12 juillet 2022

Cour de cassation

Pourvoi n° 21-83.710

Chambre criminelle - Formation de section

Publié au Bulletin - Publié au Rapport

ECLI:FR:CCASS:2022:CR00769

Titres et sommaires

UNION EUROPEENNE - Principes de primauté et d'effectivité du droit de l'Union européenne - Effet - Inapplication des dispositions nationales contraires

Le principe de primauté du droit de l'Union européenne impose d'assurer le plein effet de ses dispositions en laissant, au besoin, inappliquée toute réglementation contraire de la législation nationale

---

UNION EUROPEENNE - Données de connexion - Règles de conservation et d'accès aux données - Méconnaissance - Conservation généralisée et indifférenciée des données de connexion aux fins de lutte contre la criminalité

Doivent être écartés, comme contraires au droit de l'Union européenne, lequel s'oppose à une conservation généralisée et indifférenciée, à titre préventif, des données de trafic et de localisation aux fins de lutte contre la criminalité, quel que soit son degré de gravité, l'article L. 34-1, III, du code des postes et communications électroniques, dans sa version issue de la loi n° 2013-1168 du 18 décembre 2013, ainsi que l'article R. 10-13 dudit code, en ce qu'ils imposaient aux opérateurs de services de communications 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, à celles relatives aux adresses IP attribuées à la source d'une connexion

---

UNION EUROPEENNE - Données de connexion - Règles de conservation et d'accès aux données - Conformité - Conservation généralisée et indifférenciée des données de connexion aux fins de sauvegarde de la sécurité nationale

En revanche et dès lors que le droit de l'Union européenne admet la conservation généralisée et indifférenciée des données de connexion aux fins de sauvegarde de la sécurité nationale, est conforme au droit de l'Union l'obligation faite aux opérateurs de télécommunications électroniques de conserver ces données de manière généralisée et indifférenciée en raison de la menace grave, réelle et actuelle ou prévisible à laquelle la France se trouve exposée depuis décembre 1994, du fait du terrorisme et de l'activité de groupes radicaux et extrémistes

---

UNION EUROPEENNE - Données de connexion - Règles de conservation et d'accès aux données - Injonction tendant à la conservation rapide des données - Conditions - Détermination

Par ailleurs, le droit de l'Union européenne, qui autorise la délivrance d'une injonction tendant à la conservation rapide des données relatives au trafic et des données de localisation stockées par les opérateurs, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale, permet

d'accéder auxdites données pour l'élucidation d'une infraction déterminée

---

UNION EUROPEENNE - Données de connexion - Règles de conservation et d'accès aux données - Injonction tendant à la conservation rapide des données - Définition

A cet égard, les articles 60-1 et 60-2 applicables en enquête de flagrance, 77-1-1 et 77-1-2 relatifs aux enquêtes préliminaires, 99-3 et 99-4 concernant l'ouverture d'une information du code de procédure pénale, doivent être analysés comme valant injonction de conservation rapide

---

UNION EUROPEENNE - Données de connexion - Règles de conservation et d'accès aux données - Injonction tendant à la conservation rapide des données - Conditions - Vérifications - Office du juge

Il appartient donc à la juridiction, saisie d'une contestation sur le recueil des données de connexion, de vérifier que, d'une part, la conservation rapide respecte les limites du strict nécessaire, d'autre part, les faits relèvent de la criminalité grave, au regard de la nature des agissements en cause, de l'importance du dommage qui en résulte, des circonstances de la commission des faits et de la durée de la peine encourue

---

UNION EUROPEENNE - Données de connexion - Règles de conservation et d'accès aux données - Injonction tendant à la conservation rapide des données - Conditions - Contrôle par une juridiction ou une entité administrative indépendante - Exclusion - Ministère public

S'agissant de l'autorisation d'accéder aux données de connexion qui, selon la jurisprudence de la Cour de justice de l'Union européenne (CJUE), ne peut relever de la compétence du ministère public, ne sont pas conformes au droit de l'Union les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale, 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, qui n'exerce pas l'action publique mais statue de façon impartiale sur le sort de celle-ci, est habilité à contrôler l'accès aux données de connexion

---

UNION EUROPEENNE - Données de connexion - Règles de conservation et d'accès aux données - Méconnaissance - Contestation possible des éléments de preuve résultant de l'exploitation de ces données - Principe d'effectivité du droit de l'Union européenne - Compatibilité

En cas d'irrégularité affectant la conservation ou l'accès aux données de connexion, le principe d'effectivité posé par la Cour de justice de l'Union européenne (CJUE) est respecté, la législation française, et notamment les articles 156 et suivants du code de procédure pénale, offrant à toute personne mise en examen ou poursuivie la possibilité de contester efficacement la pertinence des éléments de preuve résultant de l'exploitation des données de connexion

