COUR DE CASSATION

Parquet général

Droit jurisprudentiel sur la rétention des données de communication et impact sur les législations nationales et les procédures pénales - Le cas français

Intervention de Monsieur Rémy HEITZ,

Procureur général près la Cour de cassation, 27 mai 2024

Mesdames et Messieurs les procureurs généraux, chers collègues,

A mon tour, je remercie très chaleureusement la présidence luxembourgeoise, chère Martine, pour son accueil et pour l'organisation parfaite de cette 15ème réunion du Réseau des procureurs généraux de l'Union européenne.

A la tête du parquet général de la Cour de cassation française depuis moins d'un an, je participe pour la première fois à ce rassemblement, qui est l'occasion de faire la connaissance d'un grand nombre de partenaires. Je nourris beaucoup d'attentes à l'égard de notre Réseau, auquel je souhaite contribuer pleinement.

Je me réjouis, pour cette première intervention d'évoquer un sujet essentiel, celui des données de connexion. Un sujet d'intérêt commun pour nos parquets généraux depuis plus de 10 ans[1], et qui n'a cessé de prendre de l'importance à mesure que nos vies se sont numérisées.

Corrélativement, les données de connexion sont devenues omniprésentes dans les enquêtes pénales[2], qu'elles soient d'ailleurs utilisées à charge ou à décharge.

C'est d'autant plus vrai que s'est ajoutée à la délinquance classique la cybercriminalité. Or, pour ces infractions commises en ligne, les métadonnées sont les seules preuves disponibles.

Mais ces données de connexion sont aussi une menace potentielle pour les libertés des citoyens, une atteinte possible à leur vie privée par les autorités nationales.

C'est en ce sens que la jurisprudence de la CJUE s'est construite autour de deux grands principes : Une interdiction de conservation généralisée et indifférenciée des données de trafic et de localisation, sauf, à titre exceptionnel, lorsque pèse une menace grave sur la sécurité nationale, d'une part. Le contrôle préalable par une juridiction ou une autorité indépendante de l'accès à ces données dans le cadre des enquêtes, d'autre part.

Cette jurisprudence, dans beaucoup de nos Etats, a d'abord été une surprise puis a fait l'objet de controverses. Un rapport sénatorial français a évoqué à cet égard un « choc procédural », pour les services d'enquête comme pour les parquets[3].

---

[1] Le premier arrêt de la CJUE, *Digital Rights Ireland*[1], datant du 8 avril 2014.

[2] On estime ainsi que ces métadonnées sont présentes en France dans 85% des enquêtes pénales : Agnès CANAYER et M. Philippe BONNECARRÈRE, Rapport d'information sur les modalités d'investigation recourant aux données de connexion dans le cadre des enquêtes pénales, 15 novembre 2023.

[3] On se souvient qu'encore récemment les responsables des services de police de 26 États membres ont appelé à une évolution de la jurisprudence dans une déclaration commune faite à Lisbonne le 30 mars 2023[3]. On connaît aussi l'existence du « groupe d'experts de haut niveau » européen – ADELE - installé en juin 2023 dans le cadre de l'initiative de la Présidence suédoise « Going Dark »[3], et placé sous l'autorité conjointe de la Commission et du Conseil pour réfléchir à ces enjeux.

De leur côté, les législateurs ont dû se remettre en cause et intervenir. Ils l'ont parfois fait tardivement, en procédant en plusieurs étapes et sans forcément que leur œuvre soit aujourd'hui totalement achevée. Il faut dire que la solution à trouver n'a absolument rien d'évident, les autorités nationales étant prises en étau entre, d'une part, la criminalité organisée, déstabilisatrice et tentaculaire, et, d'autre part, celui de la surveillance de masse, liberticide, avec, pour chacun d'eux, les données comme arme.

Nous traitons donc ce matin d'un sujet à la fois aride, très complexe techniquement, déterminant pour nos enquêtes et sensible politiquement.

Dans ce contexte délicat, les jurisprudences de nos hautes cours nationales ont décliné celle de la CJUE, tout en amenant la Cour à clarifier sa position par les très nombreuses questions préjudicielles qu'elles lui ont posées. Elles ont aussi mis en lumière les enjeux entourant l'interaction de cette jurisprudence avec celle de la CEDH.

Qu'en est-il alors de la législation et de la jurisprudence françaises, en matière de conservation des données de connexion, tout d'abord, et d'accès à ces données, ensuite ?

1/ S'agissant de la conservation des données, il faut rappeler que la CJUE, par sa décision *La Quadrature du Net* du 6 octobre 2020[4], a jugé que la législation française ne pouvait imposer à titre préventif aux opérateurs de communications électroniques et aux fournisseurs d'accès à Internet une conservation généralisée et indifférenciée des données relatives au trafic et à la localisation, sans justifier dans le même temps d'une menace pour la sécurité nationale.

