Cour de justice de l'Union européenne
COMMUNIQUE DE PRESSE n° 29/21
Luxembourg, le 2 mars 2021

Presse et Information

Arrêt dans l'affaire C-746/18
H. K/Prokuratuur

L'accès, à des fins pénales, à un ensemble de données de communications électroniques relatives au trafic ou à la localisation, permettant de tirer des conclusions précises sur la vie privée, n'est autorisé qu'en vue de lutter contre la criminalité grave ou de prévenir des menaces graves contre la sécurité publique

Le droit de l'Union s'oppose par ailleurs à une réglementation nationale donnant compétence au ministère public pour autoriser l'accès d'une autorité publique à ces données afin de mener une instruction pénale

Une procédure pénale a été engagée en Estonie contre H. K. des chefs de vol, d'utilisation de la carte bancaire d'un tiers et de violence à l'égard de personnes participant à une procédure en justice. H. K. a été condamnée pour ces infractions par un tribunal de première instance à une peine privative de liberté de deux ans. Cette décision a ensuite été confirmée en appel.

Les procès-verbaux sur lesquels s'appuie la constatation de ces infractions ont été établis, notamment, sur la base de données à caractère personnel générées dans le cadre de la fourniture de services de communications électroniques. La Riigikohus (Cour suprême, Estonie), devant laquelle un pourvoi en cassation a été introduit par H. K., a émis des doutes quant à la compatibilité avec le droit de l'Union [1] des conditions dans lesquelles les services d'enquête ont eu accès à ces données.

Ces doutes concernent, en premier lieu, la question de savoir si la durée de la période pour laquelle les services d'enquête ont eu accès aux données constitue un critère permettant d'évaluer la gravité de l'ingérence que constitue cet accès dans les droits fondamentaux des personnes concernées. Ainsi, lorsque cette période est très brève ou que la quantité de données recueillies est très limitée, la juridiction de renvoi s'est interrogée sur le fait de savoir si l'objectif de lutte contre la criminalité en général, et pas seulement de lutte contre la criminalité grave, est susceptible de justifier une telle ingérence. En second lieu, la juridiction de renvoi a nourri des doutes quant à la possibilité de considérer le ministère public estonien, compte tenu des différentes missions qui lui sont confiées par la réglementation nationale, comme une autorité administrative « indépendante » au sens de l'arrêt Tele2 Sverige et Watson e.a. [2], susceptible d'autoriser l'accès de l'autorité chargée de l'enquête aux données concernées.

Par son arrêt, prononcé en grande chambre, la Cour juge que la directive « vie privée et communications électroniques », lue à la lumière de la Charte, s'oppose à une réglementation nationale permettant l'accès des autorités publiques à des données relatives au trafic ou à des données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des

[1] Plus précisément, avec 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 (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" »), 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 (ci-après la « Charte »).

[2] Arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a., C-203/15 et C-698/15 point 120 ; voir également communiqué de presse n°145/16.

équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique. Selon la Cour, la durée de la période pour laquelle l'accès à ces données est sollicité et la quantité ou la nature des données disponibles pour une telle période n'ont pas d'incidence à cet égard. En outre, la Cour considère que cette même directive, lue à la lumière de la Charte, s'oppose à une réglementation nationale donnant compétence au ministère public pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation afin de mener une instruction pénale.

Appréciation de la Cour

S'agissant des conditions dans lesquelles l'accès aux données relatives au trafic et aux données de localisation conservées par les fournisseurs de services de communications électroniques peut, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, être accordé à des autorités publiques, en application d'une mesure prise au titre de la directive « vie privée et communications électroniques » [3], la Cour rappelle ce qu'elle a jugé dans son arrêt La Quadrature du Net e.a. [4]. Ainsi, cette directive n'autorise les États membres à adopter, entre autres à ces fins, des mesures législatives visant à limiter la portée des droits et des obligations prévus par cette directive, notamment l'obligation de garantir la confidentialité des communications et des données relatives au trafic [5], que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte [6]. Dans ce cadre, la directive s'oppose à des mesures législatives imposant aux fournisseurs de services de communications électroniques, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

En ce qui concerne l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, poursuivi par la réglementation en cause, conformément au principe de proportionnalité, la Cour considère que seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'accès des autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de permettre de tirer des conclusions précises sur la vie privée des personnes concernées, sans que d'autres facteurs tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès.

S'agissant de la compétence donnée au ministère public pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation afin de diriger une instruction pénale, la Cour rappelle qu'il appartient au droit national de déterminer les conditions dans lesquelles les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données dont ils disposent. Toutefois, pour satisfaire à l'exigence de proportionnalité, une telle réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et indiquer en quelles circonstances et sous quelles conditions matérielles et procédurales une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire.

Selon la Cour, aux fins de garantir, en pratique, le plein respect de ces conditions, il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit subordonné à un

---

[3] Article 15, paragraphe 1, de la directive « vie privée et communications électroniques ».
[4] Arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, points 166 à 169 ; voir également communiqué de presse n°123/20.
[5] Article 5, paragraphe 1, de la directive « vie privée et communications électroniques ».
[6] En particulier, les articles 7, 8 et 11 ainsi que l'article 52, paragraphe 1, de la Charte.

contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité intervienne 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. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais.

À cet égard, la Cour précise que le contrôle préalable requiert, entre autres, que la juridiction ou l'entité chargée d'effectuer ce contrôle dispose de toutes les attributions et présente toutes les garanties nécessaires en vue d'assurer une conciliation des différents intérêts et droits en cause. S'agissant plus particulièrement d'une enquête pénale, un tel contrôle exige que cette juridiction ou cette entité soit en mesure 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 et, d'autre part, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel des personnes dont les données sont concernées par l'accès. Lorsque ce contrôle est effectué non par une juridiction mais par une entité administrative indépendante, celle-ci doit jouir d'un statut lui permettant d'agir, lors de l'exercice de ses missions, de manière objective et impartiale et doit être, à cet effet, à l'abri de toute influence extérieure.

D'après la Cour, il en résulte que l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale. Or, tel n'est pas le cas d'un ministère public qui, comme c'est le cas du ministère public estonien, dirige la procédure d'enquête et exerce, le cas échéant, l'action publique. Il s'ensuit que le ministère public n'est pas en mesure d'effectuer le contrôle préalable susmentionné.

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 : Antoine Briand ☎ (+352) 4303 3205.