La CJUE limite la surveillance rétroactive à la lutte contre la criminalité grave

Kastriot Lubishtani, le 30 mars 2021

Le droit de l'Union européenne s'oppose à une réglementation nationale permettant une surveillance rétroactive ou l'accès d'autorités publiques aux données secondaires conservées par les fournisseurs de services de télécommunications électroniques pour toute procédure pénale. Il l'autorise néanmoins pour les procédures concernant la lutte contre la criminalité grave ou la prévention de menaces graves.

Arrêt CJUE C-746/18 du 2 mars 2021

Accusé d'avoir commis plusieurs vols, utilisé la carte bancaire d'une tierce personne pour retirer de l'argent à un bancomat et violenté une autre personne, H. K. est condamné à une peine privative de liberté de deux ans par un tribunal de première instance estonien. Les faits sont établis à l'aide d'une surveillance rétroactive ou des données secondaires de télécommunication qui ont été obtenues par les autorités de poursuite auprès d'un fournisseur estonien de services de télécommunications électroniques.

Devant le tribunal d'appel, puis la Cour suprême nationale, H. K. conteste la recevabilité de ces moyens de preuve et la conformité du droit estonien au droit européen. La Cour suprême estonienne saisit ainsi la Cour de justice de l'Union européenne d'une demande de décision préjudicielle au sujet de l'interprétation de l'art. 15 Directive 2002/58/CE vie privée et communications électroniques (Directive ePrivacy). Se pose en particulier la question de savoir si les données secondaires de télécommunication peuvent être utilisées dans toutes les procédures pénales ou si elles ne doivent l'être que dans certaines d'entre elles.

La Directive 2002/58/CE vise à garantir les droits fondamentaux au respect de la vie privée (art. 7) et la protection des données à caractère personnel (art. 8) protégés par la Charte des droits fondamentaux de l'Union. Des restrictions aux droits prévus par la Directive sont autorisées en vertu de l'art. 15 ch. 1 :

> « 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 ou d'utilisations non autorisées du système de communications électroniques [...]. 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 dans le présent paragraphe ».

Se référant à sa jurisprudence La Quadrature du Net, la CJUE énonce des lignes directrices au sujet de l'interprétation de l'art. 15 par. 1 Directive 2002/58/CE.

Tout d'abord, l'accès par des autorités publiques aux fins de la prévention, de l'élucidation et de la poursuite d'infractions pénales à des données relatives au trafic et de localisation n'est possible que si ces dernières ont été conservées par des fournisseurs de services de télécommunications électroniques de manière conforme à l'art. 15 ch. 1 précité, lequel s'oppose à une réglementation prévoyant une conservation généralisée et indifférenciée de ces données.

Ensuite, l'accès à ces données et la restriction aux droits protégés par la Directive ne peuvent être justifiés que par le même objectif d'intérêt général ayant contraint les fournisseurs à les conserver. Ce motif justificatif doit être apprécié « en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité ».

La CJUE rappelle que des ingérences graves aux art. 7 et 8 de la Charte de l'Union ne sont admissibles qu'aux fins de la lutte contre la criminalité grave et la prévention de menaces graves contre la sécurité publique. La conservation de données relatives au trafic et de localisation et leur accès par des autorités publiques sont précisément des ingérences graves, étant donné que ce traitement permet de tirer des conclusions précises sur la vie des personnes concernées. Par contre, ne relèvent en principe pas de ce niveau de gravité les mesures législatives visant le traitement de données relatives à l'identité civile uniquement des utilisateurs de moyens de télécommunications, car elles ne permettent de tirer aucune conclusion sur les communications et ainsi sur la vie privée. D'autres facteurs relatifs à la proportionnalité, comme la durée de la période couverte par l'accès des autorités publiques et donc la quantité, ne sont pas déterminants à cet égard.

En l'espèce, l'art. 111 du Code de procédure pénale estonien fait obligation aux fournisseurs de services de télécommunications électroniques de conserver pendant une année les

données secondaires, à savoir notamment celles se rapportant à la source et la destination d'une communication (numéro, nom et adresse de l'appelant et de l'appelé), la date, le début et la fin de l'appel, ainsi que la localisation de l'appareil de téléphonie. Ces données sont accessibles au ministère public selon une procédure d'autorisation aux fins de l'instruction pénale.

