_swissprivacy.law

Utilisation de données de communications dans les enquêtes pénales

Alexandre Barbey, le 31 mai 2022

La conservation généralisée et indifférenciée de données liées à des communications n'est possible que dans le but de sauvegarder la sécurité nationale. S'il s'agit de lutter contre la criminalité grave, seule une conservation ciblée et délimitée par des critères objectifs et non discriminatoires est autorisée.

Arrêt de la Cour de justice de l'Union européenne du 5 avril 2022 dans l'affaire C-140/20

L'arrêt du 5 avril 2022 de la Cour de justice de l'Union européenne (CJUE) donne un cadre juridique clair sur l'utilisation qui peut être faite dans une procédure pénale de données relatives au trafic téléphonique et de localisation s'y rapportant.

L'affaire débute lorsqu'une personne condamnée pour meurtre par les autorités irlandaises conteste la validité d'une loi nationale transposant une version modifiée de la Directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Plusieurs questions relatives à l'interprétation du texte européen sont posées à la CJUE.

La Directive 2002/58 pose en particulier le principe de la confidentialité des communications effectuées sur un réseau public et des données s'y rapportant. Uniquement les utilisateurs du réseau doivent pouvoir avoir accès aux communications, par opposition à des tiers, qui ne le peuvent pas, de quelle que manière que ce soit. Des tiers ne doivent notamment pas pouvoir intercepter et enregistrer les communications (art. 5 par. 1 Directive 2002/58). De plus, les fournisseurs d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent avoir effacé ou rendu anonymes les données relatives au trafic concernant les utilisateurs lorsqu'elles ne sont plus nécessaires, notamment après la transmission des communications, l'établissement de factures, la fourniture de services à valeur ajoutée ou encore la détection de fraudes. Les données de localisation liées aux communications ne doivent être traitées qu'après avoir été anonymisées. Cependant, si la personne a donné son consentement, il n'y a pas besoin d'anonymisation (art. 6 par. 1 et 9 par. 1 Directive 2002/58).

L'art. 15 par. 1 Directive 2002/58 permet toutefois aux États membres de l'Union européenne

de limiter la portée de ces droits et obligations lorsque cela s'avère proportionnel pour sauvegarder la sécurité nationale, la défense et la sécurité publique ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.

La CJUE examine tout d'abord si les États membres peuvent transposer la Directive 2002/58 dans une loi autorisant une conservation généralisée et indifférenciée des données de trafic et de localisation à des fins de lutte contre la criminalité grave. Le principe de la Directive 2002/58 est qu'il est interdit à des personnes autres que les utilisateurs de stocker ces données. L'art. 15 Directive 2002/58, qui permet une certaine dérogation au principe, doit être interprété de manière stricte dans le sens que la restriction ne doit pas devenir la règle, mais doit répondre à l'un des objectifs décrits à cette disposition. De plus, toute limitation des droits et obligations doit se conformer à la Charte des droits fondamentaux de l'Union européenne, notamment le droit au respect de la vie privée et le droit à la protection des données personnelles (art. 7 et 8 Charte). De ce point de vue, la conservation de données de trafic et de localisation pose problème, car celles-ci révèlent de nombreuses informations sensibles à propos des personnes concernées, permettant de créer un profil de la personnalité. La CJUE constate qu'une conservation généralisée et indifférenciée de telles données engendre un risque d'abus et d'accès illicite (cf. arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18).

Dès lors que des droits fondamentaux sont concernés, la CJUE indique, en se fondant sur la jurisprudence de la Cour européenne des droits de l'Homme (voir notamment arrêt CourEDH *Big Brother Watch et autres contre Royaume-Uni* du 25 mai 2021, résumé *in* LawInside.ch/1063/), que des obligations positives à charge des États peuvent découler des droits fondamentaux consacrés par la Charte. Ces obligations impliquent l'adoption de dispositions permettant de lutter efficacement contre la criminalité. Ces dernières doivent toutefois poser un cadre légal clair qui permet de concilier les différents intérêts légitimes et les droits à protéger. Il s'agit donc de déroger aux droits fondamentaux de certaines personnes pour protéger ceux d'autres.

