

Conditions d'accès aux données personnelles de connexion dans le cadre d'enquêtes pénales

Description

Cass. crim., 12 juillet 2022, n^{os} 21-83.710, 21-83.820, 21-84.096, 20-86.652.

Par quatre arrêts du 12 juillet 2022 (n^{os} 21.83.710, 21-83.820, 21-84.096 et 20-86.652), la Chambre criminelle de la Cour de cassation détermine, sur la base du droit européen, et particulièrement de la jurisprudence de la Cour de justice de l'Union européenne (CJUE), les droits et obligations relatifs aux conditions de conservation et d'accès aux données de connexion aux services de communications électroniques (téléphone et communication en ligne), détenues par les opérateurs (fournisseurs d'accès et hébergeurs), dans le cadre d'enquêtes pénales.

Principes du droit européen

Les principes du droit européen, en la matière, sont déterminés notamment par la Charte des droits fondamentaux de l'Union européenne et, plus précisément, par la directive 2002/58/CE, 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 (dite « vie privée et communications électroniques »), et par l'interprétation qu'en fait la Cour de justice.

Directive du 12 juillet 2002

En son article 15, la directive du 12 juillet 2002 pose que « *les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations* » qu'elle détermine, en matière de « *confidentialité des communications* » et s'agissant des « *données relatives au trafic* », « *lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État –, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales [...]. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés* ». Toutes ces mesures sont prises dans le respect des principes généraux du droit européen.

Jurisprudence de la CJUE

Dans un arrêt du 6 octobre 2020 (C-511/18, C-512/18 et C-520/18, *La Quadrature du Net et autres*), la Cour de justice a posé 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* »

. Se référant à la directive du 12 juillet 2002, telle que modifiée par la directive 2009/136/CE, du 25 novembre 2009, elle a ajouté que « 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 ».

Et également que, « 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 de connexion, pour une période temporellement limitée au strict nécessaire ; une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs des 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 [...] et que les personnes concernées disposent de garanties effectives contre les risques d'abus ».

Dans un arrêt du 2 mars 2021 (C-746/18), la Cour de justice a, en revanche, précisé que « le droit de l'Union 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 aux données de localisation » ; et, dans un arrêt du 5 avril 2022 (C-140/20), qu'il « en est de même pour un fonctionnaire de police, qui ne constitue pas une juridiction et ne présente pas toutes les garanties d'indépendance et d'impartialité requises ». C'est sur la base de ces principes du droit européen que la Cour de cassation s'est prononcée dans les arrêts du 12 juillet 2022.

Application en droit français

Dans ces arrêts du 12 juillet 2022, la Cour de cassation a dû apprécier la conformité des dispositions du Code des postes et des communications électroniques aux exigences du droit européen.

Code des postes et des communications électroniques

Dans sa version en vigueur au moment des faits, l'article 34-1 du Code des postes et des communications électroniques (CPCE) imposait, aux opérateurs de services de télécommunications électroniques, la

conservation généralisée et indifférenciée, pour une durée maximale d'un an, des données de connexion, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

Arrêts du 12 juillet 2022

Dans les différentes affaires qui ont donné lieu aux arrêts du 12 juillet 2022, les moyens au pourvoi faisaient notamment valoir que *« viole l'article 15 de la directive 2002/58/CE, du 12 juillet 2002 modifiée, lu à la lumière [...] 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 »*.

Se référant à la jurisprudence de la Cour de justice, la Cour de cassation pose que *« seule est admise une conservation généralisée et indifférenciée »* des données personnelles de connexion *« 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 »*.

La Cour de cassation ajoute que, *« 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 des 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 période 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 [...] et que les personnes concernées disposent de garanties effectives contre les risques d'abus »*.

Mention est ainsi faite de ce que *« l'article 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 »*

[...] pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ».

Pour la Cour de cassation, « il résulte des principes » européens « 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 ».

La Cour pose que, « en revanche, l'obligation de conservation des données de trafic et de localisation imposée aux opérateurs [...] 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 [...] est conforme au droit de l'Union, comme poursuivant l'objectif de sauvegarde de la sécurité nationale ».

Considérant que la France se trouvait, à l'époque de certains des faits poursuivis, « 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 », la Cour conclut que « 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 [...] qui ont fait l'objet des réquisitions litigieuses, était conforme au droit de l'Union ».

En revanche, la Cour de cassation considère : que le droit européen « 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 » ; qu'« un fonctionnaire de police ne constitue pas une juridiction et ne présente pas toutes les garanties d'indépendance et d'impartialité requises » ; et que « 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 ». Elle en conclut que les dispositions du Code de procédure pénale en vigueur à cet égard « sont contraires au droit de l'Union » en ce qu'elles « ne prévoient pas un contrôle préalable par une juridiction ou une entité administrative indépendante ».

La Cour estime, en revanche, que « le juge d'instruction est habilité à contrôler l'accès aux données de connexion », car, « d'une part, il n'est pas une partie à la procédure mais une juridiction », et du fait, que « d'autre part, il n'exerce pas l'action publique, mais statue de façon impartiale sur le sort de celle-ci ».

Ainsi interprétées par la Cour de cassation, se référant aux textes de droit européen et à la jurisprudence de la CJUE en la matière, les dispositions qui encadrent la conservation et l'accès aux données de connexion aux services de communications électroniques doivent assurer un équilibre juste et délicat entre, d'un côté, les nécessités de l'action pénale, dans la recherche et la condamnation des auteurs d'infractions et, de

l'autre, la protection de la vie privée des personnes concernées.

Categorie

1. Droit

date créée

6 février 2023

Auteur

emmanuelderieux