---

UNION EUROPEENNE - Données de connexion - Règles de conservation et d'accès aux données - Objet - Protection de la vie privée, du droit à la protection des données à caractère personnel et du droit à la liberté d'expression - Méconnaissance - Portée

Par ailleurs, dès lors que les modalités de conservation et d'accès aux données de connexion ont pour objet la protection du droit au respect de la vie privée, du droit à la protection des données à caractère personnel et du droit à la liberté d'expression, leur méconnaissance n'affecte qu'un intérêt privé, de sorte que le requérant à la nullité n'est recevable que s'il prétend être titulaire ou utilisateur de l'une des lignes identifiées ou s'il établit qu'il a été porté atteinte à sa vie privée

---

UNION EUROPEENNE - Données de connexion - Règles de conservation et d'accès aux données - Injonction tendant à la conservation rapide des données - Conditions - Contrôle par une juridiction ou une entité administrative indépendante - Défaut - Existence d'un grief - Conditions - Détermination

L'existence d'un grief pris de l'absence de contrôle préalable par une juridiction ou une entité administrative indépendante n'est établie que lorsque l'accès a porté sur des données irrégulièrement conservées, pour une finalité moins grave que celle ayant justifié la conservation hors hypothèse de la conservation rapide, n'a pas été circonscrit à une procédure visant à la lutte contre la criminalité grave ou a excédé les limites du strict nécessaire

Texte de la **décision**

Entête

N° Y 21-83.710 FS-B R

N° 00769

GM
12 JUILLET 2022

REJET

M. SOULARD président,

R É P U B L I Q U E F R A N Ç A I S E
_____

AU NOM DU PEUPLE FRANÇAIS
_____

ARRÊT DE LA COUR DE CASSATION, CHAMBRE CRIMINELLE,
DU 12 JUILLET 2022

M. [C] [L] [E] a formé un pourvoi contre l'arrêt de la chambre de l'instruction de la cour d'appel de Paris, 7e section, en date du 27 mai 2021, qui, dans l'information suivie contre lui, notamment, des chefs de meurtre et tentative, destruction de biens, en bande organisée, et association de malfaiteurs, a prononcé sur sa demande d'annulation de pièces de la procédure.

Par ordonnance en date du 23 septembre 2021, le président de la chambre criminelle a prescrit l'examen immédiat du pourvoi.

Un mémoire a été produit.

Sur le rapport de Mme Ménotti, conseiller, les observations de la SCP Célice, Texidor, Périer, avocat de M. [L] [E], et les conclusions de M. Desportes, premier avocat général, l'avocat du demandeur ayant eu la parole en dernier, après débats en l'audience publique du 19 mai 2022 où étaient présents M. Soulard, président, Mme Ménotti, conseiller rapporteur, M. Bonnal, M. de Larosière de Champfeu, Mme Leprieur, Mme Sudre, M. Maziau, Mme Issenjou, M. Turbeaux, Mme Labrousse, M. Seys, M. Dary, Mme Thomas, M. Laurent, conseillers de la chambre, Mme Barbé, M. Violeau, M. Mallard, Mme Guerrini, M. Michon, conseillers référendaires, M. Desportes, premier avocat général, et M. Maréville, greffier de chambre,

la chambre criminelle de la Cour de cassation, composée des président et conseillers précités, après en avoir délibéré conformément à la loi, a rendu le présent arrêt.

Exposé du litige

Faits et procédure

1. Il résulte de l'arrêt attaqué et des pièces de la procédure ce qui suit.

2. À la suite d'une fusillade intervenue le 24 août 2019 au cours de laquelle [D] [P] a été tué, diverses investigations ont été effectuées par les enquêteurs sous le régime de la flagrance, puis une information a été ouverte des chefs susvisés, le 6 septembre suivant.

