COUR DE CASSATION

Notice au rapport relative à l'arrêt n° 769 du 12 juillet 2022
Pourvoi n° 21-83.710 – Chambre criminelle

Le recours aux données de connexion est une méthode d'investigation à laquelle les services de police judiciaire ont, sous le contrôle de l'autorité judiciaire, de plus en plus fréquemment recours. Ces données permettent, notamment, de déterminer la localisation et les mouvements des personnes soupçonnées au moment des faits objet de l'enquête, d'identifier leurs interlocuteurs, ainsi que la fréquence et la durée des communications.

Dans une procédure ouverte des chefs de meurtre et tentative, destruction de biens, en bande organisée, et association de malfaiteurs, une des personnes mises en examen a saisi la chambre de l'instruction d'une requête en annulation des actes d'investigation fondés sur l'exploitation de ces données de connexion, tant au cours de l'enquête de flagrance qu'après ouverture d'une information judiciaire, en ce que la conservation desdites données et l'accès des enquêteurs à celles-ci seraient contraires au droit de l'Union européenne.

Saisie d'un pourvoi contre l'arrêt rejetant ces requêtes en nullité, la Cour de cassation a, par l'arrêt commenté[1], ainsi que par plusieurs autres rendus le même jour[2], été amenée à statuer pour la première fois sur cette question.

[1] Crim., 12 juillet 2022, pourvoi n° 21-83.710, publié au *Bulletin* et au *Rapport annuel*.

[2] Crim., 12 juillet 2022, pourvoi n° 21-83.820 ; pourvoi n° 21-84.096 ; pourvoi n° 20-86.652 et pourvoi n° 21-83.805, tous publiés au *Bulletin*.

En matière de données de connexion, la jurisprudence de la Cour de justice de l'Union européenne (CJUE) s'est construite par touches successives. Les décisions principalement invoquées au soutien du pourvoi ont été rendues à partir de l'année 2020[3].

Tel qu'interprété par ces arrêts, le droit de l'Union entend limiter strictement la possibilité d'imposer aux opérateurs de télécommunications la conservation des données de connexion, puis les conditions de l'accès à celles-ci, au motif que ces données permettent de disposer d'informations très précises concernant la vie privée des personnes. La CJUE considère donc que cette conservation et cet accès constituent une ingérence grave dans les droits fondamentaux des personnes concernées.

Par l'arrêt commenté, la Cour de cassation a statué d'abord sur les conditions de conservation des données de connexion (I) puis sur la question de l'accès auxdites données (II), enfin sur les conséquences à tirer de la méconnaissance du droit de l'Union (III).

I. La conservation des données de connexion

Le texte national relatif à la conservation des données de connexion, dont le pourvoi affirmait la non-conformité au droit de l'Union, est l'article L. 34-1, III, du code des postes et des communications électroniques, dans sa version applicable du 20 décembre 2013 au 31 juillet 2021. Ce texte imposait aux opérateurs de services de télécommunications électroniques la conservation généralisée et indifférenciée 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 » et pour une durée maximale d'un an.

La CJUE a dit pour droit, dans les arrêts précités, qu'il résulte de l'article 15, § 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, § 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.

[3] CJUE, gde ch., arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18 ; CJUE, gde ch., arrêt du 2 mars 2021, Prokuratuur, C-746/18 ; CJUE, gde ch., arrêt du 5 avril 2022, Commissioner of An Garda Síochána, C-140/20.

En revanche, le droit de l'Union ne s'oppose pas à une telle conservation « dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave [...] pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible »[4].

En d'autres termes, la conservation préventive, généralisée et indifférenciée des données de connexion n'est conforme au droit de l'Union que si elle vise à la sauvegarde de la sécurité nationale. Par sécurité nationale, il faut entendre « la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme »[5].

La CJUE précise les autres conditions dans lesquelles la conservation, soit ciblée, soit généralisée et indifférenciée, selon les cas, de tel ou tel type de données qu'elle énumère est admissible.

L'arrêt commenté juge en conséquence « 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 de la répression de la criminalité grave, aux adresses IP ».

Il retient, en revanche, que les dispositions précitées du code des postes et des communications électroniques sont conformes au droit de l'Union en ce qu'elles permettent « notamment la recherche, la constatation et la poursuite des atteintes aux intérêts fondamentaux de la Nation et des actes de terrorisme ».

La Cour de cassation, qui invite les juges à rechercher l'existence d'une menace grave, réelle et actuelle ou prévisible pour la sécurité nationale, juge, à cet égard, que depuis décembre 1994 et à la date des faits, l'État français se trouve confronté à des menaces graves du fait des attentats terroristes, de sorte que l'obligation faite aux opérateurs de télécommunications électroniques de conserver ces données de manière généralisée et indifférenciée était, pour ce motif, conforme au droit de l'Union.

---

[4] CJUE, gde ch., arrêt du 6 octobre 2020, La Quadrature du Net e.a., précité, § 137.

[5] Même arrêt, § 135.

La CJUE inclut parmi les conditions dans lesquelles elle admet la conservation des données de connexion l'injonction de « conservation rapide » de celles-ci, laquelle trouve son fondement dans l'article 16 de la Convention de Budapest du 23 novembre 2001 sur la cybercriminalité, ratifiée par la France. Ainsi, si les données sont régulièrement conservées à titre préventif pour les besoins de la sécurité nationale, il est possible d'enjoindre aux opérateurs de les conserver également, de manière ciblée et pour les besoins de la répression dans une affaire particulière relevant de la criminalité grave.

Par ailleurs, elle juge que la « conservation rapide » n'est pas limitée aux données de connexion des seules personnes soupçonnées de vouloir commettre ou d'avoir commis une infraction pénale, pourvu que ces données puissent contribuer à l'élucidation de l'infraction, « sur la base d'éléments objectifs et non discriminatoires »[6].

