trois décisions permettent de situer l'apport de *French Data Network*. Leur rapprochement montre une continuité dans la place de la Constitution et une évolution dans la méthode de traitement du conflit normatif[25].

Décision	Question	Méthode ou solution
Sarran, 30 octobre 1998	Un engagement international peut-il prévaloir sur la Constitution dans l'ordre interne ?	La supériorité reconnue aux engagements internationaux ne s'étend pas aux dispositions constitutionnelles.
Arcelor, 8 février 2007	Comment contrôler la constitutionnalité d'un acte transposant directement une directive ?	Recherche d'une protection équivalente en droit de l'Union ; contrôle européen si elle existe, contrôle constitutionnel direct sinon.
French Data Network, 21 avril 2021	Comment traiter une exigence constitutionnelle invoquée en défense contre l'éviction d'une règle nationale contraire au droit de l'Union ?	Recherche d'équivalence, puis examen concret d'une éventuelle privation de garanties ; refus du contrôle *ultra vires* de la Cour de justice.

24. Même décision, dispositif : texte intégral.
25. Les trois décisions sont accessibles dans leurs versions officielles : *Sarran*, 1998, *Arcelor*, 2007 et *French Data Network*, 2021, points 4 à 8. Le tableau expose le rapprochement pédagogique proposé par le présent dossier.

L'apport propre de l'arrêt est la formulation de l'office du juge lorsque l'argument constitutionnel est présenté pour défendre la norme nationale. Le raisonnement d'équivalence dépasse ainsi la seule configuration de l'acte de transposition examinée dans *Arcelor*.

La portée de cette extension dépend de ses limites. Le juge ne dispose ni d'une autorisation générale d'écarter le droit de l'Union, ni d'un pouvoir de révision des décisions de la Cour de justice. L'affaire reste concrète : la réserve constitutionnelle est examinée à partir des garanties effectivement offertes par les mécanismes disponibles, tandis que plusieurs dispositions nationales sont censurées.

10. Une méthode de commentaire

Une problématique possible consiste à demander dans quelle mesure *French Data Network* renouvelle l'office du juge administratif pour concilier le plein effet du droit de l'Union avec la garantie effective des exigences constitutionnelles.

Le plan suivant permet de relier la méthode et son application :

I. La conciliation de la primauté du droit de l'Union avec la suprématie interne de la Constitution

- **A.** La pleine effectivité du droit de l'Union dans l'ordre interne.
- **B.** La sauvegarde subsidiaire des exigences constitutionnelles dépourvues de protection européenne équivalente.

II. L'approfondissement de l'office du juge administratif

- **A.** L'extension de l'équivalence des protections à la défense de la norme nationale.
- **B.** La mise en œuvre concrète de la conciliation en matière de données de connexion.

Le commentaire doit expliquer les conditions de la réserve constitutionnelle avant d'en discuter la portée. Il gagne aussi à distinguer les configurations *Arcelor* et *French Data Network*, à traiter expressément le refus du contrôle *ultra vires* et à examiner les annulations prononcées. Sans cette dernière étape, la présentation risquerait de réduire l'arrêt à une opposition abstraite entre deux normes suprêmes.

Le fil conducteur est donc un enchaînement : assurer le plein effet du droit de l'Union ; rechercher une protection européenne équivalente ; en l'absence d'équivalence, vérifier une éventuelle privation effective de garanties constitutionnelles. L'application de cette méthode explique à la fois la reconnaissance des impératifs de sécurité et les corrections imposées au droit français.