La conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ?

Matthieu Audibert

Droit de l'espace numérique

JURISPRUDENCE JUDICIAIRE

Par le capitaine Matthieu Audibert

La conservation et l'accès aux données techniques de connexion. Vers un nouveau paradigme pour les enquêtes judiciaires ?

Cour de justice de l'Union européenne (CJUE), affaire C-746/18, arrêt du 2 mars 2021 H.K/Prokuratuur

Dans la continuité de sa jurisprudence établie depuis 2014[1], la CJUE poursuit l'encadrement des dispositions juridiques liées à la conservation[2] et maintenant à l'accès, à des fins pénales, aux données techniques de connexion. Dans le même temps, la CJUE pose un certain nombre de garanties liées à cet accès qui mettent à mal les prérogatives du procureur de la République et certaines prérogatives du juge d'instruction au regard de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 lue à la lumière de la charte des droits fondamentaux de l'Union européenne (UE).

S'agissant des faits, un individu (H.K) a été condamné en première

1. Arrêt du 8 avril 2014, Digital Rights Ireland et Seitlinger e.a., C-293/12 et C-594/12 ; arrêt du 21 décembre 2016, Tele2 Sverige, C-203/15 et C-698/15 ; arrêt du 6 octobre 2020, La Quadrature du Net e.a. contre Premier ministre e.a., C-511/18, C-512/18 et C-520/18.

2. LASSALLE, Maxime, Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE, *Recueil Dalloz*, 2021, p. 406.

instance à une peine privative de liberté de deux ans pour avoir commis plusieurs vols, escroqueries et exercé des actes de violences. Pour déclarer coupable cet individu, la juridiction de première instance s'est fondée sur différents actes réalisés par les services d'enquête et notamment l'obtention de données relatives aux communications électroniques. Ces données peuvent être récupérées par les enquêteurs suite à l'autorisation délivrée par le procureur territorialement compétent. Plus précisément, ces données concernent plusieurs numéros de téléphones de l'individu et les différentes identités associées.

Condamné en première instance, il fait appel et celui-ci est rejeté par la cour d'appel estonienne. Il introduit alors un pourvoi en cassation contre cette décision auprès de la Cour suprême de son pays et conteste notamment la recevabilité des procès-verbaux établis à partir des données techniques de connexion récupérées par les enquêteurs sur autorisation du procureur.

Saisie de ce pourvoi, la juridiction suprême estonienne va sursoir à statuer et va adresser trois questions préjudicielles à la CJUE :

« Convient-il d'interpréter l'article 15, paragraphe 1, de la directive [2002/58], lu conjointement avec les articles 7, 8, 11 et 52, paragraphe 1, de la [Charte], en ce sens que l'accès des autorités nationales, dans le cadre d'une procédure pénale, à des données permettant de retrouver et d'identifier la source et la destination d'une communication téléphonique à partir du téléphone fixe ou mobile du suspect, d'en déterminer la date, l'heure, la durée et la nature, d'identifier le matériel de communication utilisé ainsi que de localiser le matériel de communication mobile utilisé constitue une ingérence tellement grave dans les droits fondamentaux garantis par les articles

précités de la Charte que, lors de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales, cet accès doit être limité à la lutte contre la criminalité grave, indépendamment de la période pour laquelle les autorités nationales ont accès aux données conservées ?

Convient-il d'interpréter l'article 15, paragraphe 1, de la directive [2002/58] à partir du principe de proportionnalité tel que formulé aux points 55 à 57 de [l'arrêt du 2 octobre 2018, Ministerio Fiscal (C-207/16, EU:C:2018:788),] en ce sens que, si la quantité des données visées à la première question, auxquelles les autorités nationales ont accès, n'est pas très importante (tant du point de vue de la nature des données que du point de vue de la longueur de la période concernée), l'ingérence dans les droits fondamentaux qui en découle peut être justifiée de manière générale par l'objectif de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales et que, plus la quantité des données auxquelles les autorités nationales ont accès est importante, plus les infractions pénales contre lesquelles l'ingérence est destinée à lutter doivent être graves ?

