MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

RÉPUBLIQUE FRANÇAISE

Paris, le 1er avril 2019

À MONSIEUR LE PRÉSIDENT

ET À MESDAMES ET MESSIEURS LES MEMBRES

DE LA COUR DE JUSTICE DE L'UNION EUROPÉENNE

OBSERVATIONS

DU GOUVERNEMENT DE LA RÉPUBLIQUE FRANÇAISE

DANS L'AFFAIRE

C-746/18

H.K.

I – INTRODUCTION

1. Par une décision du 12 novembre 2018, la Cour suprême (Estonie) a, en application de l'article 267 TFUE, posé à la Cour les questions préjudicielles suivantes :

« *1° Convient-il d'interpréter l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002* [concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)], *lu conjointement avec les articles 7, 8, 11 et 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne 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 ?*

2° Convient-il d'interpréter l'article 15, paragraphe 1, de la directive 2002/58/CE à partir du principe de proportionnalité tel que formulé aux points 55 à 57 de l'arrêt de la Cour du 2 octobre 2018 dans l'affaire C-207/16 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 ?

3° Convient-il de considérer que l'exigence figurant au deuxième point du dispositif de l'arrêt de la Cour du 21 décembre 2016 dans les affaires jointes C-203/15 et C-698/15, 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/CE 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 ? »

2. Ces questions appellent, de la part du gouvernement français, les observations qui suivent.

II – RAPPEL DES FAITS ET DE LA PROCEDURE

3. Le gouvernement français se réfère aux rappels des faits et de la procédure qui figurent dans la décision de renvoi.

III – DROIT APPLICABLE

1) La charte des droits fondamentaux de l'Union européenne

4. L'article 6 de la Charte, relatif au droit à la liberté et à la sûreté, dispose :

« *Toute personne a droit à la liberté et à la sûreté.* »

5. L'article 7 de la Charte, relatif au respect de la vie privée et familiale, dispose :

« *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications.* »

6. L'article 8 de la Charte, relatif à la protection des données à caractère personnel, dispose :

« *1. Toute personne a droit à la protection des données à caractère personnel la concernant.*

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. ».

7. L'article 11 de la Charte, relatif à la liberté d'expression et d'information, dispose :

« *Toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières.* »

8. L'article 52 de la Charte, relatif à la portée et à l'interprétation des droits et des principes, dispose :

« *1. Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui. (...)*

3. Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention. Cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue. (...) »

2) La directive 2002/58/CE, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

9. Le onzième considérant de la directive 2002/58 énonce :

« *À l'instar de la directive 95/46/CE, la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit communautaire. Elle ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.* »

10. L'article 15, paragraphe 1, de la directive 2002/58, relatif à l'application de certaines dispositions de la directive 95/46/CE, dispose :

« *1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive 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, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. 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. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne. (...)* »

3) La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données

11. L'article 13 de la directive 95/46 dispose :

« *1. Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus à l'article 6 paragraphe 1, à l'article 10, à l'article 11 paragraphe 1 et aux articles 12 et 21, lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder :*

a) la sûreté de l'État;

b) la défense;

c) la sécurité publique;

d) la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de manquements à la déontologie dans le cas des professions réglementées ;

e) un intérêt économique ou financier important d'un État membre ou de l'Union européenne, y compris dans les domaines monétaire, budgétaire et fiscal;

f) une mission de contrôle, d'inspection ou de réglementation relevant, même à titre occasionnel, de l'exercice de l'autorité publique, dans les cas visés aux points c), d) et e) ;

g) la protection de la personne concernée ou des droits et libertés d'autrui.

2. Sous réserve de garanties légales appropriées, excluant notamment que les données puissent être utilisées aux fins de mesures ou de décisions se rapportant à des personnes précises, les États membres peuvent, dans le cas où il n'existe manifestement aucun risque d'atteinte à la vie privée de la personne concernée, limiter par une mesure

législative les droits prévus à l'article 12 lorsque les données sont traitées exclusivement aux fins de la recherche scientifique ou sont stockées sous la forme de données à caractère personnel pendant une durée n'excédant pas celle nécessaire à la seule finalité d'établissement de statistiques. »

IV – RÉPONSE AUX QUESTIONS PREJUDICIELLES POSEES

1) Sur les deux premières questions

12. Par ses deux premières questions, que le gouvernement français propose de traiter ensemble, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens que la durée de la période pour laquelle les autorités nationales ont accès à des données personnelles telles que des données relatives au trafic et des données de localisation, qui permettent 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 l'un des critères objectifs susceptibles de définir les circonstances et les conditions dans lesquelles un tel accès aux données des abonnés doit être accordé afin que les autorités nationales assurent la prévention, la recherche, la détection et la poursuite d'infractions pénales.

13. Le gouvernement français propose de répondre à cette question par l'affirmative.

14. En premier lieu, le gouvernement français entend rappeler que l'accès des autorités nationales compétentes aux données relatives au trafic et aux données de localisation dans le cadre de la lutte contre la criminalité doit être apprécié au regard du principe de proportionnalité garanti par l'article 52, paragraphe 1, de la Charte, qui encadre cet accès.

