COUR DE CASSATION

AVIS ORAL DE M. PETIPREZ, AVOCAT GÉNÉRAL

Arrêts n° 769, 771, 772 et 774 du 12 juillet 2022 – Chambre criminelle

Pourvois n° 21-83.710, 21-83.729, 21-84.096 et 21-83.820

Conclusions de Philippe Petitprez, avocat général

Audience de formation mixte du 19 mai 2022

Il me revient de conclure oralement sur la question spécifique de la conservation des données de connexion telle que posée par les pourvois n° 702 à 704 au rapport de Mmes Sylvie Ménotti et Pascale Labrousse (Dossiers Y2183710, U2183729, T2183820 et T2184096).

Pour aller à l'essentiel, mes observations n'auront trait qu'aux données de trafic et de localisation, c'est à dire les données générées par l'utilisation des réseaux de communication électroniques, soit les contacts d'une personne, la date l'heure et la durée des échanges ainsi que les données qui résultent du bornage d'un appareil par l'antenne relais à laquelle il s'est connecté.

Rappelons que la Cour de justice de l'Union européenne interprétant les dispositions de la directive 2002/58 dite vie privée et communication électronique, a posé dans les arrêts Télé 2, Quadrature du net et plus récemment Commissioner of An Garda Siochana, le principe de la prohibition du stockage généralisé et indifférencié de ces données par les opérateurs, pour les besoins de la lutte contre la criminalité.

L'idée qui est au cœur de la jurisprudence de la Cour de Justice est celle que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent anonymes et ne puissent pas faire l'objet d'un enregistrement, sauf s'ils y consentent.

Ces prescriptions donnent lieu à un régime plus rigoureux et plus strict que celui qui ressort de la jurisprudence de la Cour européenne des droits de l'homme. En effet, il n'apparaît pas qu'à ce jour, la Cour EDH, qui se contente d'un seuil de protection minimal, ait jugé contraire à l'article 8 de la Convention, la conservation de ces données par les opérateurs de téléphonie, pour les besoins de la prévention et de la répression des infractions.

Etant rappelé que les droits fondamentaux garantis par la CEDH font partie du droit de l'Union en tant que principes généraux, il nous apparaît que les moyens qui invoquent l'article 8 de la Convention doivent être réunis à ceux qui critiquent la conservation des données sur le fondement du droit de l'Union.

Les décisions de la Cour de justice et particulièrement l'arrêt Quadrature du net du 6 octobre 2020, intervenu sur questions préjudicielles posées par le Conseil d'Etat et la Cour constitutionnelle belge, ont eu des répercussions importantes en droit interne.

Les conséquences des réponses aux questions préjudicielles ont été tirées par le Conseil d'Etat, dans son arrêt French Data Network du 21 avril 2021, puis par le législateur qui a modifié l'article L. 34-1 du code des postes et communications électroniques qui, de fait, imposait aux opérateurs de conserver de façon généralisée et indifférenciée, pendant un an, les données de trafic et de localisation de l'ensemble de leurs utilisateurs, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

Par décision du 25 février 2022, le Conseil constitutionnel a lui-même jugé que les dispositions de cet article L. 34-1, dans sa version ancienne, portaient une atteinte disproportionnée au droit au respect de la vie privée et devaient être déclarées contraires à la Constitution. Il a toutefois différé l'entrée en vigueur de cette déclaration d'inconstitutionnalité.

Les autres états membres n'ont pas encore tiré toutes les conséquences des arrêts de la CJUE. A l'exception des Pays-Bas qui ont opté pour la solution radicale de ne plus imposer aucun stockage de données aux opérateurs, mais également de la Belgique et de l'Autriche qui connaissent le système de gel rapide des données disponibles, sur lequel je reviendrai, des réflexions sont toujours en cours, notamment en Allemagne, pays qui a adressé à la Cour de justice de nouvelles questions préjudicielles, actuellement pendantes.

J'ajoute que la Cour de justice doit encore apporter des réponses aux questions que vous avez posées par deux arrêts du 1er avril 2020, portant sur l'articulation entre la directive vie privée et les textes de l'Union européenne relatifs aux abus de marché, appelant les Etats membres à instaurer des dispositifs de conservation de données de

connexion permettant aux autorités administratives d'apporter la preuve d'opérations d'initiés ou de manipulations de marché et d'en identifier les auteurs.

