Cour de justice de l'Union européenne
COMMUNIQUE DE PRESSE n° 58/22
Luxembourg, le 5 avril 2022

Presse et Information

Arrêt dans l'affaire C-140/20
Commissioner of the Garda Síochána e.a.

La Cour confirme que le droit de l'Union s'oppose à une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation afférentes aux communications électroniques aux fins de la lutte contre les infractions graves

Une juridiction nationale ne peut limiter dans le temps les effets d'une déclaration d'invalidité d'une législation nationale prévoyant une telle conservation

En mars 2015, G.D. a été condamné à une peine de réclusion à perpétuité pour le meurtre d'une femme en Irlande. Dans l'appel formé contre sa condamnation devant la cour d'appel d'Irlande, l'intéressé a notamment reproché à la juridiction de première instance d'avoir, à tort, admis comme éléments de preuve des données relatives au trafic et des données de localisation afférentes à des appels téléphoniques. Afin de pouvoir contester, dans le cadre de la procédure pénale, la recevabilité desdites preuves, G.D. a engagé parallèlement, auprès de la Haute Cour d'Irlande, une procédure civile visant à constater l'invalidité de certaines dispositions de la loi irlandaise de 2011 régissant la conservation de ces données et l'accès à celles-ci, au motif que cette loi violait les droits que lui confère le droit de l'Union. Par décision du 6 décembre 2018, la Haute Cour a fait droit à l'argumentation de G.D. L'Irlande a interjeté appel de cette décision devant la Cour suprême d'Irlande, qui est la juridiction de renvoi dans la présente affaire.

Par son renvoi, la Cour suprême a demandé des éclaircissements sur les exigences du droit de l'Union en matière de conservation desdites données aux fins de la lutte contre les infractions graves ainsi que sur les garanties nécessaires en matière d'accès à ces mêmes données. Elle s'interroge, par ailleurs, sur la portée et l'effet temporel d'une éventuelle déclaration d'incompatibilité qu'elle devrait prononcer, dès lors que la loi irlandaise de 2011 a été adoptée aux fins de transposer la directive 2006/24/CE [1], déclarée invalide par la Cour dans l'arrêt du 8 avril 2014, Digital Rights Ireland e.a. [2].

Dans son arrêt, la Cour, réunie en grande chambre, confirme, en premier lieu, sa jurisprudence constante [3] selon laquelle le droit de l'Union [4] **s'oppose à des mesures législatives nationales prévoyant, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation afférentes aux communications électroniques, aux fins de la lutte contre les infractions graves**.

---

[1] Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54).

[2] Arrêt du 8 avril 2014, Digital Rights Ireland, C-293/12 (voir le CP nº. 54/14).

[3] Arrêts du 8 avril 2014, Digital Rights Ireland, C-293/12, du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15 (voir le CP nº 145/16), du 6 octobre 2020, Privacy International, C-623/17, La Quadrature du Net e.a., C-511/18, C-512/18, Ordre des barreaux francophones et germanophone e.a., C-520/18 (voir le CP nº 123/20), et du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18 (voir le CP n° 29/21).

[4] 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 (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la « directive "vie privée et communications électroniques" »), lue 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 (ci-après la « Charte »).

En effet, la directive vie privée et communications électroniques ne se limite pas à encadrer l'accès à de telles données par des garanties visant à prévenir les abus, mais consacre, en particulier, le **principe de l'interdiction du stockage** des données relatives au trafic et à la localisation. La conservation de ces données constitue ainsi, d'une part, une dérogation à cette interdiction de stockage et, d'autre part, une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte.

Si la directive vie privée et communications électroniques permet aux États membres de limiter ces droits et ces obligations aux fins notamment de la lutte contre les infractions pénales, de telles limitations doivent toutefois notamment respecter le principe de proportionnalité. Ce principe requiert le respect non seulement des exigences d'aptitude et de nécessité, mais également de celle ayant trait au **caractère proportionné** de ces mesures par rapport à l'objectif poursuivi. Ainsi, la Cour a déjà jugé que l'objectif de lutte contre la criminalité grave, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, telle que celle instaurée par la directive 2006/24, soit considérée comme nécessaire. Dans le même ordre d'idées, même les obligations positives des États membres sur la mise en place de règles permettant une lutte effective contre les infractions pénales ne sauraient avoir pour effet de justifier des ingérences aussi graves que celles que comporte une législation nationale prévoyant une telle conservation dans les droits fondamentaux de la quasi-totalité de la population, sans que les données des personnes concernées soient susceptibles de révéler un lien, au moins indirect, avec l'objectif poursuivi.

La Cour rappelle encore que différentes obligations positives sont à la charge des pouvoirs publics en vertu de la Charte, consistant, par exemple, dans l'adoption de mesures juridiques visant à protéger la vie privée et familiale, la protection du domicile et des communications, mais aussi la protection de l'intégrité physique et psychique des personnes ainsi que l'interdiction de la torture et des traitements inhumains et dégradants. Il leur appartient dès lors de procéder à une **conciliation des différents intérêts légitimes et droits en cause**. En effet, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, et ce en effectuant une **pondération équilibrée** entre, d'une part, cet objectif d'intérêt général et, d'autre part, les droits en cause, tout en vérifiant que l'importance dudit objectif est en relation avec la gravité de l'ingérence que comporte cette mesure.

Ces considérations amènent la Cour à rejeter notamment l'argumentation selon laquelle la criminalité particulièrement grave pourrait être assimilée à une menace pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible et peut, pendant une durée limitée, justifier une mesure de conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En effet, une telle menace se distingue, par sa nature, sa gravité et le caractère spécifique des circonstances qui la constituent, du risque général et permanent qu'est celui de survenance de tensions ou de troubles, même graves, à la sécurité publique ou celui d'infractions pénales graves.