15. A cet égard, il n'est pas contestable que l'accès des autorités publiques à de telles données est constitutif d'une ingérence dans le droit fondamental au respect de la

vie privée, consacré à l'article 7 de la Charte, même en l'absence de circonstances permettant de qualifier cette ingérence de « grave » et sans qu'il importe que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de ladite ingérence. Un tel accès constitue également une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti à l'article 8 de la Charte, puisqu'il constitue un traitement de données à caractère personnel (voir arrêt du 2 octobre 2018, Ministerio fiscal, C-207/16, EU:C:2018:788, point 51 et jurisprudence citée).

16. Dès lors que l'accès à des données personnelles telles que les données de trafic et de localisation implique des ingérences dans les droits fondamentaux au respect de la vie privée et à la protection des données personnelles, l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de la directive 2002/58, qui sont susceptibles de justifier une règlementation nationale régissant l'accès des autorités publiques aux données conservées par les fournisseurs de services de communications électroniques et dérogeant, ainsi, au principe de confidentialité des communications électroniques, revêt un caractère exhaustif, de telle sorte que cet accès doit répondre effectivement et strictement à l'un de ces objectifs (voir arrêt Ministerio fiscal, précité, point 52 et jurisprudence citée).

17. Dans ce cadre, si le libellé de ces dispositions de la directive 2002/58 ne limite pas l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales à la lutte contre les seules infractions graves, mais vise les « infractions pénales » en général (voir arrêt Ministerio fiscal, précité, point 53), le principe de proportionnalité implique qu'une réglementation régissant les conditions dans lesquelles les fournisseurs de services de communications électroniques accordent aux autorités nationales compétentes l'accès à ces données personnelles doit assurer qu'un tel accès n'ait lieu que dans les limites du strict nécessaire (voir arrêt du 21 décembre 2016, Tele2 Sverige, C-203/15, EU:C:2016:970, points 115 et 116 ; voir arrêt Ministerio fiscal, précité, point 55).

18. En conséquence, l'objectif poursuivi par une réglementation nationale qui déroge au principe de confidentialité des données personnelles échangées dans le cadre de communications électroniques devant être en relation avec la gravité de l'ingérence dans les droits fondamentaux qu'entraîne cet accès, en matière de prévention, de recherche,

de détection et de poursuites d'infractions pénales, seule la lutte contre la criminalité grave est susceptible de justifier un accès des autorités publiques à des données à caractère personnel conservées par les fournisseurs de services de communications qui, prises dans leur ensemble, permettent de tirer des conclusions précises concernant la vie privée des personnes dont les données sont conservées (voir, en ce sens, arrêt Tele2 Sverige, précité, point 99).

19. En effet, conformément au principe de proportionnalité, une ingérence grave ne peut être justifiée, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, que par un objectif de lutte contre la criminalité devant également être qualifiée de « grave » (voir arrêt Ministerio fiscal, précité, point 56).

20. En revanche, lorsque l'ingérence que comporte un tel accès n'est pas grave, ledit accès est susceptible d'être justifié par un objectif de prévention, de recherche, de détection et de poursuite d' « infractions pénales » en général (voir arrêt Ministerio fiscal, précité, point 57).

21. A titre d'exemple, la Cour a jugé que l'accès d'autorités publiques aux données visant à l'identification des titulaires de cartes SIM activées avec un téléphone mobile volé, telles que les nom, prénom et, le cas échéant, adresse de ces titulaires, comportait une ingérence dans les droits fondamentaux de ces derniers, consacrés par la Charte, qui ne présente pas une gravité telle que cet accès devrait être limité, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, à la lutte contre la criminalité grave (voir arrêt Ministerio fiscal, précité, point 63).

22. Ainsi, c'est bien à la lumière du principe de proportionnalité, tel qu'interprété par la Cour, qui impose une relation entre, d'une part, l'objectif poursuivi par une règlementation régissant l'accès aux données à caractère personnel, et d'autre part, la gravité de l'ingérence dans les droits fondamentaux en cause que cet accès entraîne, qu'il convient d'examiner les questions posées par la juridiction de renvoi dans la présente affaire.

23. En deuxième lieu, le gouvernement français estime qu'il résulte de la jurisprudence de la Cour que l'appréciation du degré de gravité de l'ingérence que

comporte l'accès des autorités publiques à des données à caractère personnel résulte d'un examen concret des circonstances propres à chaque espèce, lesquelles peuvent inclure la durée de la période pour laquelle les autorités ont accès à ces données.

24. En effet, la Cour a jugé qu'il convenait de déterminer « en fonction des circonstances de l'espèce » si l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'un accès de la police judiciaire à des données personnelles telles que des données relatives au trafic et des données de localisation comporterait, doit être considérée comme étant « grave » (voir arrêt Ministerio fiscal, précité, point 58).

25. Or, si dans l'arrêt Ministerio fiscal, précité, la Cour a jugé que la nature des données en cause constituait un critère pertinent pour apprécier la gravité de l'ingérence selon que le type de données auxquelles les autorités compétentes accèdent permet, ou non, de tirer des conséquences précises sur la vie privée des personnes concernées, le gouvernement français estime qu'il en va de même de la durée pour laquelle l'accès aux données est sollicité.

26. Ainsi, pour déterminer si des données permettent de tirer des conclusions précises concernant la vie privée de personnes dont les données sont concernées, de sorte que l'accès à ces données doit être considéré comme une ingérence grave, la Cour, conformément aux conclusions de son avocat général, a tenu compte, dans son appréciation des circonstances de l'espèce qui étaient soumises à son examen dans l'affaire Ministerio fiscal, précitée, du fait que de telles données concernaient « une période déterminée » (voir, arrêt Ministerio fiscal, précité, point 60).