L'interdiction de stockage des données, énoncée par la CJUE n'est pas absolue. La Cour admet en effet plusieurs exceptions :

Il s'agit d'abord des données conservées par les opérateurs pour leurs propres besoins, c'est à dire à des fins commerciales ou, par extension, pour assurer la sécurité des réseaux.

Cette dérogation trouve sa transposition aujourd'hui comme hier dans les article L. 34-1 et R. 10-14 du CPCE. La conservation des données pour les nécessités de la facturation et du paiement des prestations est autorisée pendant un an, c'est à dire jusqu'à la fin de la période pendant laquelle la facture peut être contestée tandis que certaines données peuvent être conservées pendant trois mois pour la sécurité des réseaux et des installations.

Deuxième exception admise par la Cour de justice : La conservation généralisée et indifférenciée des données de trafic et de localisation peut être justifiée par l'objectif de sauvegarde de la sécurité nationale, autrement dit, dans l'esprit de la Cour, à des fins de lutte contre le terrorisme et contre les atteintes aux intérêts fondamentaux de la nation.

Une telle conservation est cependant assortie de plusieurs conditions, dont deux sont essentielles : La menace doit s'avérer réelle et actuelle ou prévisible et la conservation ne peut être prescrite que pour une durée limitée.

La troisième exception est relative aux mesures de conservation que les Etats peuvent adopter afin de lutter contre la criminalité grave et de prévenir des menaces graves contre la sécurité publique que l'on peut classer en deux catégories :

- Il s'agit, pour la première, de la conservation ciblée des données de connexion sur la base de critères géographiques tel que le taux de criminalité ou le caractère sensible de certains lieux comme les aéroports, les gares etc. ou encore en fonction de catégories de personnes, par exemple celles faisant l'objet de mesures de surveillance ou de condamnations inscrites au casier judiciaire.

Il est permis de s'interroger, comme l'a fait le Conseil d'Etat sur l'efficacité de ces dispositifs ou encore leur conformité avec le principe constitutionnel d'égalité devant la loi, mais ce n'est pas l'objet de l'audience d'aujourd'hui.

- L'autre mesure préconisée réside dans la conservation dite rapide des données qui a un champ plus large que la conservation ciblée et qui peut intervenir quel que soit le stade de l'enquête. La Cour de justice se réfère ici au mécanisme autonome issu de la Convention de Budapest du 23 novembre 2001 sur la cybercriminalité, ratifiée par la France, qui permet aux Etats de requérir, dans le cadre d'une enquête pénale, le gel

temporaire des données stockées par les opérateurs afin de permettre aux autorités compétentes d'obtenir ensuite leur divulgation.

Si la Convention de Budapest recommande aux Etats d'instaurer dans leur législation une phase d'injonction de conservation des données puis une phase d'obtention de ces données auprès des opérateurs, elle introduit une certaine souplesse puisqu'elle n'impose pas de prévoir impérieusement une phase préalable de gel des données.

Dans le cadre des procédures soumises à votre examen, vous ne pourrez que tirer les conséquences des arrêts de la Cour de justice et, contrairement à la position défendue par les chambres de l'instruction, vous écarterez nécessairement comme contraires au droit de l'Union les dispositions de l'article L. 34-1 du CPCE dans leur ancienne rédaction.

Vous constaterez dès lors qu'à la date des réquisitions litigieuses, aucun dispositif de notre droit ne permettait d'imposer aux opérateurs de conserver les données de connexion aux fins de lutte contre la criminalité.

Ceci dit, si la non-conformité est certaine, sa portée doit être relativisée puisque nous vous proposons de retenir, à la suite du Conseil d'Etat, que la conservation généralisée et indifférenciée des données pouvait être imposée aux opérateurs dans des conditions conformes au droit de l'Union, pour des motifs de sauvegarde de la sécurité nationale.

Cette possibilité est aujourd'hui inscrite dans notre législation puisque, depuis la loi du 30 juillet 2021, l'article L. 34-1 du CPCE prévoit qu'un impératif de sauvegarde de la sécurité nationale, en cas de menace grave, actuelle ou prévisible, permet sur injonction du premier ministre et pour une durée maximale d'un an renouvelable la conservation généralisée et indifférenciée de données de trafic et de localisation.