3. Interpellé le 23 juin 2020, M. [C] [L] [E] a été mis en examen le 26 juin et placé en détention provisoire.

4. Le 28 décembre 2020, il a déposé une requête en nullité.

Moyens

Examen des moyens

Sur le premier moyen

Enoncé du moyen

5. Le moyen critique l'arrêt attaqué en ce qu'il a rejeté la requête en annulation de pièces présentées par M. [L] [E], alors « que par mémoire distinct, il est sollicité le renvoi au Conseil constitutionnel d'une question prioritaire de constitutionnalité portant sur la conformité aux droits et libertés que la Constitution garantit, et en particulier au droit au respect de la vie privée garanti par l'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789, de l'article L. 34-1 du code des postes et des communications électroniques ; que l'abrogation de ce texte, en vertu duquel ont été recueillies, conservées et exploitées les données concernant M. [L] [E], entraînera la cassation de l'arrêt. »

Motivation

Réponse de la Cour

6. Si le Conseil constitutionnel a, dans sa décision n° 2021-976/977 QPC du 25 février 2022, déclaré contraires à la Constitution certaines dispositions de l'article L. 34-1 du code des postes et des communications électroniques en ce qu'elles portent une atteinte disproportionnée au droit au respect de la vie privée, il a précisé que les mesures en cause ne peuvent être contestées sur le fondement de cette inconstitutionnalité.

7. Il s'ensuit que le moyen est devenu sans objet.
Sur les deuxième et troisième moyens

Moyens

Enoncé des moyens

8. Le deuxième moyen critique l'arrêt attaqué en ce qu'il a rejeté la requête en annulation de pièces présentée par M. [L] [E], alors :

« 1°/ que viole l'article 15 de la directive 2002/58/CE du 12 juillet 2002 modifiée, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne la juridiction qui retient à l'encontre d'une personne des éléments de preuve obtenus par un recueil et une conservation préventifs, généralisés et indifférenciés des données relatives au trafic et des données de localisation incompatibles avec le droit de l'Union, notamment parce que ce recueil et cette conservation ne sont ni ciblés ni soumis à l'autorisation et au contrôle d'une autorité indépendante ; qu'au cas d'espèce, M. [L] [E] faisait valoir, pour solliciter l'annulation des données de trafic et de localisation requises, obtenues et exploitées à son encontre, que ces données avaient été conservées de façon préventive, généralisée et indifférenciée en violation des textes précités ; qu'en ne répondant pas à ce moyen opérant, la chambre de l'instruction a violé l'article 593 du code de procédure pénale ;

2°/ que viole l'article 15 de la directive 2002/58/CE du 12 juillet 2002 modifiée, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne la juridiction qui retient à l'encontre d'une personne des éléments de preuve obtenus par un recueil et une conservation préventifs, généralisés et indifférenciés des données relatives au trafic et des données de localisation incompatibles avec le droit de l'Union, notamment parce que ce recueil et cette conservation ne sont ni ciblés ni soumis à l'autorisation et au contrôle d'une autorité indépendante ; qu'au cas d'espèce, M. [L] [E] faisait valoir, pour solliciter l'annulation des données de trafic et de localisation requises, obtenues et exploitées à son encontre, que ces données avaient été conservées de façon préventive, généralisée et indifférenciée en violation des textes précités ; qu'en retenant, pour rejeter cette demande, que l'atteinte ainsi portée à la vie privée de M. [L] [E] était proportionnée à l'objectif poursuivi, la chambre de l'instruction a violé les articles 15 de la directive 2002/58/CE du 12 juillet 2002 modifiée, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne. »

9. Le troisième moyen critique l'arrêt attaqué en ce qu'il a rejeté la requête en annulation de pièces présentée par M. [L] [E], alors « que viole le droit à la vie privée garanti par l'article 8 de la Convention européenne des droits de l'homme la juridiction qui retient à l'encontre d'une personne des éléments de preuve obtenus par un recueil et une conservation des données relatives au trafic et des données de localisation préventifs, généralisés, indifférenciés et échappant à toute autorisation ou contrôle d'une autorité indépendante ; qu'au cas d'espèce, M. [L] [E] faisait valoir, pour solliciter l'annulation des données de trafic et de localisation requises, obtenues et exploitées à son encontre, qu'en violation du texte précité ces données avaient été conservées de façon préventive, généralisée et indifférenciée, et que leur recueil ne faisait l'objet ni d'une autorisation en amont ni d'un contrôle en aval par une autorité indépendante ; qu'en retenant, pour rejeter cette demande ; qu'il en déduisait que l'atteinte ainsi portée à sa vie privée était disproportionnée à l'objectif poursuivi ; qu'en retenant, pour rejeter la requête, que l'ingérence dans la vie privée de M. [L] [E] résultant du recueil et de l'exploitation de ces données était proportionnée au but légitime de poursuite des infractions pénales, la chambre de l'instruction a violé l'article 8 précité. »

Motivation

Réponse de la Cour

10. Les moyens sont réunis.

11. Afin de garantir l'effectivité de l'ensemble des dispositions du droit de l'Union européenne, le principe de primauté impose aux juridictions nationales d'interpréter, dans toute la mesure du possible, leur droit interne de manière conforme au droit de l'Union. A défaut de pouvoir procéder à une telle interprétation, le juge national a l'obligation d'assurer le plein effet des dispositions du droit de l'Union en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il [L] à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel (CJCE, arrêt du 9 mars 1978, Simmenthal, 106/77).