27. En effet, dans ses conclusions sur cette affaire, l'avocat général, M. Saugmandsgaard Øe, avait d'emblée relevé que la demande d'accès en cause dans ce litige portait « sur une période clairement définie et réduite dans le temps », à savoir une douzaine de jours, et avait pris en compte cette durée limitée pour souligner le caractère ciblé de cette mesure (voir, conclusions sur l'affaire Ministerio fiscal, EU:C:2018:300, points 33 et 84).

28. Ce faisant, la Cour a confirmé sa jurisprudence issue de l'avis 1/15, du 26 juillet 2017, relatif à l'Accord PNR UE – Canada (EU:C:2017:592), à l'occasion duquel

elle a évalué le caractère nécessaire des ingérences que comportait l'accord envisagé en examinant les modalités d'utilisation et de conservation des données à caractère personnel qui y étaient prévues, en particulier sous l'angle de la durée des mesures envisagées (voir points 194 et 207 à 209, ainsi que les conclusions, précitées, sur l'affaire Ministerio fiscal, note de bas de page 99).

29. En conséquence, la durée de la période pour laquelle les autorités nationales ont accès à des données personnelles, telles que des données relatives au trafic et des données de localisation qui permettent 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 l'un des critères objectifs susceptibles de définir les circonstances et les conditions dans lesquelles un tel accès aux données des abonnés peut être accordé, conformément au principe de proportionnalité garanti par l'article 52, paragraphe 1, de la Charte, afin que les autorités nationales assurent, notamment, la poursuite d'infractions pénales.

30. En troisième lieu, le Gouvernement français estime que les conditions matérielles et procédurales d'accès des autorités compétentes aux données à caractère personnel conservées par les fournisseurs de services de communications électroniques, qui incluent la définition de la notion de « criminalité grave » de nature à justifier un tel accès à des fins de prévention, de recherche, de détection et de poursuites d'infractions pénales ainsi que la détermination de la durée de la période sur laquelle peut porter cet accès, ne doivent pas être appréhendées comme des notions autonomes du droit de l'Union mais relèvent du législateur national, selon des critères objectifs qu'il lui appartient de définir, et doivent ensuite être laissées à l'appréciation des autorités judiciaires de chaque État membre en fonction de leur droit pénal matériel.

31. En effet, il résulte d'une jurisprudence constante que, pour autant que le droit de l'Union, y compris les principes généraux de celui-ci, ne comporte pas de règles communes, la mise en œuvre d'une réglementation européenne par les autorités nationales compétentes doit suivre les règles de procédure et de forme prévues par le droit de l'État membre concerné, sous réserve que le recours aux règles nationales s'effectue dans la

mesure nécessaire à l'exécution des dispositions du droit de l'Union et pour autant que l'application de ces règles nationales ne porte pas atteinte à la portée et à l'efficacité de ce droit, y compris des principes généraux de celui-ci (voir arrêt du 19 septembre 2002, Huber, C-336/00, EU:C:2002:509, point 61 et jurisprudence citée ; également, arrêt du 11 février 1971, Norddeutsches Vieh- und Fleischkontor / Hauptzollamt Hamburg St Annen, C-39/70, EU:C:1971:16, point 4).

32. Dans ce cadre, la Cour a expressément jugé qu'afin de garantir que l'accès des autorités nationales compétentes aux données conservées soit limité au strict nécessaire, il appartient au droit national de déterminer, en se fondant sur des critères objectifs, les circonstances et les conditions matérielles et procédurales dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données des abonnés ou des utilisateurs inscrits (voir arrêt Tele2 Sverige, précité, points 118 et 119).

33. Ces conditions matérielles incluent, d'une part, les critères objectifs permettant de délimiter les infractions pouvant être considérées comme suffisamment graves pour justifier une ingérence grave dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, d'autre part, les catégories de données auxquelles l'accès peut être autorisé et la durée de la période sur laquelle peut porter un tel accès, au regard de l'ampleur et de la gravité de l'ingérence dans les droits fondamentaux précités que constitue cet accès.

34. A cet égard, il ressort du point 41 de l'arrêt Digital Rights Ireland, précité, que la Cour a dégagé la notion de « criminalité grave », en interprétant la notion « d'infractions graves » contenue à l'article 1er, paragraphe 1, de la directive 2006/24. Dans l'arrêt Tele2 Sverige, précité, la Cour a ensuite repris cette notion dans le cadre de la directive 2002/58, sans la repréciser.

35. Or l'article 1er, paragraphe 1, de la directive 2006/24, qui définissait l'objectif matériel de cette directive comme visant à garantir la disponibilité des données de connexion à des fins de recherche, de détection et de poursuites d'infractions graves, opérait un renvoi exprès aux droits nationaux en ce qui concerne la définition de telles infractions. En outre, la notion de « criminalité grave » retenue par la Cour dans les arrêts Digital Rights Ireland et Tele2 Sverige, précités, n'apparaît ni dans la directive 2002/58 ni

dans la règlementation générale de l'Union en matière de protection des données à caractère personnel[1], ni dans aucune législation pertinente en matière de protection des données à caractère personnel autre que la directive 2006/24.

