COUR DE CASSATION, CHAMBRE CRIMINELLE, 12 JUILLET 2022, POURVOI N° 21-83.820

MOTS CLEFS : données de connexion — données de trafic — données de localisation — conservation des données de connexion — exploitation des données de connexion

Dès lors que les données relatives au trafic et les données de localisation « peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées », la Cour de justice de l'Union européenne (CJUE) s'attache particulièrement à borner les conditions dans lesquelles la conservation des données de connexion et l'accès à ces dernières peuvent être effectués. Elle s'est plus spécifiquement intéressée à la conservation et à l'accès des données de connexion dans le cadre de procédures pénales. Par les quatre arrêts rendus le 12 juillet 2022, la chambre criminelle de la Cour de cassation réceptionne les décisions rendues par la CJUE dans ce cadre précis.

FAITS : En l'espèce, plusieurs dizaines de kilogrammes de cocaïne ont été découvertes à la suite de l'interception d'une embarcation dans les eaux territoriales au large de la Martinique. Dans le cadre de cette affaire, un homme est mis en examen des chefs d'importation et exportation de stupéfiants en bande organisée, infractions à la législation sur les stupéfiants et associations de malfaiteurs. Contestant la manière dont ses données ont été utilisées contre lui par les enquêteurs, il dépose une requête en nullité visant les réquisitions des enquêteurs portant sur les données de trafic et de localisation ainsi que les actes d'exploitation de ces données.

PROCÉDURE : Par un arrêt de la cour d'appel de Fort-de-France du 8 juin 2021, le requérant voit sa demande d'annulation rejetée et se pourvoit en cassation. Selon lui, ces données avaient fait l'objet d'une conservation irrégulière en ce que la législation française imposait aux opérateurs de conserver pendant un an les données de connexion pour la recherche d'infractions pénales, ce qui était contraire au droit de l'Union européenne ; d'un accès irrégulier en ce que les données auraient du être récupérées à la suite d'une autorisation d'une juridiction ou entité administrative indépendante et non pas à la suite d'une autorisation du juge d'instruction.

PROBLÈMES DE DROIT : Dans le cadre de procédures impliquant une personne mise en examen pour trafic de stupéfiants, il est question de savoir si, d'une part, la conservation indifférenciée et généralisée des données de connexion peut être imposée et si, d'autre part, le juge d'instruction est compétent pour y autoriser l'accès.

SOLUTION : La Cour de cassation rejette le pourvoi car estime que la conservation des données trafic et de localisation ainsi que l'accès à celles-ci ont été régulièrement effectués. D'une part, la Cour énonce que la conservation généralisée et indifférenciée des données de connexion peut être imposée s'il existe une menace grave à la sécurité nationale. D'autre part, elle précise que le juge d'instruction est habilité à contrôler l'accès aux données de connexion.

SOURCES : Cour de cassation, *Note explicative relative aux arrêts de la chambre criminelle du 12 juillet 2022 (pourvois n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652)*

Cour de cassation, *Enquêtes pénales : conservation et accès aux données de connexion*

CJUE, 6 octobre 2020, aff. C- 511/18 et C- 512/18, aff. C- 520/18

NOTE :

L'Union européenne proscrit la conservation généralisée et indifférenciée des données de connexion, même lorsqu'il s'agit des données de trafic et de localisation aux fins de lutte contre la criminalité (CJUE, 6 octobre 2020), mais admet toutefois certaines exceptions. En vertu du principe de primauté du droit de l'Union, les juridictions nationales sont tenues d'interpréter la législation nationale à la lumière de la législation européenne. En l'espèce, la chambre criminelle de la Cour de cassation a dû se prononcer sur la conformité du droit interne au droit de l'Union sur la question de la conservation des données de trafic et de localisation et de l'accès à celles-ci.

Une conservation généralisée et indifférenciée des données de connexion peut être justifiée par une menace grave à la sécurité nationale. La Cour de cassation énonce que la conservation généralisée et indifférenciée des données de trafic et de localisation est possible lorsqu'il est question de la sauvegarde de la sécurité nationale. Encore faut-il caractériser une menace grave à la sécurité nationale, ce que la chambre criminelle ne manque pas de faire : les pièces relatives aux attentats commis en France depuis 1994 révèlent en effet une menace grave à la sécurité nationale antérieurement aux faits de cette affaire.

