Recueil de la jurisprudence

ARRÊT DE LA COUR (grande chambre)

2 mars 2021 *

« Renvoi préjudiciel – Traitement des données à caractère personnel dans le secteur des communications électroniques – Directive 2002/58/CE – Fournisseurs de services de communications électroniques – Confidentialité des communications – Limitations – Article 15, paragraphe 1 – Articles 7, 8 et 11 ainsi que article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne – Législation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation par les fournisseurs de services de communications électroniques – Accès des autorités nationales aux données conservées à des fins d'enquêtes – Lutte contre la criminalité en général – Autorisation donnée par le ministère public – Utilisation des données dans le cadre du procès pénal en tant qu'éléments de preuve – Recevabilité »

Dans l'affaire C-746/18,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par la Riigikohus (Cour suprême, Estonie), par décision du 12 novembre 2018, parvenue à la Cour le 29 novembre 2018, dans la procédure pénale contre

H. K.,

en présence de :

Prokuratuur,

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M^me^ R. Silva de Lapuerta, vice–présidente, MM. J.–C. Bonichot, A. Arabadjiev, M^me^ A. Prechal et M. L. Bay Larsen, présidents de chambre, MM. T. von Danwitz (rapporteur), M. Safjan, M^me^ K. Jürimäe, MM. C. Lycourgos et P. G. Xuereb, juges,

avocat général : M. G. Pitruzzella,

greffier : M^me^ C. Strömholm, administratrice,

vu la procédure écrite et à la suite de l'audience du 15 octobre 2019,

considérant les observations présentées :

– pour H. K., par M^e^ S. Reinsaar, vandeadvokaat,

– pour le Prokuratuur, par M. T. Pern et M^me^ M. Voogma, en qualité d'agents,

– pour le gouvernement estonien, par M^me^ N. Grünberg, en qualité d'agent,

* Langue de procédure : l'estonien.

– pour le gouvernement danois, par M. J. Nymann-Lindegren et M^me^ M. S. Wolff, en qualité d'agents,

– pour l'Irlande, par M^mes^ M. Browne, G. Hodge et J. Quaney ainsi que par M. A. Joyce, en qualité d'agents, assistés de M. D. Fennelly, barrister,

– pour le gouvernement français, initialement par MM. D. Dubois et D. Colas ainsi que par M^mes^ E. de Moustier et A.-L. Desjonquères, puis par M. D. Dubois ainsi que par M^mes^ E. de Moustier et A.-L. Desjonquères, en qualité d'agents,

– pour le gouvernement letton, initialement par M^mes^ V. Kalniņa et I. Kucina, puis par M^mes^ V. Soņeca et V. Kalniņa, en qualité d'agents,

– pour le gouvernement hongrois, par M. M. Z. Fehér et M^me^ A. Pokoraczki, en qualité d'agents,

– pour le gouvernement polonais, par M. B. Majczyna, en qualité d'agent,

– pour le gouvernement portugais, par M. L. Inez Fernandes ainsi que par M^mes^ P. Barros da Costa, L. Medeiros et I. Oliveira, en qualité d'agents,

– pour le gouvernement finlandais, par M. J. Heliskoski, en qualité d'agent,

– pour le gouvernement du Royaume-Uni, par M. S. Brandon et M^me^ Z. Lavery, en qualité d'agents, assistés de M. G. Facenna, QC, et de M. C. Knight, barrister,

– pour la Commission européenne, initialement par MM. H. Kranenborg et M. Wasmeier ainsi que par M^mes^ P. Costa de Oliveira et K. Toomus, puis par MM. H. Kranenborg et M. Wasmeier ainsi que par M^me^ E. Randvere, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 21 janvier 2020,

rend le présent

Arrêt

1 La demande de décision préjudicielle porte sur l'interprétation de 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) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après 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 des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

2 Cette demande a été présentée dans le cadre d'une procédure pénale engagée contre H. K. des chefs de vol, d'utilisation de la carte bancaire d'un tiers et de violence à l'égard de personnes participant à une procédure en justice.

Le cadre juridique

Le droit de l'Union

3 Les considérants 2 et 11 de la directive 2002/58 énoncent :

« (2) La présente directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la [Charte]. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de [celle-ci].

[...]

(11) À l'instar de 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 (JO 1995, L 281, p. 31)], 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 [de l'Union]. 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 [signée à Rome le 4 novembre 1950], 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. »

4 Selon l'article 2 de la directive 2002/58, intitulé « Définitions » :

« Sauf disposition contraire, les définitions figurant dans la directive [95/46] et dans la directive 2002/21/CE du Parlement européen et du Conseil du 7 mars 2002 relative à un cadre réglementaire commun pour les réseaux et les services de communications électroniques (directive "cadre") [(JO 2002, L 108, p. 33),] s'appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables :

a) "utilisateur" : toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;

b) "données relatives au trafic" : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation ;

c) "données de localisation" : toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ;

d) "communication" : toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit ;

[...] »

5 Aux termes de l'article 5 de la directive 2002/58, intitulé « Confidentialité des communications » :

« 1. Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1. Le présent paragraphe n'empêche pas le stockage technique nécessaire à l'acheminement d'une communication, sans préjudice du principe de confidentialité.

[...]