36. Il s'en déduit que le législateur de l'Union a délibérément reconnu aux Etats membres la compétence de définir les infractions pénales qu'ils jugent suffisamment graves, au sens de leur droit pénal matériel, pour justifier l'accès des autorités nationales compétentes aux données conservées par les fournisseurs de services de communications électroniques. Il en va a fortiori de même s'agissant de la durée de la période sur laquelle peut être accordé cet accès, qui ne fait l'objet d'aucune disposition de droit de l'Union.

37. Dans ces conditions, en l'absence d'harmonisation du droit pénal matériel des Etats membres pour la mise en œuvre de la législation relative à la protection des données à caractère personnel conservées par les fournisseurs de services de communications électroniques, la notion de « criminalité grave » ne peut pas faire l'objet d'une interprétation uniforme sur le territoire de l'ensemble des Etats membres et ne peut donc pas être considérée comme une notion autonome du droit de l'Union, au sens de la jurisprudence de la Cour (voir, par exemple, arrêt du 24 mai 2016, Dworzecki, C-108/16 PPU, EU:C:2016:346, point 28 et jurisprudence citée). De même, la durée pertinente de la période sur laquelle peut porter l'accès des autorités compétentes à de telles données ne saurait faire l'objet d'une appréciation uniforme sur le territoire de l'ensemble des Etats membres.

38. Par suite, il y a lieu de tenir compte de l'intention du législateur de l'Union de reconnaître, d'une part, aux législateurs nationaux la compétence pour définir, dans leur droit pénal matériel, selon des critères objectifs qu'il leur appartient de

---

[1] C'est-à-dire la directive 95/46, le règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) et la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

déterminer, les types d'infractions qu'ils estiment relever de la criminalité grave, d'autre part, aux autorités judiciaires nationales le pouvoir d'apprécier, *in concreto*, si les infractions en cause sont suffisamment graves pour justifier l'accès des autorités nationales compétentes aux données conservées par les fournisseurs de services de communications électroniques et pour apprécier la durée de la période sur laquelle un tel accès est autorisé.

39. A titre subsidiaire, si la Cour devait juger qu'il résulte du point 60 de l'arrêt Digital Rights Ireland, précité, qu'il lui appartient, en l'absence d'intervention du législateur de l'Union, de définir des critères objectifs délimitant le domaine de la « criminalité grave » au sens et pour l'application de l'article 15, paragraphe 1, de la directive 2002/58, de tels critères objectifs ne sauraient, en tout état de cause, avoir pour conséquence de se substituer à la compétence nationale et de faire obstacle à la marge d'appréciation des Etats membres pour définir les types d'infractions susceptibles de relever de ce domaine (voir, par analogie dans le contexte de la décision-cadre 2001/220/JAI[2], arrêt du 21 octobre 2010, Eredics et Sápi, C-205/09, EU:C:2010:623, points 37 à 39, et arrêt du 15 septembre 2011, Gueye et Salmerón Sánchez, C-483/09, EU:C:2011:583, point 75).

40. Dans ce cadre, la notion de « criminalité grave » devrait être interprétée, dans le respect de la marge d'appréciation dont disposent les Etats membres, au regard d'un ensemble de critères objectifs alternatifs tels que, notamment, l'existence d'une peine privative de liberté, le caractère intentionnel de l'infraction, les circonstances aggravantes de l'infraction, la récidive ou encore la nature et l'ampleur des préjudices causés et des intérêts sociaux méconnus[3]. De même, les Etats membres devraient disposer d'une large marge d'appréciation pour la détermination des catégories de données auxquelles l'accès

---

[2] Décision-cadre du Conseil, du 15 mars 2001, relative au statut des victimes dans le cadre de procédures pénales (2001/220/JAI).

[3] A ce titre, s'il va de soi que les atteintes portées aux intérêts fondamentaux de la nation, aux institutions ou à l'intégrité du territoire national relèvent, par nature, du domaine de la criminalité grave, les atteintes portées à la vie, à l'intégrité physique ou psychique et à la dignité des personnes devraient également constituer des critères objectifs pertinents aux fins de définir la notion de « criminalité grave ». De même, les atteintes aux biens entraînant un préjudice patrimonial important pour la victime devraient pouvoir relever de ce domaine. Enfin, la gravité d'une infraction peut tenir au fait qu'elle s'inscrive dans un phénomène sériel, portant une atteinte répétée à l'ordre public.

des autorités est susceptible de constituer une ingérence grave dans les droits fondamentaux de la personne concernée ainsi que pour la définition de la durée de la période sur laquelle porte un tel accès.

41. En quatrième et dernier lieu, le gouvernement français entend démontrer que si l'accès aux données de trafic et de localisation conservées par les fournisseurs de communications électroniques sur une certaine période est justifié et indispensable en matière de lutte contre la criminalité grave, notamment en matière de terrorisme, un tel accès s'avère également capital, au quotidien, pour la lutte contre la criminalité de droit commun, de sorte que le critère tiré de la durée d'accès aux données ne saurait être apprécié indépendamment des autres circonstances qui président à la demande d'accès, afin d'examiner le caractère strictement proportionné de cette ingérence.