La CJUE souligne que les États membres doivent prévoir des règles claires et précises pour déroger à des droits fondamentaux, de manière à ce 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 ». Le principe de la proportionnalité doit être respecté, le but de la dérogation aux droits fondamentaux étant la lutte contre la criminalité grave. Au niveau de l'aptitude, les données conservées doivent donc permettre de prévenir, de détecter ou de poursuivre des infractions graves. Des ingérences graves dans

les droits fondamentaux ne sont possibles que dans le but de lutter contre des infractions graves.

La CJUE distingue deux buts de l'art. 15 par. 1 Directive 2002/58 permettant de limiter certains droits et obligations de cette Directive.

D'une part, l'objectif de sauvegarde de la sécurité nationale est le plus important. Il s'agit de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société, en particulier en luttant contre le terrorisme. S'il s'agit du but visé, il permet les ingérences les plus grandes dans les droits fondamentaux d'autrui. Ainsi, il est possible dans ce cas que la législation nationale permette d'ordonner aux fournisseurs de services de télécommunications, pendant une période limitée, mais renouvelable, de procéder à une conservation *généralisée* et *indifférenciée* des données de trafic et de localisation lorsqu'une menace grave pour la sécurité nationale est réelle, actuelle ou prévisible. Cette décision doit pouvoir faire l'objet d'un réexamen.

D'autre part, si l'objectif est de lutter contre la criminalité grave, seule une conservation *ciblée* des données et *délimitée* par des critères objectifs et non discriminatoires est possible. Par exemple, les États membres peuvent ordonner la conservation des données relatives à des personnes faisant l'objet d'une enquête ou d'autres mesures de surveillance actuelles ou dont le casier judiciaire indique une condamnation pour des actes de criminalité grave pouvant impliquer un risque élevé de récidive. Les données peuvent également être conservées lorsqu'elles se rapportent à un lieu géographique déterminé de manière objective et non discriminatoire se trouvant être le théâtre d'un nombre élevé d'actes de criminalité grave.

Les autorités peuvent également conserver de manière généralisée et indifférenciée les adresses IP, également pour une période temporellement limitée au strict nécessaire, les données relatives à l'identité civile des utilisateurs.

La CJUE indique en outre que, à la fois pour lutter contre la criminalité grave et pour sauvegarder la sécurité nationale, les États membres de l'Union européenne peuvent adopter une législation nationale leur permettant de prendre des décisions pour que les données de trafic et de localisation soient stockées par les fournisseurs de services de communications au-delà du délai légal après lequel celles-ci doivent être anonymisées, pour une durée déterminée. Les données concernant d'autres personnes que le prévenu, telles la victime et des personnes de son entourage, peuvent être conservées, dans la limite du strict nécessaire.

Enfin, l'accès à de telles données par les autorités compétentes, en particulier la police, doit faire l'objet d'une procédure stricte. La demande doit être motivée et un contrôle, juridictionnel ou administratif indépendant, préalable à l'accès doit exister. La Cour précise que ce contrôle ne peut pas être effectué par un ministère public.

L'arrêt analysé contient des règles claires sur l'utilisation qui peut être faite des données liées aux communications. Il rappelle l'importance des droits fondamentaux des personnes concernées et met l'accent sur la mise en balance des intérêts, nécessaire et préalable à toute conservation ou utilisation de ces données.

En droit suisse, la LSCPT (RS 780.1) est la base légale régissant la surveillance des télécommunications. Une surveillance peut être mise en place dans le cadre d'une procédure pénale (art. 1er al. 1 let. a LSCPT). Le Service de surveillance, une institution fédérale autonome, est chargé de la surveillance et exploite un système informatique de traitement de données (art. 3 et 6 LSCPT). Il fournit les renseignements demandés aux autorités compétentes et les fournisseurs de services de communications sont tenus de collaborer (art. 15, 21 ss et 26ss LSCPT). L'ordonnance mettant en application la loi fait actuellement l'objet d'une révision, commentée dans swissprivacy/135.

Proposition de citation : Alexandre Barbey, Utilisation de données de communications dans les enquêtes pénales, 31 mai 2022 *in* www.swissprivacy.law/148