Convient-il de considérer que l'exigence figurant au deuxième point du dispositif de [l'arrêt du 21 décembre 2016, Tele2 (C-203/15 et C-698/15, EU:C:2016:970)], selon laquelle l'accès des autorités nationales compétentes aux données doit être soumis à un contrôle préalable par une juridiction ou une autorité administrative indépendante, signifie que l'article 15, paragraphe 1, de la directive [2002/58] doit être interprété en ce sens que l'on peut considérer comme une autorité administrative indépendante le ministère public

qui dirige la procédure d'instruction et qui, ce faisant, est, en vertu de la loi, tenu d'agir de manière indépendante, en étant uniquement soumis à la loi et en examinant, dans le cadre de la procédure d'instruction, à la fois les éléments à charge et les éléments à décharge concernant la personne poursuivie, mais qui représente l'action publique au cours de la procédure judiciaire ultérieure ? »

Saisie de ces questions préjudicielles, la CJUE va, tout en rappelant sa jurisprudence antérieure sur l'interdiction faite aux États membres de procéder à une conservation généralisée et indifférenciée des données techniques de connexion, préciser que cet accès doit être « circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention des menaces graves contre la sécurité publique »[3] (I).

En outre, la CJUE va indiquer que le droit de l'UE s'oppose à ce que le ministère public, en charge de diriger l'enquête pénale et, le cas échéant, d'engager l'action publique, puisse autoriser l'accès aux enquêteurs aux données techniques de connexion. Ce dernier point implique de nombreuses conséquences pour le Parquet français mais également pour le juge d'instruction (II).

3. Point 60 1).

Droit de l'espace numérique

I. La notion de criminalité grave ou de menace grave contre la sécurité publique comme seul critère autorisant l'accès aux autorités publiques aux données techniques de connexion

Ce nouvel arrêt de la CJUE rappelle une solution qui n'est pas nouvelle (A). Toutefois, combiné à l'arrêt Quadrature du Net, ce nouvel arrêt relatif aux données de connexion est susceptible d'entraîner de lourdes conséquences dans le succès de nombreuses enquêtes judiciaires (B).

A) Une solution non nouvelle dégagée par la CJUE s'agissant de la conservation des données de connexion

Dans ses questions préjudicielles, la Cour suprême estonienne s'interroge sur les modalités d'accès à ces données au regard de l'article 15 §1 de la directive 2002/58. L'accès par les autorités nationales, dans le cadre d'une enquête judiciaire, à ces données constitue-t-il une ingérence tellement grave dans les droits fondamentaux garantis par la Charte que cet accès doit faire l'objet d'une limitation à la lutte contre la criminalité, nonobstant la période pendant les enquêteurs ont eu accès à ces données ?[4]

En outre, la Cour suprême estonienne s'interroge au regard du volume de données concernées. L'argumentation sous-jacente de l'Estonie étant que si le volume de données n'est pas très important,

4. Point 26 1).

aussi bien s'agissant de la nature de celles-ci que de la période de collecte, cela peut-il justifier que l'ingérence qui en découle dans les droits fondamentaux puisse être justifiée par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales ?[5] En outre, de manière implicite, la juridiction estonienne tente de soumettre un accès proportionné à la gravité de l'infraction. Autrement dit, plus l'infraction est grave, plus la qualité de données accessibles serait importante[6].

Dans l'argumentaire du gouvernement estonien, il est intéressant de souligner que l'accès aux données conservées en vertu du droit national estonien peut être sollicité pour tout type d'infraction pénale[7], ce qui est également le cas du droit français[8].

Pour répondre à ces questions préjudicielles, la CJUE rappelle sa jurisprudence antérieure. Tout d'abord, elle subordonne l'accès à ces données à leur conservation de manière conforme au droit de l'Union[9]. Elle rappelle le principe dégagé dans l'arrêt Quadrature du Net du 6 octobre 2020, à savoir que le droit de l'Union s'oppose à des législations nationales prévoyant à des fins pénales, à titre préventif, la conservation généralisée et indifférenciée des données

5. Point 26 2).
6. *Ibid*.
7. Point 28.
8. Articles L. 34-1 et R. 10-13 du Code des postes et des communications électroniques et dispositions du Code de procédure pénale, voir par exemple l'article 60-1.
9. Point 29. Voir aussi arrêt du 6 octobre 2020, La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, point 167).

techniques de connexion (de localisation et de trafic)[10][11].