12. Il convient, dès lors, d'examiner si, à la date des réquisitions litigieuses, la réglementation française sur la conservation et l'accès aux données de connexion était conforme au droit de l'Union.

Sur la régularité de la conservation

Sur les exigences du droit de l'Union en matière de conservation générale et indifférenciée des données de connexion

13. La Cour de justice de l'Union européenne (CJUE) a dit pour droit qu'il résulte de l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, que le droit de l'Union européenne s'oppose à une conservation généralisée et indifférenciée, à titre préventif, des données de trafic et de localisation aux fins de lutte contre la criminalité, quel que soit son degré de gravité. Seule est admise une conservation généralisée et indifférenciée de ces données, en cas de menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, sur injonction faite aux fournisseurs de services de télécommunications électroniques, pouvant faire l'objet d'un contrôle effectif par une juridiction ou une autorité administrative indépendante, dont la décision est dotée d'un effet contraignant, chargée de vérifier l'existence d'une telle menace et le respect des conditions et garanties devant être prévues, injonction ne pouvant être émise que pour une période limitée au strict nécessaire, mais renouvelable en cas de persistance de la menace.

14. En revanche, le droit de l'Union ne s'oppose pas à des mesures législatives prévoyant, aux fins de lutte contre la criminalité grave :

- 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 ;
- une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;
- une conservation généralisée et indifférenciée des données relatives à l'identité civile, aux comptes et aux paiements des utilisateurs de moyens de communications électroniques ;
- le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, 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, dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

15. Cette conservation rapide a pour fondement l'article 16 de la Convention du Conseil de l'Europe sur la cyber-criminalité, signée à Budapest le 23 novembre 2001, les Etats membres pouvant prévoir dans leur législation qu'un accès aux données de trafic et de localisation peut avoir lieu à des fins de lutte contre la criminalité grave, en vue de l'élucidation d'une infraction déterminée, dans le respect des conditions matérielles et procédurales prévues en droit européen (CJUE, arrêt du 6 octobre 2020, La Quadrature du Net e.a., [4] e.a., C-511/18, C-512/18, C-520/18).

16. Selon la CJUE, la conservation rapide et l'accès aux données ainsi conservées peuvent porter sur les données stockées par les fournisseurs de services de communications électroniques sur la base des articles 5, 6 et 9 de la directive 2002/58/CE ou sur celle des mesures législatives prises en vertu de l'article 15, paragraphe 1 (CJUE, arrêt La Quadrature du net, précité, points 160 et 167).

17. Cette position a été maintenue dans l'arrêt Commissioner of An Garda Siochana du 5 avril 2022 (C-140/20, points 85 et 87), la Cour ayant seulement écarté, à nouveau, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation aux fins de lutte contre la criminalité grave pour répondre à une objection du gouvernement danois (même arrêt, points 96 à 100).

18. La conservation rapide peut donc porter sur les données que détiennent les opérateurs de télécommunications électroniques, soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale.

19. L'interprétation qui exclurait du champ d'application de la conservation rapide les données conservées aux fins de sauvegarde de la sécurité nationale priverait d'effet utile sa finalité, qui est de permettre aux autorités nationales, en matière de lutte contre la criminalité grave, d'accéder à des données qui n'ont pas été conservées dans ce but.

20. Par ailleurs, une telle mesure peut être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave, pour autant que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction, telles les données de la victime et celles de son entourage social ou professionnel (CJUE, arrêt Commissioner of An Garda Siochana, précité, point 88).

Sur la conservation généralisée et indifférenciée des données de connexion en droit français

21. L'article L. 34-1, III, du code des postes et des communications électroniques, dans sa version en vigueur à la date des faits, imposait aux opérateurs de services de télécommunications électroniques la conservation généralisée et indifférenciée, pour une durée maximale d'un an, des données de connexion énumérées à l'article R. 10-13 dudit code, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

22. Ce dernier texte, dans sa version en vigueur à la date des faits, précisait que cette obligation de conservation, d'une durée d'un an, portait sur :
a) les informations permettant d'identifier l'utilisateur ;
b) les données relatives aux équipements terminaux de communication utilisés ;
c) les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
d) les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
e) les données permettant d'identifier le ou les destinataires de la communication.