42. A cet égard, la Cour a constaté que, compte tenu de l'importance croissante des moyens de communication électronique, les données de trafic et de localisation permettaient aux autorités nationales compétentes en matière de poursuites pénales de disposer de possibilités supplémentaires d'élucidation des infractions graves et constituaient donc un instrument utile pour les enquêtes pénales. Ainsi, elle a considéré que la conservation de telles données était apte à réaliser l'objectif de lutte contre la criminalité grave et le terrorisme international afin de garantir la sécurité publique (voir arrêt Digital Rights Ireland e.a., précité, point 49).

43. Or il convient d'indiquer que la limitation systématique de l'accès des autorités compétentes aux données de trafic et de localisation pour une durée particulièrement réduite, telle que celle mentionnée au point 23 de la décision de renvoi, dans le cadre des enquêtes portant sur des faits de criminalité qui ne sauraient être caractérisés comme graves ou particulièrement graves, comme c'est le cas dans le litige au principal, porterait gravement atteinte à l'efficacité d'un grand nombre d'enquêtes pour lesquelles les autorités compétentes, aux fins de manifestation de la vérité, doivent disposer d'un accès aux mêmes données pour une période plus longue.

44. Il en va ainsi, en particulier, dans les situations suivantes.

45. D'une part, en cas de disparition inquiétante d'une personne, notamment d'un mineur, les enquêteurs, par définition, ne connaissent pas la date exacte de la disparition et doivent être en capacité de remonter dans le temps sur une période de plus d'un jour afin de reconstituer la localisation et les derniers faits et gestes connus de cette personne et d'identifier les derniers contacts qu'elle a eus, ce alors qu'une telle disparition peut s'avérer, in fine, dépourvue d'un caractère de gravité au sens du droit pénal, comme lorsque la disparition correspond à une fugue.

46. D'autre part, les enquêteurs ont besoin d'un accès aux données de trafic et de localisation pour une période plus longue qu'une simple journée lorsque la nature de l'infraction est précisément définie par la répétition du comportement délictuel, par exemple, en matière de harcèlement ou d'appels téléphoniques ou messages électroniques malveillants répétés, notamment entre conjoints, ou lorsque les faits ont été réitérés, comme cela est le cas dans le litige au principal.

47. Enfin, il en va de même lorsque les modalités de participation à l'infraction impliquent une entente préalable et donc des échanges en amont de la commission d'une infraction, par exemple pour les associations de malfaiteurs, les trafics de stupéfiants ou de simples complicités.

48. A cet égard, il convient de garder à l'esprit qu'au commencement de l'enquête, le degré de gravité de l'infraction susceptible d'avoir été commise n'apparaît pas nécessairement aux enquêteurs, et que des faits a priori dépourvus de gravité peuvent révéler, in fine, la commission d'actes particulièrement graves, d'où l'importance de ménager la possibilité pour les enquêteurs d'accéder à des données pour une durée plus ou moins longue, selon les situations auxquelles ils sont confrontés.

49. A titre d'exemple, le gouvernement français souhaite citer un cas réel, datant de septembre 2018, caractérisé par la disparition inquiétante d'une jeune femme de vingt ans dans l'Est de la France. Une information judiciaire a été ouverte. Grâce aux réquisitions en matière de téléphonie, effectuées sur une période de temps de plusieurs jours, un suspect qui ne faisait pas partie de l'entourage de la victime a pu être identifié. Cette personne était entrée en contact avec la victime à la faveur d'une recherche d'appartement. Grâce à cette identification, une perquisition a été diligentée au domicile de

ce suspect : des traces de sang abondantes comportant l'ADN de la victime y ont été retrouvées. Il a été mis en examen des chefs d'assassinat, enlèvement et séquestration.

50. En conclusion, si l'accès aux données de trafic et de localisation conservées par les fournisseurs de communications électroniques sur une certaine période est justifié et indispensable en matière de lutte contre la criminalité grave, notamment en matière de terrorisme, un tel accès s'avère également capital, au quotidien, pour la lutte contre la criminalité de droit commun.

51. Dans ce cadre, seules les législations des Etats membres sont à même de garantir, lors de la détermination des modalités d'accès aux données de trafic et de localisation, l'efficacité de ce dispositif aux fins d'assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales, en précisant les durées des périodes pour lesquelles les autorités compétentes doivent pouvoir accéder aux données de trafic et de localisation en fonction des situations auxquelles ces autorités sont confrontées, et ce dans le strict respect du principe de proportionnalité.

52. En conséquence, le gouvernement français propose de répondre aux première et deuxième questions posées par la juridiction de renvoi en ce sens que la durée de la période pour laquelle les autorités nationales ont accès à des données personnelles telles que des données relatives au trafic et des données de localisation, qui permettent 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 l'un des critères objectifs susceptibles de définir les circonstances et les conditions dans lesquelles un tel accès aux données des abonnés peut être accordé, conformément au principe de proportionnalité garanti par l'article 52, paragraphe 1, de la Charte, afin que les autorités nationales assurent, notamment, la poursuite d'infractions pénales.

2) Sur la troisième question

53. Par sa troisième question, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, tel qu'interprété par la Cour dans son arrêt Tele2 Sverige, précité, doit être interprété en ce sens que le ministère public d'un Etat membre tel que celui en cause dans le litige au principal peut être regardé comme l'autorité chargée du contrôle préalable de l'accès des autorités nationales compétentes aux données personnelles conservées par les fournisseurs de services de communications électroniques, lorsqu'un tel accès vise à assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales, y compris lorsqu'il représente l'action publique au cours de la procédure judiciaire ultérieure.