Le même article dispose pour l'avenir que, dans le cadre de la criminalité et de la délinquance grave, la faculté est ouverte à l'autorité judiciaire d'accéder à ces données de connexion, via une injonction de conservation rapide

La possibilité d'un stockage des données pour préserver la sécurité nationale suppose de caractériser, au moment des fait, l'existence d'une menace grave et imminente. Vous ne trouverez pas cette précision dans les arrêts des différentes chambres de l'instruction. Mais nous pensons que cette question ne peut être abandonnée à l'appréciation des juridictions du fond et nous vous proposons, afin d'assurer une application uniforme du droit, de vous appuyer sur l'analyse du Conseil d'Etat et au besoin de vous référer à la liste, communiquée par le parquet général de Paris, des attentats djihadistes commis sur le sol français durant les périodes considérées, qui atteste de la persistance et de l'intensité de la menace terroriste.

Il ne suffit pas cependant d'admettre que, dans les différentes procédures, la conservation des données pouvait être justifiée pour faire face à une menace grave pour la sécurité nationale. Aux paragraphes 96 à 100 de l'arrêt « Garda Siochana », la Cour de justice, en réponse aux observations du gouvernement danois, a exclu d'emblée que les autorités nationales compétentes puissent aux fins de lutte contre la criminalité grave, accéder directement à des données qui ont été stockées à d'autres fins.

La CJUE réserve cependant la faculté de mise en œuvre de la conservation rapide en indiquant au paragraphe 87 de l'arrêt que les Etats membres doivent spécifier dans leur législation la finalité de cette conservation rapide, dès lors qu'elle ne correspond plus à « celles pour lesquelles les données ont été collectées et conservées initialement » et que seules la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier l'ingérence dans les droits fondamentaux qu'est susceptible de comporter une telle conservation.

Ce faisant, la Cour de justice admet nécessairement, comme elle l'avait déjà fait dans l'arrêt Quadrature du net, que ce sont toutes les données disponibles qui peuvent être temporairement gelées, qu'il s'agisse de celles recueillies à des fins commerciales ou pour faire à une menace grave pour la sécurité nationale.

On voit mal, d'ailleurs, comment un tri pourrait être opéré dans les données stockées en fonction de la finalité pour laquelle elles ont été conservées initialement même si cela ne paraît pas techniquement infaisable.

Le mode d'accès aux données par la voie de la conservation rapide est en tant que tel inconnu en droit interne, ou du moins l'était jusqu'à la modification de l'article L. 34-1 du CPCE, mais le code pénal, en imposant à tout un chacun de répondre aux réquisitions judiciaires, instaure un pouvoir de réquisition, qui peut parfaitement être assimilé à une injonction de conservation rapide.

Par ailleurs, la notion de criminalité grave relève de l'appréciation concrète du juge pénal, par référence à la nature de l'infraction et à l'ensemble des faits de l'espèce. En effet, la Cour de justice n'impose pas au législateur d'énumérer les infractions relevant du champ de la criminalité grave en se référant à des catégories strictement prédéfinies en droit interne.

A cet égard, la récente loi du 2 mars 2022 fixe un seuil de gravité des infractions en limitant le recours aux réquisitions de données de connexion aux procédures portant sur un crime ou sur un délit puni d'au moins trois ans d'emprisonnement.
En l'espèce, vous êtes en mesure de constater, dans les différentes procédures, que les infractions poursuivies, meurtre en bande organisée ou encore grands trafics de stupéfiants, entrent bien dans le champ de la criminalité ou de la délinquance grave et que les données de connexion dont le stockage était justifié par des impératifs de sécurité nationale étaient accessibles par le biais de l'injonction de conservation rapide.

Si vous ne retenez pas cette solution, vous pourriez considérer que les données exploitées dans ces procédures doivent être réputées comme ayant été conservées par les opérateurs pour leurs besoins propres. C'est particulièrement vrai lorsque les réquisitions de données de connexion ont été délivrées dans un temps très proche de l'utilisation par les personnes concernées des moyens de communication électronique.

Si toutefois aucune de ces solutions ne vous paraît envisageable, la Cour de justice pourrait être saisie à titre préjudiciel afin de préciser à la fois la notion de conservation rapide et la permission d'accéder ou non par le biais de cette mesure à l'ensemble des données stockées par les opérateurs quelle qu'en soit la finalité.

En définitive nos conclusions tendent au rejet par substitution de motifs des moyens qui invoquent la contrariété au droit de l'Union de la conservation des données auxquelles les enquêteurs ont eu accès dans les différentes procédures.

Je vous remercie.