23. Il prévoyait également que, pour les activités de téléphonie, l'opérateur devait conserver les données relatives au trafic et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

Sur la conformité du droit français au droit européen s'agissant de la conservation généralisée et indifférenciée des données de connexion

24. Il résulte des principes rappelés aux paragraphes 13 et 14 qu'il convient d'écarter les textes précités de droit interne en ce qu'ils imposaient 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 et aux informations relatives aux comptes et aux paiements, ainsi que, dans le cadre de la recherche et la répression de la criminalité grave, aux adresses IP.

25. En revanche, l'obligation de conservation des données de trafic et de localisation imposée aux opérateurs par l'article L. 34-1, III, du code précité, mis en oeuvre par l'article R. 10-13 dudit code, en ce qu'elle permet notamment la recherche, la constatation et la poursuite des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme, infractions incriminées aux articles 410-1 à 422-7 du code pénal, est conforme au droit de l'Union, comme poursuivant l'objectif de sauvegarde de la sécurité nationale.

26. La durée de conservation de ces données, pour une année, apparaît strictement nécessaire aux besoins de la sauvegarde de la sécurité nationale.

27. Pour autant, les dispositions des articles précités du code des postes et des communications électroniques ne subordonnent pas le maintien de cette obligation de conservation à un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale.

28. Il s'ensuit que cette obligation de conservation ne vaut injonction au sens où l'entend la CJUE et cette conservation n'est régulière que si le juge saisi du contentieux constate, sous le contrôle de la Cour de cassation, l'existence d'une menace présentant les caractéristiques précitées.

29. A cet égard, même en tenant compte de l'exigence du droit de l'Union selon laquelle cette conservation ne saurait présenter un caractère systémique (CJUE, arrêt La Quadrature du Net, précité, point 138), il résulte notamment des pièces régulièrement produites par le procureur général près la Cour de cassation relatives aux attentats commis en France depuis décembre 1994, soit antérieurement à la date des faits, que la France se trouve exposée, en raison du terrorisme et de l'activité de groupes radicaux et extrémistes, à une menace grave et réelle, actuelle ou prévisible à la sécurité nationale.

30. Dès lors, l'obligation faite aux opérateurs de télécommunications électroniques de conserver de façon généralisée et indifférenciée aux fins de sauvegarde de la sécurité nationale les données de connexion énumérées à l'article R. 10-13 du code précité, qui ont fait l'objet des réquisitions litigieuses, était conforme au droit de l'Union.

31. Le Conseil d'Etat n'a d'ailleurs déclaré illégales les dispositions de cet article qu'en ce qu'elles imposaient aux opérateurs de communications électroniques, aux fournisseurs d'accès à internet et aux hébergeurs la conservation généralisée et indifférenciée des données de connexion, autres que les données relatives à l'identité civile, aux adresses IP et aux informations relatives aux comptes et aux paiements, aux fins de lutte contre la criminalité et de prévention des menaces à l'ordre public et ne prévoyaient pas un réexamen périodique de l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale (CE, 21 avril 2021, French Data Network, n° 393099, point 58).

Sur la conservation rapide en droit français

32. Il convient ensuite de rechercher s'il existait, à la date des faits, une réglementation conforme au droit de l'Union permettant la conservation rapide des données de trafic et de localisation. Une telle réglementation doit notamment préciser la ou les finalités pour laquelle ou lesquelles une conservation rapide peut être ordonnée (CJUE, arrêt La Quadrature du Net, précité, point 132).

33. A la date des faits, la communication des données de trafic ou de localisation conservées par les opérateurs de télécommunication pouvait faire l'objet de réquisitions lors d'une enquête de flagrance, en application des articles 60-1 et 60-2 du code de procédure pénale, par un officier de police judiciaire ou par un agent de police judiciaire agissant sous son contrôle, lors d'une enquête préliminaire, sur le fondement des articles 77-1-1 et 77-1-2 dudit code, sur autorisation du procureur de la République, enfin, en cas d'ouverture d'une information, en application des articles 99-3 et 99-4, de ce code, par un officier de police judiciaire autorisé par commission rogatoire du juge d'instruction. La régularité de ces opérations peut être contestée devant la chambre de l'instruction ou la juridiction de jugement, sous le contrôle de la

Cour de cassation.

34. Ces dispositions, qui prévoyaient la communication immédiate des données de connexion aux autorités nationales compétentes, doivent être analysées comme valant injonction de conservation rapide, au sens de la Convention de Budapest. En effet, le rapport explicatif de celle-ci précise que l'injonction de conservation rapide peut résulter d'une injonction de produire.

35. En outre, aux termes du sixième alinéa du paragraphe III de l'article préliminaire du code de procédure pénale, les mesures portant atteinte à la vie privée d'une personne ne peuvent être prises, sur décision ou sous contrôle effectif de l'autorité judiciaire, que si elles sont, au regard des circonstances de l'espèce, nécessaires à la manifestation de la vérité et proportionnées à la gravité de l'infraction.