Une conservation « rapide » des données de connexion peut être envisagée lorsqu'il est question de la sauvegarde de la sécurité nationale, dans le respect de certaines conditions. La Cour énonce que les dispositions permettant d'ordonner la conservation « rapide » des données de connexion, dans le but d'élucider une infraction déterminée relevant de la criminalité grave, sont conformes au droit de l'Union lorsqu'il est question de la sauvegarde de la sécurité nationale. En l'espèce, les enquêteurs ont demandé par voie de réquisitions la conservation des données de trafic et de localisation dans un objectif de sauvegarde de la sécurité nationale, ce qui caractérise une injonction de conservation « rapide ».
Le juge est alors tenu, d'une part, de regarder si l'infraction en cause relève bien de la criminalité grave et, d'autre part, si la conservation est opérée de manière strictement nécessaire. En l'espèce, le juge a estimé que le trafic de cocaïne en bande organisée rentre dans le champ de la criminalité grave et que les investigations consistant à exploiter les données de trafic et de localisation étaient nécessaires à la poursuite de cette infraction pénale.

La compétence du juge d'instruction pour autoriser l'accès aux données de connexion est validée par la Cour. Le droit de l'Union impose un contrôle préalable par une juridiction ou une entité administrative indépendante. Dans le cas d'espèce, la Cour n'a pas remis en question la compétence du juge d'instruction pour autoriser l'accès aux données de connexion. En l'espèce, l'accès aux données de l'homme mis en examen a donc été régulièrement effectué puisque les enquêteurs ont agi sur commission rogatoire du juge d'instruction.

Seule la personne victime d'un accès irrégulier à ses données de connexion peut invoquer un grief. La Cour prévoit deux conditions : soit la personne est titulaire ou utilisateur d'une des lignes identifiées, soit elle établit une atteinte à sa vie privée. En l'espèce, l'homme mis en examen ne peut pas solliciter la nullité des réquisitions au titre de l'atteinte à sa vie privée dans la mesure où l'ingérence dans sa vie privée était

proportionnée à la poursuite de l'infraction pénale dans laquelle il était mis en cause.
Par ailleurs, même si l'homme mis en examen avait bien un droit sur les lignes téléphoniques, il s'avère que ses données de connexion ont été régulièrement conservées et que l'accès à celles-ci a été autorisé par une juridiction indépendante.

Maud PRÉCHACQ
Master 2 Droit des médias électroniques
AIX-MARSEILLE UNIVERSITÉ, IREDIC 2022

ARRÊT (Cour de cassation, Chambre criminelle, 12 juillet 2022, pourvoi n° 21-83.820) :

8. L'article L. 34-1, III, du code des postes et des communications électroniques, dans sa version issue de la loi n° 2013-1168 du 18 décembre 2013, mis en oeuvre par l'article R. 10-13 dudit code, tel qu'il résultait du décret n° 2012-436 du 30 mars 2012, est contraire au droit de l'Union européenne en ce qu'il imposait aux opérateurs de services de télécommunications électroniques, aux fins de lutte contre la criminalité, la conservation généralisée et indifférenciée des données de connexion, à l'exception des données relatives à l'identité civile, aux informations relatives aux comptes et aux paiements, ainsi qu'en matière de criminalité grave, de celles relatives aux adresses IP attribuées à la source d'une connexion.

9. En revanche, la France se trouvant exposée, depuis décembre 1994, à une menace grave et réelle, actuelle ou prévisible à la sécurité nationale, les textes précités de droit interne étaient conformes au droit de l'Union en ce qu'ils imposaient aux opérateurs de services de télécommunications électroniques de conserver de façon généralisée et indifférenciée les données de trafic et de localisation, aux fins de la recherche, de la constatation et de la poursuite des infractions portant atteinte aux intérêts fondamentaux de la Nation et des actes de terrorisme, incriminés aux articles 410-1 à 422-7 du code pénal.