Le Conseil constitutionnel français, pour sa part, a estimé inconstitutionnelle une conservation généralisée et indifférenciée de telles données[5].

Amenée à trancher la question au sein de l'ordre judiciaire français[6], la chambre criminelle de la Cour de cassation a, par quatre arrêts rendus le 12 juillet 2022[7], tiré les conséquences de ces décisions et précisé les conditions de conformité du droit français à celui de l'Union.

Pour ce faire, elle a, comme la CJUE, opéré une distinction parmi les catégories de données de connexion selon le degré d'atteinte à la vie privée, en retenant l'application d'un régime juridique strict pour les données de trafic et de localisation, auxquelles je consacrerai mon propos.

S'agissant de leur conservation généralisée et indifférenciée, la Cour de cassation a écarté l'application des dispositions législatives et réglementaires qui la prévoyaient, à titre préventif, aux fins de lutte contre la criminalité[8].

A l'inverse, elle a confirmé l'application du texte[9] qui l'exigeait en raison de la menace grave, réelle et actuelle ou prévisible à laquelle la France est exposée depuis décembre 1994, du fait du terrorisme et de l'activité de groupes radicaux et extrémistes[10].

---

[4] CJUE, 6 octobre 2020, *La Quadrature du net, French Data Network et a.* (C-511/18, C-512/18, C-520/18),
[5] Décision n° 2021-976/977 QPC du 25 février 2022
[6] Pour l'ordre administratif, v. CE, Assemblée, 21 avril 2021, n° 393099, Publié au recueil Lebon, points 3 à 10).
[7] Crim. 12 juillet 2022, n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652
[8] L'article L. 34-1, III, du code des postes et communications électroniques et l'article R. 10-13 du même code.
[9] Article L34-1 III du code des postes et des communications électroniques
[10] Crim., 12 juillet 2022, n° 21-83.710, § 13 et 14, § 24 à 29.

Sur ce fondement, en conformité avec le droit européen, la loi française continue d'offrir la possibilité au premier ministre d'enjoindre aux opérateurs de communications électroniques de conserver ces données, pour une durée d'un an.

Une faculté dont le pouvoir réglementaire se saisit continuellement[11], pour permettre à notre pays de faire face à une menace que chacun sait vive et durable.

Une fois ces données conservées pour un motif étranger à la lutte contre la criminalité, se pose la question des conditions dans lesquelles l'autorité judiciaire peut y accéder dans le cadre des enquêtes diligentées.

2/ C'est la seconde étape du raisonnement, celle de l'accès judiciaire aux données de connexion.

Un accès que n'interdit pas le droit de l'Union, mais qu'il soumet à une double condition tenant, d'une part, à un critère de nécessité, d'autre part, à un contrôle préalable et indépendant.

S'agissant du critère de nécessité, la Cour de cassation a, là encore, tiré les conséquences du droit européen pour imposer que cet accès n'aille pas au-delà de ce qui est, d'un point de vue matériel ou temporel, strictement nécessaire à la prévention ou à la répression de l'infraction concernée. Exigeant un contrôle effectif en la matière, elle a jugé que tel n'était pas le cas en présence de réquisitions émises par un juge d'instruction en exécution d'une commission rogatoire générale[12].

C'est donc un critère de réelle nécessité qu'impose notre droit. Un critère qui tient aux spécificités de chaque procédure, mais en premier lieu à la gravité suffisante de l'infraction visée.

A cet égard, la CJUE a jugé il y a quelques jours[13] que, pour délimiter le champ dans lequel l'accès à ces données peut intervenir, la définition des « infractions graves » relève de la compétence des Etats membres. Elle a toutefois précisé que la fixation d'un quantum de peine encouru était un critère objectif pertinent, en jugeant qu'un seuil fixé par référence à une peine maximale de réclusion de trois ans n'apparaissait pas comme étant excessivement bas[14].

C'est une décision rassurante s'agissant de la conventionnalité du droit français, puisque que notre législateur[15] avait, dès mars 2022, globalement restreint les réquisitions permettant cet accès aux procédures portant sur une infraction punie d'au moins trois ans d'emprisonnement.