36. Il s'ensuit que les dispositions précitées combinées peuvent être interprétées de façon conforme au droit de l'Union comme permettant, pour la lutte contre la criminalité grave, en vue de l'élucidation d'une infraction déterminée, la conservation rapide des données de connexion stockées, même conservées aux fins de sauvegarde de la sécurité nationale.

37. 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.

38. 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.

Sur l'accès aux données

Sur les exigences européennes en matière d'accès aux données

39. La CJUE a jugé (CJUE, arrêt du 2 mars 2021, H.K./Prokuratuur, C-746/18) que l'accès aux données de connexion ne peut être autorisé que :

- si ces données ont été conservées conformément aux exigences du droit européen ;
- s'il a eu lieu pour la finalité ayant justifié la conservation ou une finalité plus grave, sauf conservation rapide ;
- s'il est limité au strict nécessaire ;
- s'agissant des données de trafic et de localisation, s'il est circonscrit aux procédures visant à la lutte contre la criminalité grave ;
- et s'il est soumis au contrôle préalable d'une juridiction ou d'une entité administrative indépendante.

Sur l'exigence d'un contrôle préalable

40. Il résulte de la jurisprudence de la CJUE que l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11, ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux, s'oppose à une réglementation nationale donnant compétence au ministère public, qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et à la localisation (CJUE, arrêt H.K./Prokuratuur, précité). Elle juge également qu'un fonctionnaire de police ne constitue pas une juridiction et ne présente pas toutes les garanties d'indépendance et d'impartialité requises (CJUE, arrêt Commissioner of An Garda Siochana, précité).

41. En effet, la CJUE rappelle qu'il est essentiel que l'accès des autorités nationales compétentes aux données conservées

soit subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, susceptible d'assurer un juste équilibre entre, d'une part, les intérêts liés aux besoins de l'enquête dans le cadre de la lutte contre la criminalité grave, et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel.

42. Ainsi, les articles 60-1, 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 un contrôle préalable par une juridiction ou une entité administrative indépendante.

43. En revanche, le juge d'instruction est habilité à contrôler l'accès aux données de connexion. En effet, d'une part, il n'est pas une partie à la procédure mais une juridiction qui statue notamment sur les demandes d'actes d'investigation formées par les parties, lesquelles disposent d'un recours en cas de refus ; d'autre part, il n'exerce pas l'action publique mais statue de façon impartiale sur le sort de celle-ci, mise en mouvement par le ministère public ou, le cas échéant, la partie civile.

Sur les conséquences de la méconnaissance des exigences du droit de l'Union européenne

44. La CJUE juge qu'il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe d'autonomie procédurale, de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas moins favorables que celles régissant des situations similaires soumises au droit interne - principe d'équivalence - et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union - principe d'effectivité - (CJUE, arrêt La Quadrature du Net, précité, point 223).

45. Le principe d'effectivité impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union ou encore au moyen d'un accès à ces données en violation de ce droit, à l'occasion d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si celles-ci ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits (CJUE, arrêt La Quadrature du Net, précité, points 226 et 227).

46. A cet égard, il résulte des articles 156 et suivants du code de procédure pénale que toute personne mise en examen peut solliciter du juge d'instruction une expertise et, le cas échéant, une contre-expertise, sous le contrôle de la chambre de l'instruction, lorsque se pose une question d'ordre technique. Il en est de même devant la juridiction de jugement.

47. Il s'ensuit que la législation française offre ainsi à toute personne mise en examen ou poursuivie la possibilité de contester efficacement la pertinence des éléments de preuve résultant de l'exploitation des données de connexion.

48. Le principe d'équivalence commande que l'ensemble des règles de procédure nationales s'applique indifféremment aux recours fondés sur la violation du droit de l'Union et aux recours fondés sur la méconnaissance du droit interne ayant un objet et une cause semblables.

49. Hors les cas de nullité d'ordre public, qui touchent à la bonne administration de la justice, la juridiction, saisie d'une requête ou d'une exception de nullité, doit d'abord rechercher si le requérant a intérêt à demander l'annulation de l'acte, puis, s'il a qualité pour la demander et, enfin, si l'irrégularité alléguée lui a causé un grief. Pour déterminer si le requérant a qualité pour agir en nullité, la juridiction doit examiner si la formalité substantielle ou prescrite à peine de nullité, dont la méconnaissance est alléguée, a pour objet de préserver un droit ou un intérêt qui lui est propre (Crim., 7 septembre 2021, pourvoi n° 21-80.642, publié au Bulletin).