Grâce à cette disposition, les autorités publiques estoniennes peuvent accéder à un ensemble de données qui leur permet de tirer des « conclusions précises, voire très précises » au sujet de la vie privée des personnes concernées. En effet, ces données permettent de déterminer leurs habitudes de vie quotidienne, mais aussi leurs déplacements journaliers, leurs relations sociales, mais aussi les milieux sociaux fréquentés, ainsi que leurs lieux de séjour.

Ainsi, il s'agit d'une ingérence grave aux droits consacrés par la Charte de l'Union, cela nonobstant l'étendue temporelle de l'accès de l'autorité et de la quantité ou de la nature des données disponibles pour une telle période. Même l'accès à une courte période ou à une quantité limitée de données concernant le trafic ou la localisation est susceptible de fournir des informations précises sur la vie privée des personnes concernées.

Enfin, la CJUE constate que le droit estonien autorise l'accès à ces données pour tout type d'infraction pénale et que, par conséquent, cette ingérence n'est pas limitée dans le cas présent à la lutte contre la criminalité grave.

En conclusion, l'art. 15 par. 1 Directive 2002/58/CE, interprété à la lumière des art. 7 et 8 de la Charte de l'Union, s'oppose à une réglementation nationale permettant l'accès d'autorités publiques aux données secondaires conservées par les fournisseurs de services de télécommunications électroniques pour toute procédure pénale. Une surveillance rétroactive est toutefois autorisée pour les procédures pénales qui concernent exclusivement la lutte contre la criminalité grave ou la prévention de menaces graves.

Cet arrêt opère une pesée des intérêts entre la sécurité d'une part et le droit au respect de la vie privée et la protection des données d'autre part, en accordant à ces derniers une importance accrue, ce qu'il convient de saluer.

Il permet de mettre en lumière la différence d'appréciation à cet égard entre les autorités européennes et suisses au travers de la jurisprudence helvétique au sujet de l'interprétation de l'art. 273 du Code de procédure pénale. Cette disposition prévoit que les données secondaires peuvent être obtenues par le ministère public pour une surveillance rétroactive pour

tout « crime », tout « délit » ou encore toute « contravention au sens de l'art. 179septies CP », à la condition toutefois, par renvoi à l'art. 269 CPP, que cette mesure se justifie au regard « de la gravité de l'infraction » (al. 1 let. b) et que « les mesures prises jusqu'alors dans le cadre de l'instruction sont restées sans succès ou [que] les recherches n'auraient aucune chance d'aboutir ou seraient excessivement difficiles » (al. 1 let. c).

La référence aux notions de « crime » et de « délit » n'est pas véritablement restrictive, dès lors qu'elle permet en théorie au ministère public d'accéder aux données secondaires pour tout un éventail de comportements plus ou moins graves. La seule et véritable cautèle se trouve donc dans la nature « grave » que doit revêtir l'infraction en cause au sens de l'art. 269 al. 1 let. b CPP. Or MÉTILLE a mis en évidence l'interprétation très large qu'en fait le Tribunal fédéral, en retenant une gravité telle qu'elle justifie de recourir à une surveillance rétroactive au sens de l'art. 273 CPP pour un excès de vitesse sur la route, une fois de 29 km/h dans une zone limitée à 50 km/h (TF, 1B_206/2016 du 5.7.2016) et une autre fois de 25 km/h dans une zone limitée à 60 km/h (TF, 1B_235/2016 du 20.7.2016).

En outre, le projet de révision du Code de procédure pénale actuellement en discussion à l'Assemblée fédérale n'apporte pas une restriction plus sévère à l'art. 273 CPP et ne devrait rien changer de ce point de vue, sauf modification législative émanant directement des parlementaires.

En définitive, le Tribunal fédéral et le droit suisse plus généralement apparaissent moins protecteurs que le droit européen vis-à-vis du droit au respect de la vie privée garanti par l'art. 13 de la Constitution fédérale dans le contexte de procédures pénales.

Proposition de citation : Kastriot LUBISHTANI, La CJUE limite la surveillance rétroactive à la lutte contre la criminalité grave, 30 mars 2021 *in* www.swissprivacy.law/66