Ensuite, la CJUE va se livrer à un contrôle de proportionnalité dans l'accès à ces données entre, d'une part, la gravité de l'ingérence dans les droits fondamentaux et, d'apéutre part, l'objectif d'intérêt général poursuivi[12]. Il s'agit là encore d'un rappel de sa position exprimée dans l'arrêt Quadrature du Net[13]. La CJUE poursuit en indiquant que « seule la lutte contre la criminalité et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés [par la Charte][14] ». Ces ingérences sont notamment celles qui « impliquent la conservation des données relatives au trafic et des données de localisation, qu'elle soit généralisée et indifférenciée ou ciblée[15]».
Sur ce point, la CJUE conclut que « seules des ingérences ne présentant pas un caractère grave peuvent être justifiées par l'objectif (…) de prévention, de recherche, de détection et de poursuite d'infractions pénales en général[16]».
Sur les données, la CJUE fait ensuite la distinction avec les données

10. Point 30. Voir aussi arrêt du 6 octobre 202, La Quadrature du Net e.a, c- 1/18, C-512/18 et c-520/18, point 168.
11. LASSALLE, Maxime, Protection des données, renseignements, procédure pénale et enquêtes administratives : l'approche française remise en cause par la CJUE, *Recueil Dalloz*, 2021, p. 406.
12. Points 31 et 32.
13. Arrêt du 6 octobre 2020, La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, point 131.
14. Points 33.
15. *Ibid*.
16. *Ibid*. Voir aussi arrêt du 6 octobre 2020, La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, points 140 et 146.

relatives à l'identité civile des utilisateurs non associées aux données de communication. Pour les premières, considérant que celles-ci ne permettent pas, à elles seules, de connaître les usages de l'utilisateur ou encore sa localisation, la CJUE considère que leur conservation n'est pas en contradiction avec le droit de l'Union[17]. Il convient de souligner que la Cour européenne des droits de l'Homme adopte la même solution s'agissant des données relatives à l'identité civile des utilisateurs[18][19].

Dans la suite de son raisonnement, la CJUE considère l'accès limité à une quantité limitée de données de connexion comme étant un critère inopérant pour justifier une telle ingérence[20] et rappelle, comme dans l'arrêt Quadrature du Net[21], que le juge pénal est tenu d'écarter « des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union ou encore au moyen d'un accès de l'autorité compétente à ces données en violation de ce droit, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la

17. Point 34. Voir aussi arrêt du 6 octobre 2020, La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, points 157 et 158.

18. CEDH, *Brayer contre Allemagne*, 30 janvier 2020, n° 50001/12.

19. DE MONTECLER Marie-Christine. Protection des données : la CJUE infléchit sa jurisprudence. *AJDA*, 2020, p. 1880.

20. Point 40.

21. Arrêt du 6 octobre 2020, La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, points 226 et 227.

connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits[22]».

Pour conclure sur ces deux questions, la CJUE écarte les critères liés à la durée de l'accès aux données et à la nature des données disponibles pour conclure que le droit de l'Union[23] n'autorise l'accès, dans le cadre des enquêtes judiciaires, aux données de connexion permettant de tirer des conclusions sur la vie privée des personnes visées par les investigations, que dans le cadre de la lutte contre la criminalité grave ou pour prévenir des menaces graves contre la sécurité publique[24].

B) Quelles conséquences pour les enquêtes judiciaires ?

Pour commencer, il peut être intéressant de comparer l'appréhension juridique des données techniques de connexion et les données de contenu par les services d'enquête.
D'un point de vue technique, s'agissant des correspondances émises par la voie des communications électroniques, on distingue traditionnellement les données relatives aux contenus et les données techniques de connexion. Les premières contiennent les paroles prononcées ou écrites et les secondes les informations relatives à la connexion des appareils aux réseaux téléphoniques ou à Internet.