50. Les exigences européennes en matière de conservation et d'accès aux données de connexion ont pour objet la protection du droit au respect de la vie privée, du droit à la protection des données à caractère personnel et du droit à la liberté d'expression (CJUE, arrêt La Quadrature du Net, précité), de sorte que leur méconnaissance n'affecte qu'un intérêt

privé.

51. Il en est ainsi en particulier de l'exigence d'un contrôle préalable par une juridiction ou une entité administrative indépendante qui vise à garantir, en pratique, le plein respect des conditions d'accès aux données à caractère personnel, telles que précisées au paragraphe 39, et notamment que l'ingérence dans l'exercice des droits précités est limitée à ce qui est strictement nécessaire (CJUE, arrêt H.K./Prokuratuur précité, points 51 et 58 ; CJUE, arrêt Commissioner of An Garda Siochana précité, point 110).

52. Il s'ensuit qu'en application du principe d'équivalence, la personne mise en examen ou poursuivie n'est recevable à invoquer la violation de cette exigence en matière d'accès aux données de connexion 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 (Crim., 6 février 2018, pourvoi n° 17-84.380, Bull. crim. 2018, n° 30).

53. Enfin, le juge pénal ne peut prononcer la nullité, en application des dispositions de l'article 802 du code de procédure pénale, que si l'irrégularité elle-même a occasionné un préjudice au requérant, lequel ne peut résulter de la seule mise en cause de celui-ci par l'acte critiqué (Crim., 7 septembre 2021, précité).

54. La Cour de cassation juge que l'irrégularité fait nécessairement grief au requérant, lorsque la méconnaissance de la règle a irrévocablement affecté les droits de celui-ci.

55. Tel est le cas lorsque l'acte attentatoire à la vie privée a été accompli par une autorité qui n'était pas compétente, à défaut d'y avoir été autorisée, conformément à la loi. Tel est également le cas lorsque l'acte n'a pas été motivé par l'autorité compétente pour l'ordonner alors qu'il devait l'être (Crim., 8 juillet 2015, pourvoi n° 15-81.731, Bull. crim. 2015, n° 174).

56. A défaut, il appartient au requérant de justifier d'une atteinte à ses intérêts. La Cour de cassation juge qu'il en est ainsi notamment lorsque l'acte attentatoire à la vie privée a été accompli par un agent compétent mais sans le contrôle d'un tiers alors que celui-ci était prévu par la loi (Crim., 7 décembre 2021, pourvoi n° 20-82.733, publié au Bulletin). C'est le cas du procureur de la République ou de l'officier de police judiciaire compétent en vertu du droit national pour accéder aux données de connexion, mais qui agit sans le contrôle préalable d'une juridiction ou d'une entité administrative indépendante.

57. Il se déduit des principes énoncés ci-dessus aux paragraphes 50 et 51 que cette absence de contrôle indépendant préalable ne peut faire grief au requérant que s'il établit l'existence d'une ingérence injustifiée dans sa vie privée et dans ses données à caractère personnel, de sorte que cet accès aurait dû être prohibé.

58. Il appartient, dès lors, à la chambre de l'instruction de s'assurer du respect des quatre premières conditions énoncées au paragraphe 39 et notamment de ce que, d'une part, l'accès a porté sur des données régulièrement conservées, d'autre part, la ou les catégories de données visées, ainsi que la durée pour laquelle l'accès à celles-ci a eu lieu, étaient, au regard des circonstances de l'espèce, limitées à ce qui était strictement justifié par les nécessités de l'enquête.

59. En l'espèce, pour rejeter la demande de nullité résultant des modalités de conservation et d'accès aux données de connexion concernant M. [L] [E], la chambre de l'instruction énonce que les lignes téléphoniques utilisées par celui-ci ont été exploitées par les enquêteurs, suite à leur identification dans le cadre de l'exploitation du flux des bornes couvrant les lieux intéressant l'enquête, à savoir la scène de crime d'[Localité 2] au moment du meurtre, la scène de l'incendie du véhicule Mercedes des auteurs à [Localité 1] et le secteur du domicile de la victime, [D] [P], à [Localité 3], où était localisé de manière récurrente le véhicule utilisé par les tueurs.

60. Elle précise que l'obtention de ces données et leur exploitation ont permis de localiser l'intéressé à proximité des lieux où se trouvait [D] [P], d'en conclure qu'il surveillait ce dernier et de constater qu'il se trouvait encore aux abords de son domicile peu de temps avant son assassinat, de sorte qu'il a pu donner le signal du départ à un individu pour venir le rejoindre à cet endroit où la victime a été abattue peu de temps après.