54. Le gouvernement français propose de répondre à cette question par l'affirmative.

55. A titre liminaire, le gouvernement français estime utile de rappeler que les garanties exigées des autorités désignées par les Etats membres pour exercer le contrôle préalable de l'accès des autorités nationales compétentes aux données à caractère personnel conservées par les fournisseurs de services de communications électroniques, au sens et pour l'application de l'article 15, paragraphe 1, de la directive 2002/58, doivent être définies dans le respect du principe de l'autonomie institutionnelle des Etats membres.

56. En effet, il résulte de la jurisprudence constante de la Cour qu'en vertu du principe d'autonomie institutionnelle, lorsque des dispositions du droit de l'Union reconnaissent des pouvoirs aux Etats membres ou leur imposent des obligations aux fins de l'application de ce droit, la question de savoir de quelle façon l'exercice de ces pouvoirs et l'exécution de ces obligations peuvent être confiés par les Etats à des organes déterminés relève uniquement du système constitutionnel de chaque Etat (voir arrêt du 15 décembre 1971, International Fruit Company, C-51/71, EU:C:1971:128, point 4).

57. En premier lieu, il convient de préciser le contexte et la portée de l'obligation, qui incombe aux Etats membres, d'instituer un contrôle suffisant de l'accès aux données personnelles, lors de la mise en œuvre des mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58.

58. A cet égard, afin de garantir que l'accès des autorités nationales compétentes aux données conservées soit limité au strict nécessaire, la Cour a jugé essentiel que l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifiés, 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 intervienne 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 (voir arrêt Tele2 Sverige, précité, point 120 et jurisprudence citée).

59. Ce faisant, le gouvernement français estime que la Cour n'a pas entendu limiter la faculté d'autoriser un tel accès aux seules autorités des Etats membres qui présenteraient la qualité de « juridiction » ou d' « entité administrative indépendante », mais a entendu viser toute autorité présentant les garanties d'indépendance adéquates.

60. A cet égard, il y a lieu de relever que dans ses conclusions sous l'arrêt Digital Rights Ireland, précité, qui a posé cette exigence en son point 62, l'avocat général M. Cruz Villalón faisait valoir que toute demande d'accès devait à tout le moins être soumise au contrôle « des autorités judiciaires ou d'autorités indépendantes », les autorités ainsi visées excédant le champ des seules juridictions ou autorités administratives indépendantes (EU:C:2013:845, point 127). De même, dans ses conclusions précitées sous l'arrêt Tele2 Sverige, précité, l'avocat général M. Saugmandsgaard Øe, évoque un « contrôle indépendant », par une « entité indépendante », sans le réserver à des juridictions ou entités administratives indépendantes (points 233 à 236).

61. En outre, il convient de rappeler que la Cour s'est directement inspirée, ainsi que l'y invitait l'avocat général, M. Cruz Villalón, dans ses conclusions sous l'arrêt Digital Rights, précité, de la jurisprudence de la Cour européenne des droits de l'Homme (ci-après, la « Cour EDH ») (voir conclusions, point 109).

62. En effet, si l'interprétation de la directive 2002/58 doit être opérée au regard uniquement des droits fondamentaux garantis par la Charte, et si, conformément à son article 52, paragraphe 3, la Charte ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue que la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après, la « CEDH ») (voir arrêt Tele2

Sverige, précité, points 128 et 129), il n'en demeure pas moins que les limitations susceptibles d'être légitimement apportées au droit à la protection des données à caractère personnel reconnu par l'article 8 de la Charte correspondent à celles tolérées dans le cadre de l'article 8 de la CEDH, ainsi que la Cour l'a jugé dans l'arrêt du 9 novembre 2010, Volker und Markus Schecke et Eifert (C-92/09 et C-93/09, EU:C:2010:662, point 52).

63. A cet égard, il résulte d'une jurisprudence constante de la Cour EDH qu'un dispositif permettant aux autorités de l'Etat d'accéder aux données à caractère personnel pour des motifs de sécurité publique n'exige pas la mise en œuvre d'une autorisation préalable par une autorité judiciaire (voir Cour EDH, 6 septembre 1978, Klass e.a. c. Allemagne, CE:ECHR:1978:0906JUD000502971, § 51 ; 29 juin 2006, Weber et Saravia c. Allemagne, CE:ECHR:2010:0427JUD002303902, § 115 ; 18 mai 2010, Kennedy c. Royame-Uni, CE:ECHR:2010:0518JUD002683905, § 31 ; 4 décembre 2015, Zakharov c. Russie, CE:ECHR:2015:1204JUD004714306, §249 et §258).

64. En effet, si la Cour EDH relève qu'une autorisation judiciaire préalable constitue une garantie importante contre l'arbitraire, il ne s'agit toutefois pas d'une exigence dont l'exclusion outrepasserait les limites de ce qui peut être jugé nécessaire dans un cadre démocratique, dès lors que l'organe compétent est suffisamment indépendant à l'égard de l'exécutif (voir arrêts de la Cour EDH du 26 avril 2007, Dumitru Popescu c. Roumanie (n°2), CE:ECHR:2007:0426JUD007152501, § 71 ; Zakharov c. Russie, précité, §249 et §258 ; du 12 janvier 2016, Szabó et Vissy c. Hongrie, CE:HCR:2016:0112JUD003713814, §§ 77 et 80 ; du 19 juin 2018, Centrum för Rättvisa c. Suède, CE:ECHR:2018:0619JUD003525208 ; du 13 septembre 2018, Big Brother Watch, CE:ECHR:2018:0913JUD005817013, §§ 309 et 318).

