CONSEIL D'ÉTAT

Paris, le 21 avril 2021

COMMUNIQUÉ DE PRESSE

Données de connexion : le Conseil d'État concilie le respect du droit de l'Union européenne et l'efficacité de la lutte contre le terrorisme et la criminalité

Saisi par plusieurs associations ainsi qu'un opérateur de télécoms, le Conseil d'État a examiné la conformité des règles françaises de conservation des données de connexion au droit européen. Il a aussi été amené à vérifier que le respect du droit européen tel qu'interprété par la CJUE ne compromettait pas les exigences de la Constitution française. Il juge que la conservation généralisée des données est aujourd'hui justifiée par la menace existante pour la sécurité nationale. Il relève également que la possibilité d'accéder à ces données pour la lutte contre la criminalité grave permet, à ce jour, de garantir les exigences constitutionnelles de prévention des atteintes à l'ordre public et de recherche des auteurs d'infractions pénales.
En revanche, il ordonne au Gouvernement de réévaluer régulièrement la menace qui pèse sur le territoire pour justifier la conservation généralisée des données et de subordonner l'exploitation de ces données par les services de renseignement à l'autorisation d'une autorité indépendante.

Le droit français impose aux opérateurs de télécommunication de conserver les données de connexion de leurs utilisateurs à des fins de lutte contre la criminalité et le terrorisme

L'exploitation des données de connexion joue aujourd'hui un rôle majeur dans la recherche des infractions pénales et dans l'activité des services de renseignement, notamment pour lutter contre le terrorisme.
Ces données, parfois appelées « métadonnées » pour les distinguer de celles qui portent sur le contenu des échanges, comprennent trois catégories :

- les données d'identité, qui permettent d'identifier l'utilisateur d'un moyen de communication électronique (par exemple les nom et prénom liés à un numéro de téléphone ou l'adresse IP par laquelle un utilisateur se connecte à internet) ;
- les données relatives au trafic, parfois appelées « fadettes », qui tracent les dates, heures et destinataires des communications électroniques, ou la liste des sites internet consultés ;
- les données de localisation, qui résultent du « bornage » d'un appareil par l'antenne relais à laquelle il s'est connecté.

Le droit français impose aux opérateurs de télécommunication de conserver pendant un an toutes les données de connexion des utilisateurs pour les besoins du renseignement et des enquêtes pénales.

La CJUE a fortement limité la possibilité d'imposer aux opérateurs la conservation des données de connexion

Plusieurs associations actives dans le domaine de la protection des données personnelles ainsi qu'un opérateur de télécoms ont saisi le Conseil d'État de recours contre les décrets qui prévoient la conservation de ces données et qui organisent leur traitement pour les besoins du renseignement et des enquêtes pénales.

À cette occasion, le Conseil d'État a saisi, en 2018[1], la Cour de justice de l'Union européenne (CJUE) pour l'inviter à préciser la portée des règles issues du droit européen (directive 2002/58, dite « vie privée et communications électroniques » et règlement général sur la protection des données - RGPD). Plusieurs juridictions d'autres États membres de l'Union ont, elles aussi, saisi la CJUE dans le même but. Par trois décisions rendues le 6 octobre 2020[2], la CJUE a détaillé les limites posées à ses yeux par le droit européen.

1) La conservation généralisée et indifférenciée des données de connexion (autres que les données d'identité) ne peut être imposée aux opérateurs que pour les besoins de la sécurité nationale en cas de menace grave. En outre, l'accès à ces données par les services de renseignement doit être soumis au contrôle préalable d'une autorité indépendante et au contrôle d'un juge en aval lors de l'exploitation des données conservées.

2) Pour la lutte contre la criminalité grave, les États peuvent seulement imposer la conservation ciblée de données, dans certaines zones ou pour certaines catégories de personnes pré-identifiées comme présentant des risques particuliers. Mais, comme le prévoit la convention de Budapest de 2001, les autorités peuvent demander aux opérateurs de geler les données de trafic et de localisation relatives à une personne, pour les besoins d'une enquête pénale, sur une courte période (méthode dite de « conservation rapide » des données).