---

[11] En dernier lieu par un décret du 10 octobre 2023 portant cette injonction.
[12] Crim., 25 octobre 2022, n° 21-87.397 ; Crim., 16 janv. 2024, n° 23-80.268.
[13] CJUE, 30 avril 2024, C-178/22, Procura della Repubblica presso il Tribunale di Bolzano
[14] Dans son arrêt C178/22, la Cour renvoie à son arrêt du 21 juin 2022, Ligue des droits humains, C-817/19, §150.
[15] Loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire créant l'article 60-1-2 CPP. Elles peuvent également intervenir dans le cadre d'un délit puni d'un an d'emprisonnement commis par l'utilisation d'un réseau de communications électroniques, ou dans les procédures visant à la recherche d'une personne disparue et la reconstitution du parcours d'un auteur de crimes sériels

Saisie de l'état du droit antérieur à cette évolution législative, la Cour de cassation a quant à elle, dans ses arrêts du 12 juillet 2022, transposé l'exigence générale posée par la CJUE[16], en jugeant qu'il appartient à une juridiction saisie d'un moyen critiquant la régularité de l'accès à ces données de vérifier que l'infraction concernée relève de la criminalité grave.

Une notion que notre haute Cour a précisée par des critères d'appréciation[17], destinés à aider les acteurs opérant ce contrôle, non seulement *a posteriori*, mais également *a priori*.

Evoquant cette vérification *a priori*, j'en viens à l'autre condition posée par le droit européen, qui a posé plus de difficulté en droit français : la détermination de l'autorité chargée d'opérer un contrôle préalable à cet accès.

A cet égard, la Cour de cassation[18] a une nouvelle fois tiré les conséquences des arrêts de la CJUE en écartant l'application de plusieurs articles du code de procédure pénale[19] qui ne prévoyaient pas, dans le cadre des enquêtes menées sous l'autorité du ministère public, un contrôle mené *a priori* par une juridiction ou une entité administrative indépendante[20].

Toutefois, la Cour de cassation a soumis la nullité d'une procédure réalisée avec une telle irrégularité à la démonstration de l'existence d'une ingérence injustifiée dans la vie privée de la personne visée.

Autrement dit, elle a exigé du requérant qu'il prouve qu'un grief effectif en résultait, en établissant qu'un contrôle préalable aurait permis de constater que les conditions de cet accès n'étaient pas réunies.

Cette jurisprudence, la Cour de cassation l'a réitérée très récemment, dans un arrêt du 27 février 2024[21], en étendant son application à la géolocalisation en temps réel d'un téléphone portable.

Se saisissant de cette interprétation, les parquets français ont continué à émettre des réquisitions aux fins d'accès aux données de connexion dans les enquêtes menées sous leur autorité, tout en renforçant leur contrôle préalable s'agissant de l'absence de grief pour la personne concernée. Cette pratique, validée par la cour d'appel de Paris[22], a permis de sauvegarder un équilibre essentiel dans l'attente d'une évolution législative qui mobilise l'autorité requise par la CJUE.

***

Voilà donc une jurisprudence foisonnante, qui imbrique les décisions des juridictions nationales et européennes, dans un état du droit qui continue d'évoluer, sous l'effet notamment d'un nombre important de questions préjudicielles, mais aussi de saisines par les citoyens pour ce qui concerne la CEDH.

---

[16] La Cour a constaté que le droit de l'Union autorise la délivrance par l'autorité judiciaire d'une telle injonction soit pour leurs besoins propres, soit au titre d'une obligation de conservation imposée aux fins de sauvegarde de la sécurité nationale, afin d'accéder auxdites données pour élucider une infraction déterminée.

[17] La nature des agissements, le dommage qui en résulte, les circonstances de commission et la durée de la peine.

[18] Crim. 12 juillet 2022, n° 21-83.710, 21-83.820, 21-84.096 et 20-86.652

[19] Les articles 60-1, 60-2, 77-1-1 et 77-1-2 du code de procédure pénale.

[20] Elle a, à l'inverse, jugé que le juge d'instruction est habilité à contrôler cet accès aux données de connexion.

[21] Crim.,27 février 2024, n° 23-81.061

22 CA Paris, 16 décembre 2022 ; CA Paris, 12 janvier 2023 ; CA Paris 25 mai 2023.

Les législateurs nationaux interviennent parfois pour tirer les conséquences des décisions de nos juridictions. En France, le Sénat espère une nouvelle législation d'ici 2 ou 3 ans, ce qui correspond à l'échéance prévue pour la refonte de notre code de procédure pénale.

Mais les autorités avancent sur un terrain mouvant, alors que la solution globale relève du niveau européen. Dans ce contexte, il faut souhaiter que les négociations européennes aboutissent à un compromis garantissant non seulement les libertés, mais aussi l'efficacité des enquêtes pénales.

En tout état de cause, et pour finir sur une note positive, on peut se réjouir du fait que ces jurisprudences aient mis en valeur l'importance de la coordination de nos législations et de nos actions ; qu'elles aient fait naître une profonde réflexion sur la nécessité d'un régime commun des preuves numériques et, plus largement, d'un régime cohérent du contrôle de l'enquête pénale.

Je vous remercie de votre attention.