65. <u>En deuxième lieu</u>, et au regard de ce contexte jurisprudentiel, le gouvernement français estime nécessaire de préciser les exigences d'indépendance qui incombent à l'autorité chargée du contrôle préalable de l'accès aux données personnelles conservées par les fournisseurs de services de communications électroniques, au sens et pour l'application de l'article 15, paragraphe 1, de la directive 2002/58.

66. A cet égard, il apparaît d'emblée, au vu de la jurisprudence de la Cour EDH ainsi que du libellé même des arrêts de la Cour, qui permettent de confier cette

mission de contrôle préalable tant à une « juridiction » qu'à une « entité administrative indépendante », que les exigences d'indépendance qui incombent à cette autorité ne sauraient être strictement identiques à celles requises d'une juridiction au sens de l'article 6, paragraphe 1, de la CEDH et de l'article 47 de la Charte.

67. En effet, conformément à l'article 47 de la Charte, tel qu'interprété notamment par la Cour dans ses arrêts du 27 février 2018, Associação Sindical dos Juízes Portugueses, C-64/16 (EU:C:2018:117) et du 25 juillet 2018, LM., C-216/18 (EU:C:2018:586), l'exigence d'indépendance des juges, qui relève du contenu essentiel du droit fondamental à un procès équitable, est inhérente à la mission de juger.

68. Cette exigence s'impose donc uniquement aux instances qui relèvent de la catégorie de « juridiction » au sens défini par le droit de l'Union, appelées à prononcer des jugements. Elle ne saurait en revanche s'étendre à une « entité administrative » laquelle peut être rattachée, d'un point de vue institutionnel, à une autorité relevant du pouvoir exécutif.

69. Par conséquent, le gouvernement français estime que la notion d'indépendance qui doit caractériser l'entité administrative au sens et pour l'application de l'article 15, paragraphe 1, de la directive 2002/58 s'entend comme une autonomie fonctionnelle, qui doit permettre à cette entité d'assurer le contrôle préalable de l'accès aux données personnelles par les autorités nationales compétentes, sans interventions ni pressions extérieures susceptibles d'influencer ses décisions, ainsi que dans le respect de l'objectivité et de la stricte application de la règle de droit.

70. Une telle analyse est corroborée par l'exigence d'indépendance à l'égard du pouvoir exécutif qui, conformément à la jurisprudence de la Cour EDH citée aux points 63 et 64 des présentes observations, incombe à une telle entité administrative, et qui implique qu'elle soit séparée du pouvoir exécutif, de la même manière que, dans le cadre d'une société démocratique, le principe de séparation des pouvoirs implique la séparation des pouvoirs exécutif et judiciaire.

71. En troisième lieu, et au regard des observations qui précèdent, le gouvernement français estime que le ministère public d'un Etat membre, tel que celui en

cause dans le litige au principal, présente des garanties d'indépendance suffisantes pour assurer, en conformité avec le droit de l'Union, le contrôle préalable de l'accès des autorités nationales aux données personnelles lorsqu'un tel accès est nécessaire aux fins d'assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.

72. A cet égard, ainsi que l'a relevé la Cour à plusieurs reprises, le ministère public est une autorité appelée à participer à l'administration de la justice dans l'ordre juridique des Etats membres, alors même que les décisions émanant d'une telle autorité sont adoptées sans l'intervention d'une juridiction et ne prennent pas la forme d'un jugement (voir, en ce sens, arrêts du 11 février 2003, Gözütok et Brügge, point 28, C-187/01 et C-385/01, EU:C:2003:87 ; du 29 juin 2016, Kossowski, C-486/14, EU:2016:483, point 39).

73. De même, la Cour a relevé qu'une telle autorité exerce librement son action, conformément au principe de séparation des pouvoirs exécutif et judiciaire qui caractérise le fonctionnement d'un Etat de droit (voir, en ce sens, arrêt du 10 novembre 2016, Özçelik, C-453/16 PPU, EU:C:2016:860, point 34, et jurisprudence citée). Elle présente ainsi les garanties d'indépendance exposées au point 69 des présentes observations.

74. En outre, il convient d'indiquer que la Cour EDH a jugé que, eu égard à ses fonctions, le ministère public ne saurait être astreint aux obligations d'indépendance et d'impartialité que l'article 6 de la CEDH impose à un « tribunal », c'est-à-dire un organe juridictionnel appelé à trancher, sur la base de normes de droit et à l'issue d'une procédure organisée, toute question relevant de sa compétence (voir arrêt du 18 octobre 2018, Thiam c. France, n° 80018/12, CE:ECHR:2018:1018JUD008001812, point 71).

75. Elle ajoute que ce n'est que sous l'angle de l'article 5, paragraphe 3, de la CEDH s'agissant du contrôle juridictionnel d'une privation de liberté, et non sous l'angle de l'article 6 de la CEDH que s'imposent les exigences d'indépendance et d'impartialité à l'égard de l'exécutif qui incombent aux membres du ministère public (voir arrêts de la Cour EDH Thiam c. France, précité, point 70 ; du 29 mars 2001, Thoma c. Luxembourg, CE:ECHR:2001:0329JUD003843297 ; du 4 octobre 2007, Nastase-Silivestru c. Roumanie,

CE:ECHR:2007:1004JUD007478501 ; du 10 janvier 2013, Agnelet c. France, CE:ECHR:2013:0110JUD006119808).