L'arrêt commenté, relevant que le rapport explicatif de la Convention de Budapest précitée « précise que l'injonction de conservation rapide peut résulter d'une injonction de produire », juge que les réquisitions prévues par le droit national, sur le fondement, soit des articles 60-1 et 60-2 du code de procédure pénale, lors d'une enquête de flagrance, soit des articles 77-1-1 et 77-1-2 dudit code, lors d'une enquête préliminaire, soit des articles 99-3 et 99-4 de ce code, dans le cours de l'instruction, peuvent donc valoir « injonction de conservation rapide ».

Déclinant les exigences posées par la CJUE, il impose à la juridiction saisie de vérifier que :
- les faits en cause relèvent de la criminalité grave : il s'agit d'une appréciation au cas par cas, qui doit prendre en compte la nature des agissements en cause, l'importance du dommage, les circonstances de la commission des faits et la durée de la peine encourue ;
- la « conservation rapide » respecte les limites du strict nécessaire.

II. L'accès aux données de connexion

La CJUE conditionne l'accès aux données de connexion[7] :
- à la conformité de leur conservation aux exigences du droit européen ;
- à ce qu'il ait lieu pour la finalité ayant justifié la conservation ou une finalité plus grave, sauf conservation rapide ;
- à ce qu'il soit limité au strict nécessaire ;
- s'agissant des données de trafic et de localisation, à ce qu'il soit circonscrit aux procédures visant à la lutte contre la criminalité grave ;

[6] CJUE, gde ch., arrêt du 5 avril 2022, Commissioner of An Garda Síochána, précité, § 88.

[7] CJUE, gde ch., arrêt du 2 mars 2021, Prokuratuur, précité.

- enfin, à ce qu'il soit soumis au contrôle préalable d'une juridiction ou d'une entité administrative indépendante.

Cette dernière exigence exclut que ce contrôle soit effectué, soit par le ministère public, « qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique »[8], soit par un fonctionnaire de police, qui ne constitue pas une juridiction et ne présente pas toutes les garanties d'indépendance et d'impartialité requises[9].

L'arrêt commenté juge en conséquence que les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale, les deux premiers confiant à un officier de police judiciaire ou un agent de police judiciaire agissant sous son contrôle le soin de décider d'accéder aux données de connexion, les deux derniers exigeant seulement une autorisation du procureur de la République, sont contraires au droit de l'Union, « 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, il juge différemment s'agissant des articles 99-3 et 99-4 du même code, le juge d'instruction n'étant 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 », et n'exerçant pas l'action publique mais statuant « de façon impartiale sur le sort de celle-ci, mise en mouvement par le ministère public ou, le cas échéant, la partie civile ».

III. Les conséquences qui doivent être tirées de la méconnaissance, par les textes internes, du droit de l'Union

La CJUE renvoie, sur ce point, à l'ordre juridique de chaque État membre, à condition que les modalités procédurales nationales permettant d'assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union « 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 », ce qui suppose notamment que les justiciables soient en mesure de commenter efficacement les éléments de preuve recueillis par un recours aux données de connexion, qui proviennent d'un domaine échappant à la connaissance des juges et qui sont

[8] CJUE, gde ch., arrêt du 2 mars 2021, Prokuratuur, précité.

[9] CJUE, gde ch., arrêt du 5 avril 2022, Commissioner of An Garda Síochána, précité.

susceptibles d'influencer de manière prépondérante l'appréciation des faits – principe d'effectivité[10].

L'arrêt commenté retient d'abord qu'il est possible, en droit français, soit devant la chambre de l'instruction, soit à l'audience, pour les personnes mises en examen ou poursuivies, « de contester efficacement la pertinence des éléments de preuve résultant de l'exploitation des données de connexion ».

Il relève ensuite que les exigences européennes en matière de conservation et d'accès aux données de connexion, y compris celles tenant au contrôle préalable par une juridiction ou une entité administrative indépendante, « 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 […], de sorte que leur méconnaissance n'affecte qu'un intérêt privé ».

Une telle méconnaissance entre donc dans la catégorie des nullités qui ne peuvent être prononcées que si le requérant établit, ainsi que l'exige l'article 802 du code de procédure pénale, d'une part, que les données, dont il affirme qu'elles ont été conservées et qu'il y a été accédé en méconnaissance du droit de l'Union, entrent dans la sphère de sa vie privée, d'autre part, que cette méconnaissance lui a occasionné un préjudice, lequel ne peut résulter de sa seule mise en cause par l'acte critiqué[11].

Il en résulte que les violations du droit de l'Union, et notamment l'absence de contrôle indépendant préalable, ne peuvent « 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 ».
L'arrêt commenté conclut en conséquence que, si le droit de l'Union a été méconnu, cette irrégularité ne doit conduire à l'annulation que dans les cas suivants :
- l'accès a porté sur des données irrégulièrement conservées ;
- l'accès n'a pas été limité à une procédure visant à lutter contre la criminalité grave ;
- l'accès a excédé les limites du strict nécessaire, notamment lorsque l'ingérence dans la vie privée du requérant n'était ni nécessaire, ni proportionnée.

C'est ainsi que, dans l'espèce dont elle était saisie, la Cour de cassation a rejeté le pourvoi, dès lors qu'il résultait de l'arrêt attaqué que « l'accès aux informations litigieuses a[vait] porté sur des données régulièrement conservées et qu'il a[vait] eu lieu en vue de la poursuite

[10] CJUE, gde ch., arrêt du 6 octobre 2020, La Quadrature du Net e.a., précité, § 223.

[11] Crim., 7 septembre 2021, pourvoi n° 21-80.642, publié au *Bulletin*.

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 ».