10. Les articles 60-1 et 60-2, 77-1-1 et 77-1-2, 99-3 et 99-4 du code de procédure pénale, dans leur version antérieure à la loi n° 2022-299 du 2 mars 2022, lus en combinaison avec le sixième alinéa du paragraphe III de l'article préliminaire du code de procédure pénale, permettaient aux autorités compétentes, de façon conforme au droit de l'Union, pour la lutte contre la criminalité grave, en vue de l'élucidation d'une infraction déterminée, d'ordonner la conservation rapide, au sens de l'article 16 de la Convention du Conseil de l'Europe sur la cybercriminalité du 23 novembre 2001, des données de connexion, même conservées aux fins de sauvegarde de la sécurité nationale.

11. Il appartient à la juridiction, lorsqu'elle est saisie d'un moyen en ce sens, de vérifier, d'une part, que les éléments de fait justifiant la nécessité d'une telle mesure d'investigation répondent à un critère de criminalité grave, dont l'appréciation relève du droit national, d'autre part, que la conservation rapide des données de trafic et de localisation et l'accès à celles-ci respectent les limites du strict nécessaire.

12. S'agissant de la gravité des faits, il appartient au juge de motiver sa décision au regard de la nature des agissements de la personne poursuivie, de l'importance du dommage qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue.

13. Les articles 60-1 et 60-2, 77-1-1 et 77-1-2 du code de procédure pénale sont contraires au droit de l'Union uniquement en ce qu'ils ne prévoient pas préalablement à l'accès aux données un contrôle par une juridiction ou une entité administrative indépendante. En revanche, le juge d'instruction est habilité à contrôler l'accès aux données de connexion.

14. Une personne mise en examen n'est recevable à invoquer la violation de l'exigence précitée que si elle prétend être titulaire ou utilisatrice de l'une des lignes identifiées ou si elle établit qu'il aurait été porté atteinte à sa vie privée, à l'occasion des investigations litigieuses.

15. L'existence d'un grief pris de l'absence

d'un tel contrôle est établie si l'accès aux données de trafic et de localisation a méconnu les conditions matérielles posées par le droit de l'Union. Tel est le cas si l'accès a porté sur des données irrégulièrement conservées, s'il a eu lieu, hors hypothèse de la conservation rapide, pour une finalité moins grave que celle ayant justifié la conservation, n'a pas été circonscrit à une procédure visant à lutter contre la criminalité grave et a excédé les limites du strict nécessaire.

16. En l'espèce, M. [U] ne justifie ni même n'allègue qu'il aurait été porté atteinte à sa vie privée par les réquisitions délivrées aux opérateurs durant l'enquête ou sur commission rogatoire et tendant à obtenir les facturations détaillées et les géolocalisations des lignes téléphoniques dont il n'était ni titulaire ni utilisateur. Il n'a dès lors pas qualité pour en solliciter la nullité.

17. En revanche, il est recevable à solliciter la nullité des réquisitions portant sur les lignes téléphoniques dont il était l'utilisateur, auxquelles les enquêteurs n'ont eu accès que sur commission rogatoire du juge d'instruction.

18. C'est à tort que, pour ne pas faire droit à la nullité des procès-verbaux d'exploitation de facturations détaillées et de données géolocalisées concernant le requérant, l'arrêt énonce en substance que les articles L. 34-1 et R. 10-13 du code des postes et des communications électroniques, dans leur version en vigueur au moment des faits, prévoyaient une conservation ciblée des données de connexion.

19. En effet, une telle conservation n'existait pas en droit français.

20. L'arrêt n'encourt néanmoins pas la censure pour les motifs qui suivent.

21. D'une part, la chambre de l'instruction a, à juste titre, énoncé que les faits d'importation et d'exportation de plusieurs centaines de kilogrammes de cocaïne d'une grande pureté, en bande organisée, par une structure criminelle de dimension internationale, entrent dans le champ de la criminalité grave.

22. D'autre part, elle a également relevé que l'ingérence dans la vie privée du requérant constituée par les réquisitions aux opérateurs téléphoniques et l'exploitation des données d'identité, de trafic et de géolocalisation apparaissait tout à la fois nécessaire et proportionnée à la poursuite d'infractions pénales relevant de la criminalité grave.

23. Il s'ensuit qu'agissant sur commission rogatoire du juge d'instruction, les enquêteurs pouvaient, sans méconnaître les dispositions conventionnelles invoquées au moyen, accéder aux données de trafic et de localisation régulièrement conservées pour la finalité de la sauvegarde de la sécurité nationale.