61. Elle ajoute que M. [L] [E], mis en examen le 26 juin 2020, a eu accès à la procédure à partir de cette date et était donc, depuis lors, en mesure de commenter efficacement l'ensemble des éléments de la procédure qui caractérisait des indices graves ou concordants rendant vraisemblable son implication comme auteur ou complice des faits.

62. Elle conclut que l'ingérence alléguée dans la vie privée de M. [L] [E] du fait des réquisitions des enquêteurs aux opérateurs téléphoniques est prévue par la loi, qu'elle a eu un but légitime qui est celui de la recherche d'infractions pénales relevant de la criminalité grave, en l'espèce meurtre et tentative de meurtre en bande organisée, destruction par moyen dangereux en bande organisée, association de malfaiiteurs, recel en bande organisée, que cet objectif tendant à la recherche d'infractions pénales est nécessaire dans une société démocratique, et que cette ingérence apparaît proportionnée à la poursuite de l'objectif.

63. En l'état de ces motifs, dont il résulte que l'accès aux informations litigieuses a porté sur des données régulièrement conservées et qu'il a eu lieu en vue de la poursuite d'infractions relevant de la criminalité grave, dans des conditions limitant cet accès à ce qui était strictement justifié par les nécessités de l'enquête, la chambre de l'instruction n'a méconnu aucun des textes visés au moyen.

64. En conséquence, celui-ci doit être écarté.

65. Par ailleurs l'arrêt est régulier en la forme.

Dispositif

PAR CES MOTIFS, la Cour :

REJETTE le pourvoi ;

Ainsi fait et jugé par la Cour de cassation, chambre criminelle, et prononcé par le président le douze juillet deux mille vingt-deux.

Travaux **Préparatoires**

Rapport du conseiller

TÉLÉCHARGER (2022-07-12_RAPPORT_21-83.710.PDF - 552 KB)

Avis oral de l'avocat général

TÉLÉCHARGER (2022-07-12_AVIS_ORAL_21-83.729_ET_AUTRES.PDF - 326 KB)

Avis oral de l'avocat général

TÉLÉCHARGER (2022-07-12_AVIS_ORAL_VALAT_21-83.729_ET_AUTRES.PDF - 583 KB)

Avis oral de l'avocat général

TÉLÉCHARGER (2022-07-12_AVIS_ORAL_PETITPREZ_21-83.729_ET_AUTRES.PDF - 235 KB)

Avis de l'avocat général

TÉLÉCHARGER (2022-07-12_AVIS_21-83.710.PDF - 1.01 MB)

Documents de **communication**

Notice au rapport annuel

TÉLÉCHARGER (NOTICE_21-83.710.PDF - 249 KB)

Communiqué

TÉLÉCHARGER (COMMUNIQUÉ DONNÉES DE CONNEXION 20220712.PDF - 448 KB)

Note explicative

TÉLÉCHARGER (NOTE_EXPLICATIVE__12-07-2022.PDF - 1.14 MB)

Textes **appliqués**

- Articles 7, 8, 11 et 52, § 1, de la Charte des droits fondamentaux de l'Union européenne.
- Article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales.

Articles 5, 6, 9 et 15 de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002.

Article 16 de la Convention du Conseil de l'Europe sur la cyber-criminalité, signée à Budapest le 23 novembre 2001.

Articles 60-1, 60-2, 77-1-1, 77-1-2, 99-3, 99-4, 593 et 802 du code de procédure pénale.

Articles L. 34-1, III et R. 10-13 du code des postes et des communications électroniques.

Rapprochements de **jurisprudence**

CJCE, arrêt du 9 mars 1978, Simmenthal, C-106/77.

CJUE, arrêt du 6 octobre 2020, La Quadrature du Net e.a, French Data Network e.a, C-511/18, C- 512/18, C- 520/18.

CJUE, arrêt du 2 mars 2021, Prokuratuur, C-746/18.

CE, 21 avril 2021, n° 393099, publié au Recueil Lebon.

CJUE, arrêt du 5 avril 2022, Commissioner of An Garda Siochana, C-140/20.

Crim., 8 juillet 2015, pourvoi n° 15-81.731, Bull. crim. 2015, n° 174 (cassation partielle).

Crim., 6 février 2018, pourvoi n° 17-84.380, Bull. crim. 2018, n° 30 (déchéance et rejet).

Crim., 7 septembre 2021, pourvoi n° 21-80.642, Bull., (cassation).

Crim., 7 décembre 2021, pourvoi n° 20-82.733, Bull., (rejet).