



## COMMUNIQUE DE PRESSE n° 156/22

Luxembourg, le 20 septembre 2022

Arrêt de la Cour dans les affaires jointes C-793/19 | SpaceNet et C-794/19 | Telekom Deutschland

### **La Cour de justice confirme que le droit de l'Union s'oppose à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, sauf en cas de menace grave pour la sécurité nationale**

*Pour lutter contre la criminalité grave, les États membres peuvent toutefois, dans le strict respect du principe de proportionnalité, prévoir notamment une conservation ciblée et/ou rapide de telles données ainsi qu'une conservation généralisée et indifférenciée des adresses IP*

SpaceNet et Telekom Deutschland fournissent, en Allemagne, des services d'accès à Internet accessibles au public, Telekom Deutschland fournissant, en outre, des services téléphoniques. Elles ont contesté devant les juridictions allemandes l'obligation qui leur est imposée par la loi allemande sur les télécommunications (TKG) de conserver, à compter du 1<sup>er</sup> juillet 2017, des données relatives au trafic et des données de localisation afférentes aux télécommunications de leurs clients.

Hormis certaines exceptions, la TKG impose aux fournisseurs de services de communications électroniques accessibles au public, notamment aux fins de la répression des infractions pénales graves ou de la prévention d'un risque concret pour la sécurité nationale, la conservation généralisée et indifférenciée, pour une durée de plusieurs semaines, de l'essentiel des données relatives au trafic et des données de localisation des utilisateurs finals.

La Cour administrative fédérale allemande souhaite savoir si le droit de l'Union, tel qu'interprété par la Cour de justice <sup>1</sup>, s'oppose à une telle législation nationale.

Ses doutes naissent notamment du fait que l'obligation de conservation prévue par la TKG concernerait un nombre de données moindre et une durée de conservation plus courte (4 ou 10 semaines) que ce que prévoyaient les réglementations nationales en cause dans les affaires ayant conduit aux arrêts précédents. Ces particularités réduiraient la possibilité que les données conservées puissent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées. De plus, la TKG assurerait une protection efficace des données conservées contre les risques d'abus et d'accès illicite.

**Par son arrêt de ce jour, la Cour de justice confirme sa jurisprudence antérieure.**

Elle répond à la Cour administrative fédérale allemande que **le droit de l'Union s'oppose à une législation nationale prévoyant, à titre préventif, aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des données**

<sup>1</sup> Voir notamment arrêts du 5 avril 2022, Commissioner of An Garda Síochána e.a., [C-140/20](#) (voir aussi le CP n° 58/22), ainsi que du 6 octobre 2020, La Quadrature du Net e.a., [C-511/18](#), [C-512/18](#) et [C-520/18](#) (voir aussi le CP n° 123/20).

**relatives au trafic et des données de localisation.**

**En revanche, le droit de l'Union ne s'oppose pas à** une législation nationale

- permettant, aux fins de la sauvegarde de la sécurité *nationale*, d'enjoindre aux fournisseurs de services de communications électroniques de procéder **à une conservation généralisée et indifférenciée** des données relatives au trafic et des données de localisation, **dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale** qui s'avère réelle et actuelle ou prévisible. Une telle injonction peut être contrôlée soit par une juridiction, soit par une entité administrative indépendante et ne peut être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;
- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité *grave* et de la prévention des menaces *graves* contre la sécurité publique, **une conservation ciblée** des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;
- prévoyant, aux mêmes fins, **une conservation généralisée et indifférenciée des adresses IP** attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;
- prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, **une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs** de moyens de communications électroniques, et
- permettant, aux fins de la lutte contre la criminalité *grave* et, a fortiori, de la sauvegarde de la sécurité nationale, d'enjoindre les fournisseurs de services de communications électroniques, de procéder, pour une durée déterminée, **à la conservation rapide** des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services.

Une telle législation nationale doit, par ailleurs, assurer, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

**En ce qui concerne la TKG**, la Cour constate qu'il ressort de la décision de renvoi que l'obligation de conservation que cette loi édicte porte, notamment, sur les données nécessaires pour identifier la source d'une communication et la destination de celle-ci, la date et l'heure du début et de la fin de la communication ou, en cas de communication par SMS, message multimédia ou message similaire, le moment de l'envoi et de la réception du message ainsi que, en cas d'utilisation mobile, la désignation des cellules qui ont été utilisées par l'appelant et l'appelé au début de la communication.

Dans le cadre de la fourniture de services d'accès à Internet, l'obligation de conservation porte, notamment, sur l'adresse IP attribuée à l'abonné, la date et l'heure du début et de la fin de l'utilisation d'Internet à partir de l'adresse IP attribuée et, en cas d'utilisation mobile, la désignation des cellules utilisées au début de la connexion Internet. Les données permettant de connaître la position géographique et les directions du rayonnement maximal des antennes desservant la cellule concernée sont également conservées.

S'il est vrai que les données afférentes aux services de courrier électronique ne sont pas couvertes par l'obligation de conservation prévue par la TKG, elles ne représentent qu'une infime partie des données en cause. Sont d'ailleurs conservées, notamment, les données d'utilisateurs soumis au secret professionnel, tels que les avocats, les médecins et les journalistes.

**Ainsi, l'obligation de conservation prévue par la TKG s'étend à un ensemble très large de données relatives au trafic et de données de localisation, qui correspond, en substance, à ceux ayant conduit aux arrêts**

antérieurs précités.

**Or, cet ensemble de données relatives au trafic et de données de localisation** conservées pendant, respectivement, 10 et 4 semaines, **peut permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données sont 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, et, en particulier, d'établir un profil desdites personnes.**

En ce qui concerne les garanties prévues par la TKG, visant à protéger les données conservées contre les risques d'abus et contre tout accès illicite, la Cour relève que la conservation de ces données et l'accès à celles-ci constituent des ingérences distinctes dans les droits fondamentaux des personnes concernées, nécessitant une justification distincte. Il en découle qu'une législation nationale assurant le plein respect des conditions résultant de la jurisprudence en matière d'accès aux données conservées ne saurait, par nature, être susceptible ni de limiter ni même de remédier à l'ingérence grave dans les droits des personnes concernées qui résulterait de la conservation généralisée de ces données.

**RAPPEL :** Le renvoi préjudiciel permet aux juridictions des États membres, dans le cadre d'un litige dont elles sont saisies, d'interroger la Cour sur l'interprétation du droit de l'Union ou sur la validité d'un acte de l'Union. La Cour ne tranche pas le litige national. Il appartient à la juridiction nationale de résoudre l'affaire conformément à la décision de la Cour. Cette décision lie, de la même manière, les autres juridictions nationales qui seraient saisies d'un problème similaire.

Document non officiel à l'usage des médias, qui n'engage pas la Cour de justice.

Le [texte intégral](#) et le [résumé](#) de l'arrêt sont publiés sur le site CURIA le jour du prononcé.

Contact presse : Amanda Nouvel ☎ (+352) 4303 2524.

Des images du prononcé de l'arrêt sont disponibles sur « [Europe by Satellite](#) » ☎ (+32) 2 2964106.

Restez connectés !