3) La conservation des données de connexion n'est pas permise pour d'autres motifs, notamment pour la recherche des infractions ne relevant pas de la criminalité grave.

Le Conseil d'État vérifie que l'application du droit européen ne compromet pas les exigences de la Constitution française

À la suite des précisions apportées par la CJUE, le Conseil d'État, statuant en Assemblée du contentieux – sa formation la plus solennelle –, devait examiner la conformité du cadre juridique français au droit européen.

---

[1] CE, 26 juillet 2018, Quadrature du Net et autres et Igwan.net, n°s 394922 394925 397844 397851, T.

[2] CJUE, 6 octobre 2020, *Privacy International*, aff. C-623/17 ; *La Quadrature du Net e.a., French Data Network e.a.*, aff. C-511/18 et C-512/18 ; *Ordre des barreaux francophones et germanophone e.a.*, aff. C-520/18.

Il a, tout d'abord, précisé le cadre de son contrôle.

D'une part, et contrairement à ce que lui demandait le Gouvernement, il refuse de contrôler que les organes de l'Union européenne, et notamment la CJUE, n'ont pas excédé leurs compétences (contrôle dit de l'« *ultra vires* »).

D'autre part, le Conseil d'État rappelle que la Constitution française demeure la norme suprême du droit national.

En conséquence, il lui revient de vérifier que l'application du droit européen, tel que précisé par la CJUE, ne compromet pas en pratique des exigences constitutionnelles qui ne sont pas garanties de façon équivalente par le droit européen.

L'encadrement de la conservation des données par le droit européen ne remet pas en cause les exigences constitutionnelles relatives à la sécurité nationale et à la lutte contre la criminalité

Le Conseil d'État constate que les exigences constitutionnelles que sont 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 pénales ne bénéficient pas, en droit de l'Union, d'une protection équivalente à celle que garantit la Constitution. Il doit donc s'assurer que les limites définies par la CJUE ne mettent pas en péril ces exigences constitutionnelles.

Le Conseil d'État relève que la conservation généralisée 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. Conformément aux exigences de la Cour, il impose au Gouvernement de procéder, sous le contrôle du juge administratif, à un réexamen périodique de l'existence d'une telle menace.

En revanche, il juge illégale l'obligation de conservation généralisée des données (hormis les données peu sensibles : état civil, adresse IP, comptes et paiements) pour les besoins autres que ceux de la sécurité nationale, notamment la poursuite des infractions pénales.

Pour ces infractions, la solution suggérée par la CJUE de conservation ciblée en amont des données n'est ni matériellement possible, ni – en tout état de cause – opérationnellement efficace. En effet, il n'est pas possible de pré-déterminer les personnes qui seront impliquées dans une infraction pénale qui n'a pas encore été commise ou le lieu où elle sera commise. Toutefois, la méthode de « conservation rapide » autorisée par le droit européen peut à ce jour s'appuyer sur le stock de données conservées de façon généralisée pour les besoins de la sécurité nationale, et peut être utilisée pour la poursuite des infractions pénales.

S’agissant de la distinction établie par la Cour entre la criminalité grave et la criminalité ordinaire, pour laquelle elle n’admet aucune conservation ou utilisation de données de connexion, le Conseil d’État rappelle que le principe de proportionnalité entre gravité de l’infraction et importance des mesures d’enquête mises en œuvre, qui gouverne la procédure pénale, justifie également que le recours aux données de connexion soit limité aux poursuites d’infractions d’un degré de gravité suffisant.

S’agissant de l’exploitation des données conservées pour les besoins du renseignement, enfin, le Conseil d’État constate que le contrôle préalable par une autorité indépendante prévu par le cadre juridique français n’est pas suffisant, puisque l’avis que rend la commission nationale de contrôle des techniques de renseignement (CNCTR) avant toute autorisation n’est pas contraignant. Le droit national doit donc être modifié, même si, en pratique, le Premier ministre n’a jamais outrepassé un avis défavorable de la CNCTR pour l’accès des services de renseignement à des données de connexion.
Le Conseil d’État ordonne au Premier ministre de modifier le cadre réglementaire pour respecter ces exigences dans un délai de 6 mois.