76. Or le contrôle de l'accès des autorités compétentes, et notamment des services de police, à des données de communications électroniques dans le cadre d'une procédure pénale, ne saurait être assimilé au contrôle juridictionnel d'une privation de liberté.

77. En particulier, il ne résulte ni de l'article 6 de la CEDH, ni des dispositions correspondantes de l'article 47 de la Charte, que le principe d'impartialité, au sens restreint de l'égale distance du juge par rapport aux parties au litige et à leurs intérêts respectifs au regard de l'objet de celui-ci (arrêt LM, précité, point 65 et jurisprudence citée), ferait obstacle à ce que le ministère public autorise, au titre de ses pouvoirs d'instruction et d'enquête, un tel accès et représente l'action publique au cours de la procédure judiciaire ultérieure.

78. Ainsi, si la Cour EDH a jugé qu'un magistrat chargé de l'enquête ne saurait intervenir dans une procédure pénale ultérieure en qualité de partie poursuivante sans que son indépendance et son impartialité puissent paraître, objectivement, sujettes à caution, c'est au regard des seules dispositions de l'article 5, paragraphe 3, de la CEDH qui impliquent qu'un magistrat judiciaire au sens de cet article, doit remplir certaines conditions d'indépendance, y compris à l'égard des parties, afin de représenter, pour la personne détenue, des garanties contre l'arbitraire ou la privation injustifiée de liberté (voir arrêt du 5 avril 2001, H.B. c. Suisse, CE:ECHR:2001:0405JUD002689995, §§ 55, 62 et 64).

79. En revanche, la Cour EDH a jugé, au regard des dispositions de l'article 8 de la CEDH, garantissant le droit au respect de la vie privée, que les autorités de poursuite telles que les autorités de police peuvent prendre des mesures en vue de la surveillance d'un suspect et porter ainsi atteinte à sa vie privée, sans autorisation préalable d'un tribunal, pourvu que dans la procédure pénale ultérieure menée contre la personne concernée, les juridictions pénales puissent contrôler la légalité d'une telle mesure de surveillance, et si celle-ci était jugée illégale, aient la faculté d'exclure les éléments ainsi

obtenus du procès (voir arrêt du 2 septembre 2010, Uzun c. Allemagne, CE:ECHR:2010:0902JUD003562305, § 71).

80. Ainsi, la Cour EDH estime qu'un tel contrôle judiciaire constitue une garantie suffisante, en ce qu'elle décourage les autorités d'enquête de recueillir des preuves par des moyens illégaux. Si elle juge qu'au contraire, des mesures telles que des écoutes téléphoniques requièrent, en application de l'article 8 de la CEDH, la délivrance d'un mandat par un organe indépendant, une telle solution n'est aucunement transposable au cas de l'accès des autorités compétentes aux données de trafic et de localisation, aux fins d'enquêtes et de poursuites pénales, qui ne permet pas de révéler le contenu des communications en cause, et n'est pas, par conséquent, aussi attentatoire à la vie privée des personnes que des écoutes téléphoniques (voir arrêt Uzun c. Allemagne, précité, § 72).

81. Il résulte de tout ce qui précède que le gouvernement français propose de répondre à la troisième question posée par la juridiction de renvoi en ce sens que l'article 15, paragraphe 1, de la directive 2002/58, tel qu'interprété par la Cour dans son arrêt Tele2 Sverige, précité, doit être interprété en ce sens que le ministère public d'un Etat membre tel que celui en cause dans le litige au principal peut être regardé comme l'autorité chargée du contrôle préalable de l'accès des autorités nationales compétentes aux données personnelles conservées par les fournisseurs de services de communications électroniques, lorsqu'un tel accès vise à assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales, y compris lorsqu'il représente l'action publique au cours de la procédure judiciaire ultérieure.

*

82. Par ces motifs, le gouvernement français propose à la Cour de répondre aux questions posées par la juridiction de renvoi que :

« 1. La durée de la période pour laquelle les autorités nationales ont accès à des données personnelles telles que des données relatives au trafic et des données de localisation, qui permettent 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 l'un des critères objectifs susceptibles de définir les circonstances et les conditions dans lesquelles un tel accès aux données des abonnés peut être accordé, conformément au principe de proportionnalité garanti par l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, afin que les autorités nationales assurent, notamment, la poursuite d'infractions pénales.

2. L'article 15, paragraphe 1, de la directive 2002/58, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), tel qu'interprété par la Cour dans son arrêt du 21 décembre 2016, Tele2 Sverige, C-203/15 et C-698/15, doit être interprété en ce sens que le ministère public d'un Etat membre tel que celui en cause dans le litige au principal peut être regardé comme l'autorité chargée du contrôle préalable de l'accès des autorités nationales compétentes aux données personnelles conservées par les fournisseurs de services de communications électroniques, lorsqu'un tel accès vise à assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales, y compris lorsqu'il représente l'action publique au cours de la procédure judiciaire ultérieure. »

Diego COLAS Esther de MOUSTIER Damien DUBOIS

Agents du gouvernement français