22. Point 44.
23. Article 15 §1 de la directive 2002/58, articles 7, 8, 11 et 52 de la Charte des droits fondamentaux.
24. Point 45.

Droit de l'espace numérique

Les interceptions de correspondances (donc les données de contenu) sont possibles en matière criminelle et en matière correctionnelle si la peine encourue est égale ou supérieure à trois ans d'emprisonnement[25] dans le cadre d'une information judiciaire. S'agissant de l'enquête de flagrance et de l'enquête préliminaire, les interceptions de correspondances émises par la voie des communications électroniques sont possibles pour l'une des infractions entrant dans le champ d'application des articles 706-73 et 706-73-1 du Code de procédure pénale[26].
En revanche, que ce soit en enquête de flagrance[27], en enquête préliminaire[28] ou dans le cadre d'une information judiciaire[29], aucun seuil n'est exigé s'agissant de la possibilité de requérir les opérateurs de communication électroniques aux fins de récupérer des données techniques de connexion. Autrement dit, en droit français, il est possible de récupérer ces données aussi bien pour une contravention que pour un délit ou un crime. Cette différence de traitement entre ces deux types de données se comprend aisément, les premières portant sur les propos ou écrits échangés et les secondes sur les informations techniques relatives à la connexion des appareils aux différents réseaux. Le degré d'intrusion dans la vie privée est donc sensiblement différent.

Avec son arrêt H.K/Prokuratuur, la CJUE reprend ses solutions déjà dégagées dans les arrêts Tele2 Sverige et Quadrature du Net,

25. Article 100 du Code de procédure pénale.
26. Infractions relatives à la criminalité et à la délinquance organisées.
27. Article 60-1 du Code de procédure pénale.
28. Article 77-1-1 du Code de procédure pénale.
29. Article 99-3 du Code de procédure pénale.

s'agissant de la non-conformité au droit de l'Union de législations nationales prévoyant une conservation généralisée et indifférenciée des données techniques de connexion. L'apport de cet arrêt réside, comme nous l'avons vu précédemment, dans un accès autorisé, à des fins pénales, aux données techniques de connexion uniquement en vue de lutter contre la criminalité grave ou de prévenir des menaces graves contre la sécurité publique.

Or, réduire les données accessibles aux seules infractions pénales graves n'est pas concevable pour les services d'enquête, notamment parce que la notion « d'infraction grave » exclut de nombreuses possibilités d'investigations. Une réduction drastique du champ de conservation des données et des données accessibles méconnaît les processus d'investigations dont la vocation est aussi de garantir le droit des victimes d'obtenir un jugement et réparation pour le préjudice subi. En outre, au début d'une enquête, il est impossible de déterminer une zone délimitée qui pourrait être celle de l'auteur et de ses éventuels complices. Il est impossible pour les magistrats et les enquêteurs de connaître à l'avance les données dont ils auront besoin pour élucider les enquêtes qu'ils mènent. Enfin, il est impossible de déterminer à l'avance quelles personnes feront l'objet d'investigations[30], à charge comme à décharge. Ainsi, « plus que le dispositif national, ce sera peut-être la méthodologie d'enquête qui devra être revue[31] ».
Par ailleurs, cette possibilité d'accéder aux données de connexion

30. MOLINS, François. La protection des citoyens européens dans un monde ultra-connecté. Fondation Robert Schuman, *Question d'Europe*, n° 510, avril 2019.
31. NICAUD, Baptiste. CJUE : un équilibre – trop ? – rigoureux entre droit au respect de la vie privée et conservation des données. *AJ Pénal*, 2020, p. 531.

permet d'identifier les auteurs mais aussi et surtout de matérialiser des infractions, de démontrer des liens de complicité ou des coactions[32], de déterminer si les faits ont été commis avec des circonstances aggravantes.