En revanche, la Cour juge, en second lieu et en confirmant sa jurisprudence antérieure, que le droit de l'Union ne s'oppose pas à des mesures législatives prévoyant, dans les conditions énoncées dans son arrêt, aux fins 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** en fonction de catégories de personnes concernées ou au moyen d'un critère géographique ;

- **une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion** ;

- **une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques**, et

- une **conservation** rapide (*quick freeze*) des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services.

La Cour apporte diverses précisions concernant ces différentes catégories de mesures.

Tout d'abord, les autorités nationales compétentes peuvent prendre une mesure de conservation ciblée fondée sur un critère géographique, tel que notamment le taux moyen de criminalité dans une zone géographique donnée, sans qu'elles disposent nécessairement d'indices concrets portant sur la préparation ou la commission, dans les zones concernées, d'actes de criminalité grave. Elle ajoute qu'une telle mesure de conservation visant des lieux ou des infrastructures fréquentés régulièrement par un nombre très élevé de personnes ou des lieux stratégiques, tels que des aéroports, des gares, des ports maritimes ou des zones de péages, est susceptible de permettre aux autorités compétentes d'obtenir des informations sur la présence, dans ces lieux ou zones géographiques, des personnes y utilisant un moyen de communication électronique et d'en tirer des conclusions sur leur présence et leur activité dans lesdits lieux ou zones géographiques aux fins de la lutte contre la criminalité grave.

Ensuite, la Cour indique que ni la directive vie privée et communications électroniques ni aucun autre acte du droit de l'Union ne s'opposent à une législation nationale, ayant pour objet la lutte contre la criminalité grave, en vertu de laquelle l'acquisition d'un moyen de communication électronique, tel qu'une carte SIM prépayée, est subordonnée à la vérification de documents officiels établissant l'identité civile de l'acheteur et à l'enregistrement, par le vendeur, des informations en résultant, le vendeur étant le cas échéant tenu de donner accès à ces informations aux autorités nationales compétentes.

Enfin, la Cour relève que la directive vie privée et communications électroniques ne s'oppose pas à ce que les autorités nationales compétentes ordonnent une mesure de conservation rapide dès le premier stade de l'enquête portant sur une menace grave pour la sécurité publique ou sur un éventuel acte de criminalité grave, à savoir à partir du moment auquel ces autorités peuvent, selon les dispositions pertinentes du droit national, ouvrir une telle enquête. 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 ou une atteinte à la sécurité nationale, pour autant que ces données puissent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci ainsi que celles de son entourage social ou professionnel.

Ces différentes mesures peuvent, selon le choix du législateur national et tout en respectant les limites du strict nécessaire, trouver à s'appliquer conjointement.

La Cour rejette encore l'argumentation selon laquelle les autorités nationales compétentes devraient pouvoir accéder, aux fins de la lutte contre la criminalité grave, aux données relatives au trafic et aux données de localisation qui ont été conservées de manière généralisée et indifférenciée, conformément à sa jurisprudence, pour faire face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. En effet, cette argumentation fait dépendre cet accès de circonstances étrangères à l'objectif de lutte contre la criminalité grave. En outre, selon ladite argumentation, l'accès pourrait être justifié par un objectif d'une importance moindre que celui ayant justifié la conservation, à savoir la sauvegarde de la sécurité nationale, ce qui irait à l'encontre de la hiérarchie des objectifs d'intérêt général dans le cadre de laquelle doit s'apprécier la proportionnalité d'une mesure de conservation. Par ailleurs, autoriser un tel accès risquerait de priver de tout effet utile l'interdiction de procéder à une conservation généralisée et indifférenciée aux fins de la lutte contre la criminalité grave.

En troisième lieu, la Cour confirme que droit de l'Union s'oppose à une législation nationale en vertu de laquelle le traitement centralisé des demandes d'accès à des données conservées par les fournisseurs de services de communications électroniques, émanant de la police dans le cadre de la recherche et de la poursuite d'infractions pénales graves, incombe à un fonctionnaire de police, même lorsque celui-ci est assisté par une unité instituée au sein de la police jouissant d'un certain

degré d'autonomie dans l'exercice de sa mission et dont les décisions peuvent faire ultérieurement l'objet d'un contrôle juridictionnel. La Cour confirme en effet, à cet égard, sa jurisprudence selon laquelle, afin de garantir, en pratique, le plein respect des conditions strictes d'accès à des données à caractère personnel telles que les données relatives au trafic et à la localisation, l'accès des autorités nationales compétentes aux données conservées doit être subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, la décision de cette juridiction ou de cette entité devant intervenir à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales. Or, un fonctionnaire de police ne constitue pas une juridiction et ne présente pas toutes les garanties d'indépendance et d'impartialité requises pour pouvoir être qualifié d'entité administrative indépendante.

En quatrième lieu, la Cour confirme sa jurisprudence selon laquelle le droit de l'Union s'oppose à ce qu'une juridiction nationale limite dans le temps les effets d'une déclaration d'invalidité qui lui incombe, en vertu du droit national, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en raison de l'incompatibilité de cette législation avec la directive vie privée et communications électroniques.

Cela étant, la Cour rappelle que l'admissibilité des éléments de preuve obtenus au moyen d'une telle conservation relève, conformément au principe d'autonomie procédurale des États membres, du droit national, sous réserve du respect notamment des principes d'équivalence et d'effectivité.

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.

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