En outre, comme nous venons de le voir, la CJUE n'envisage l'accès aux données de connexion conservées que dans le cadre de la lutte contre la criminalité grave. Or, cette notion de gravité n'est pas explicitée dans l'arrêt et la jurisprudence antérieure de la CJUE relative aux données de connexion. En droit français, cette notion de gravité est déterminée en fonction de l'échelle des peines. Ainsi, un crime est par essence nécessairement grave. Or, s'agissant des délits, la liste des infractions potentiellement concernées par un accès prohibé aux données de connexion est extrêmement longue.

C'est le cas, par exemple, des infractions pouvant être exclusivement commises par la voie des communications électroniques : infractions relatives à la vie privée[33], cyberharcèlement[34], provocation à la discrimination, à la haine ou à la violence à l'égard d'une personne ou d'un groupe de personnes à raison de leur origine ou de leur appartenance à une ethnie, une nation, une race ou à une religion déterminée[35], la provocation à la haine ou à la violence à raison du sexe ou de l'orientation sexuelle, de l'identité de genre ou du handicap et provocation à des

32. *op.cit.* note 30, p. 26.
33. Articles 226-1 et suivants du Code pénal.
34. Article 222-33-2-2 du Code pénal.
35. Article 24 de la loi du 29 juillet 1881 relative à la liberté de la presse.

discriminations les concernant[36].

Ces infractions sont-elles graves ? La sanction prévue pour celles-ci varie entre un an et deux d'emprisonnement. L'application stricte de cet arrêt de la CJUE empêcherait donc le recours aux données de connexion pour enquêter sur des infractions de haine en ligne. Or, ces données sont absolument essentielles pour élucider de tels faits. Ainsi, « l'inquiétude pèse tant sur les procédures en cours que sur l'avenir des moyens d'enquêtes[37]» pour élucider ces infractions.

Enfin, l'arrêt de la CJUE faisant suite à une question préjudicielle[38], il appartient à la juridiction nationale qui a saisi la CJUE de résoudre l'affaire, conformément à la décision de la CJUE. En outre, cette décision lie les autres juridictions nationales des pays de l'Union européenne qui seraient saisies d'un problème similaire. La combinaison des arrêts Quadrature du Net et H.K/Prokuratuur est donc susceptible de remettre profondément en cause les méthodes actuelles d'enquêtes judiciaires[39][40].

Nonobstant les questions de la conservation et de l'accès à des fins pénales aux données de connexion, la CJUE vient préciser les modalités d'accès à ces données et, notamment, s'agissant du

36. *Ibid*.
37. *op.cit*. note 31, p. 26.
38. Article 267 du Traité sur l'Union européenne.
39. DAOUD, Emmanuel, BELLO, Imane, PECRIAUX, Océane. Données de connexion et sauvegarde de la sécurité nationale : l'exception confirme la règle. *Dalloz IP/IT*, 2021, p. 46.
40. *op.cit*. note 31, p. 26.

contrôle préalable de cet accès. Ce faisant, elle remet en question les prérogatives du Parquet français et, par extension, certaines prérogatives du juge d'instruction.

II. L'exclusion du ministère public dans le contrôle préalable de certains actes d'enquêtes : vers un nouveau paradigme dans la procédure pénale française ?

Il s'agit ici d'examiner la troisième question posée par la Cour suprême estonienne et la réponse apportée par la CJUE. En effet, au regard de l'article 15, paragraphe 1, de la directive 2002/58 et de l'arrêt Tele2 du 21 décembre 2016, le ministère public est-il compétent pour autoriser cet accès ? Par sa réponse, la CJUE remet en cause certaines prérogatives du ministère public français (A) et, par là même, certaines du juge d'instruction (B).

A) Une remise en cause du Parquet français au travers du ministère public estonien

Pour analyser la possibilité pour le ministère public estonien d'autoriser cet accès, la CJUE va analyser ses caractéristiques. Ainsi, il est « tenu d'agir de manière indépendante », il doit « examiner les éléments à charge et à décharge lors de la procédure d'instruction, l'objectif de cette procédure [étant] la collecte d'éléments de preuve ainsi que la réunion des autres conditions nécessaires à la tenue d'un procès », il « représente l'action publique lors du procès et (…) serait donc également partie à la procédure ». Enfin, il « est organisé de manière hiérarchique »[41].

41. Point 47. Voir également CRICHTON, Cécile. Précisions sur l'accès aux

Tout d'abord, la CJUE va contrôler le respect de l'exigence de proportionnalité dans l'accès aux données. Elle relève ainsi que la loi estonienne autorise au Parquet estonien un accès général à toutes les données sans préciser l'objectif poursuivi[42]. Elle en conclut ainsi que ces dispositions ne respectent pas l'exigence de proportionnalité[43]. Ensuite, la CJUE va ajouter un point fondamental qui impactera certainement le Parquet français. Elle indique « que l'accès des autorités nationales compétentes aux données conservées [doit être] subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante et que la décision de cette juridiction ou de cette entité [doit intervenir] 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[44] ».

Elle précise que la juridiction ou l'entité de contrôle « [doit disposer] de toutes les attributions et [doit présenter] 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

métadonnées lors du procès pénal. *Dalloz actualité*, 5 mars 2021.

42. Points 49 et 50.

43. *Ibid*.

44. Point 51. Voir également arrêt du 6 octobre 2020, La Quadrature du Net e.a, c-511/18, C-512/18 et c-520/18, point 189.

des personnes dont les données sont concernées par l'accès[45] ». Dès lors, cette juridiction ou entité de contrôle doit avoir « une position de neutralité vis-à-vis des parties à la procédure pénale[46] ».
Dans la mesure où le ministère public estonien dirige l'enquête mais est également susceptible d'exercer l'action publique, la CJUE en conclut que celui-ci ne peut être considéré comme indépendant : il n'a pas la qualité de tiers à la procédure et, notamment, vis-à-vis des enquêteurs qui demandent l'accès aux données et il peut faire l'objet d'une influence extérieure[47]. Enfin, la CJUE insiste pour rappeler qu'un contrôle de l'accès postérieur n'est pas suffisant, car il doit intervenir dans les plus brefs délais, « préalablement à tout accès, sauf cas d'urgence dûment justifié[48] ».

Forts de ces éléments, examinons la situation du Parquet français. Aux termes de la loi, la police judiciaire est exercée sous la direction du procureur de la République[49]. Il exerce l'action publique dans le respect du principe d'impartialité[50], il ne prend donc pas parti dans les enquêtes. Toutefois, c'est lui qui dispose du principe de l'opportunité des poursuites[51] et peut, le cas échéant, mettre en œuvre l'action publique et requérir une condamnation[52]. Enfin, le procureur de la République est placé sous l'autorité du procureur

45. Point 52.
46. Point 54.
47. Points 54-57.
48. Point 58.
49. Articles 12 et 41 du Code de procédure pénale.
50. Article 31 du Code de procédure pénale.
51. Article 40 du Code de procédure pénale.
52. Article 40-1 du Code de procédure pénale.

général près la Cour d'appel[53].
Or, sur ces points, la CJUE a clairement tranché[54] : le droit de l'Union s'oppose à une législation nationale qui donne compétence au ministère public, qui dirige l'enquête judiciaire et exerce, le cas échéant, l'action publique ultérieurement, pour autoriser l'accès aux enquêteurs aux données de connexion.

En droit français, dans le cadre de l'enquête de flagrance, le procureur de la République ou l'officier de police judiciaire, et l'agent de police judiciaire sous le contrôle de ce dernier, peuvent, par réquisition, récupérer les données de connexion intéressant une enquête en cours[55]. Au cours de l'enquête préliminaire, le procureur ou l'officier ou l'agent de police judiciaire, peuvent, sur autorisation du procureur de la République également récupérer ces données, toujours par réquisition[56]. Dans la loi, le contrôle préalable n'existe que dans le cadre de l'enquête préliminaire. En pratique, il existe aussi en enquête de flagrance dans la mesure où il s'agit de réquisitions émises sous frais de justice.

Ainsi, aucun tiers à la procédure, tel un juge des libertés et de la détention, n'intervient pour autoriser cet accès. Seul le procureur de la République est susceptible d'exercer un tel contrôle. Or, comme nous l'avons vu, du fait de son positionnement, il y a d'une part un problème de contrôle préalable tel qu'exigé par la CJUE mais

53. Articles 35 à 37 du Code de procédure pénale.
54. Point 60 2).
55. Article 60-1 du Code de procédure pénale.
56. Article 77-1-1 du Code de procédure pénale.

également un problème d'indépendance au sein même de l'enquête, dans la mesure où c'est le procureur qui exerce, le cas échéant, l'action publique à l'issue de l'enquête qu'il dirige.

En conclusion, le Parquet français est clairement menacé par l'arrêt de la CJUE du 2 mars, tant en raison de son positionnement dans la procédure qu'en raison de ses attributions propres.

B) Une remise en cause par ricochet du juge d'instruction ?

À première vue, le juge d'instruction ne semble pas impacté par cet arrêt de la CJUE qui ne traite que du ministère public. Pour autant, certains points de l'arrêt le concernent.

Celui-ci ne représente pas l'action publique. Son rôle est d'instruire à charge et à décharge[57]. Il procède ainsi à tous les actes d'enquête qu'il juge utiles à la manifestation de la vérité. Il peut procéder lui-même à ces actes ou les déléguer aux officiers de police judiciaire par le biais de commissions rogatoires[58]. À cet effet, les officiers de police judiciaire exercent, dans les limites de la commission rogatoire, tous les pouvoirs du juge d'instruction[59].

S'agissant des données de connexion, le juge d'instruction ou l'officier de police judiciaire commis par lui peuvent, par réquisition, récupérer les données de connexion intéressant une enquête en

57. Article 81 du Code de procédure pénale.
58. Article 151 du Code de procédure pénale.
59. Article 152 du Code de procédure pénale.

cours[60]. Ce pouvoir précis va alors rentrer en contradiction avec l'arrêt de la CJUE. Celle-ci explique en substance que celui qui exerce le contrôle préalable doit être un tiers par rapport à celui qui demande l'accès aux données de connexion. L'autorité de contrôle ne doit donc pas être impliquée dans la conduite de l'enquête pénale[61].

Or, lorsque le juge d'instruction requiert en vertu de l'article 99-3 du Code de procédure pénale, aucune entité ne contrôle préalablement sa réquisition. Seule une nullité nécessairement postérieure peut le cas échéant être soulevée[62]. Surtout, le juge d'instruction est impliqué dans l'enquête, car c'est justement son rôle d'informer à charge et à décharge[63]. La CJUE indique que le droit de l'Union « s'oppose à une réglementation nationale donnant compétence au ministère public dont la mission est de diriger la procédure d'instruction pénale (…) pour autoriser l'accès d'une autorité publique aux données [de connexion] aux fins d'une instruction pénale[64] ». Nous pouvons donc en déduire que l'article 99-3 du Code de procédure pénale semble contraire au droit de l'Union.

Le raisonnement pourrait également s'appliquer aux interceptions de correspondances bien que non concernées par cet arrêt. En effet, si en enquête de flagrance et en enquête préliminaire, celles-ci sont

60. Article 99-3 du Code de procédure pénale.
61. Point 54.
62. Article 170 du Code de procédure pénale.
63. Article 81 du Code de procédure pénale.
64. Point 59.

autorisées par le juge des libertés et de la détention[65], dans le cadre de l'information, le juge des libertés et de la détention n'intervient pas pour les autoriser[66]. Il serait paradoxal que les données de connexion fassent l'objet d'un traitement plus strict que les données de contenu, objets des interceptions. Pour ces raisons, le juge d'instruction est également menacé par ricochet par cet arrêt de la CJUE.

À cet égard, il convient de s'interroger si la jurisprudence de la CJUE n'incite pas les États membres à tendre vers la création d'un juge de l'enquête : magistrat non impliqué dans la procédure qui serait uniquement chargé, à la demande des enquêteurs ou du procureur de la République ou du juge d'instruction pourtant indépendant, d'autoriser certains actes attentatoires à des droits ou libertés.

65. Article 706-95 du Code de procédure pénale.
66. Article 100 du Code de procédure pénale.