3. Les États membres garantissent que le stockage d'informations, ou l'obtention de l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur n'est permis qu'à condition que l'abonné ou l'utilisateur ait donné son accord, après avoir reçu, dans le respect de la directive [95/46], une information claire et complète, entre autres sur les finalités du traitement. Cette disposition ne fait pas obstacle à un stockage ou à un accès techniques visant exclusivement à effectuer la transmission d'une communication par la voie d'un réseau de communications électroniques, ou strictement nécessaires au fournisseur pour la fourniture d'un service de la société de l'information expressément demandé par l'abonné ou l'utilisateur. »

6 L'article 6 de la directive 2002/58, intitulé « Données relatives au trafic », dispose :

« 1. Les données relatives au trafic concernant les abonnés et les utilisateurs traitées et stockées par le fournisseur d'un réseau public de communications ou d'un service de communications électroniques accessibles au public doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires à la transmission d'une communication sans préjudice des paragraphes 2, 3 et 5, du présent article ainsi que de l'article 15, paragraphe 1.

2. Les données relatives au trafic qui sont nécessaires pour établir les factures des abonnés et les paiements pour interconnexion peuvent être traitées. Un tel traitement n'est autorisé que jusqu'à la fin de la période au cours de laquelle la facture peut être légalement contestée ou des poursuites engagées pour en obtenir le paiement.

3. Afin de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d'un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1 dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services, pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.

[...]

5. Le traitement des données relatives au trafic effectué conformément aux dispositions des paragraphes 1, 2, 3 et 4 doit être restreint aux personnes agissant sous l'autorité des fournisseurs de réseaux publics de communications et de services de communications électroniques accessibles au public qui sont chargées d'assurer la facturation ou la gestion du trafic, de répondre aux demandes de la clientèle, de détecter les fraudes et de commercialiser les services de communications électroniques ou de fournir un service à valeur ajoutée ; ce traitement doit se limiter à ce qui est nécessaire à de telles activités.

[...] »

7 L'article 9 de la directive 2002/58, intitulé « Données de localisation autres que les données relatives au trafic », prévoit, à son paragraphe 1 :

« Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. [...] »

8 L'article 15 de ladite directive, intitulé « Application de certaines dispositions de la directive [95/46] », énonce, à son paragraphe 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]. 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 [de l'Union], y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne. »

Le droit estonien

La loi relative aux communications électroniques

9 L'article 111[1] de l'elektroonilise side seadus (loi relative aux communications électroniques, RT I 2004, 87, 593 ; RT I, 22.05.2018, 3), dans sa rédaction applicable aux faits au principal (ci-après la « loi relative aux communications électroniques »), intitulé « Obligation de conserver les données », prévoit :

« [...]

(2) Les fournisseurs de services de téléphonie fixe et de téléphonie mobile et de réseau de services de téléphonie fixe et de téléphonie mobile sont tenus de conserver les données suivantes :

1) le numéro de l'appelant et le nom et l'adresse de l'abonné ;

2) le numéro de l'appelé et le nom et l'adresse de l'abonné ;

3) en cas de services complémentaires, tels que le renvoi ou le transfert d'appel, le numéro composé et le nom et l'adresse de l'abonné ;

4) la date et l'heure du début et de la fin de l'appel ;

5) le service de téléphonie fixe ou mobile utilisé ;

6) l'identité internationale de l'abonné mobile (*International Mobile Subscriber Identity* – IMSI) de l'appelant et de l'appelé ;

7) l'identité internationale d'équipement mobile (*International Mobile Equipment Identity* – IMEI) de l'appelant et de l'appelé ;

8) l'identifiant cellulaire au moment du début de l'appel ;

9) les données identifiant la localisation géographique de la cellule par référence à l'identifiant cellulaire au cours de la période pendant laquelle les données sont conservées ;

10) en cas de services de téléphonie mobile anonymes à prépaiement, la date et l'heure de la première activation du service ainsi que l'identité de localisation d'où le service a été activé.

[...]

(4) Les données visées aux paragraphes 2 et 3 du présent article sont conservées pour une durée d'un an à compter de la date de la communication, si elles sont générées ou traitées au cours de la fourniture du service de communication. [...]

[...]

(11) Les données visées aux paragraphes 2 et 3 du présent article sont transférées :

1) conformément au kriminaalmenetluse seadustik [(code de procédure pénale)], à l'autorité chargée de l'enquête, à l'autorité habilitée à adopter des mesures de surveillance, au ministère public, au tribunal ;

[...] »

Le code de procédure pénale

10 L'article 17 du code de procédure pénale (kriminaalmenetluse seadustik, RT I 2003, 27, 166 ; RT I, 31.05.2018, 22), dispose :

« (1) Sont parties à la procédure : le ministère public, [...].

[...] »

11 L'article 30 de ce code est libellé comme suit :

« (1) Le ministère public dirige la procédure d'instruction, tout en garantissant la légalité et l'efficacité de celle-ci, et représente l'action publique lors du procès.

(2) Les compétences du ministère public dans le cadre de la procédure pénale sont exercées en son nom par un procureur qui agit de manière indépendante et qui est uniquement soumis à la loi. »

12 L'article 90[1] dudit code prévoit :

« [...]

(2) L'autorité chargée de l'enquête peut, sur autorisation du ministère public au cours d'une procédure d'instruction ou sur autorisation du tribunal au cours d'un procès devant celui-ci, demander à une entreprise de communications électroniques qu'elle fournisse les données énumérées à l'article 111[1], paragraphes 2 et 3, de la loi relative aux communications électroniques qui ne sont pas citées au paragraphe 1 du présent article. Cette autorisation indique de manière précise les dates relatives à la période au cours de laquelle il est possible d'exiger des données.

(3) Les demandes de fourniture de données au sens du présent article ne peuvent être faites que si elles sont absolument nécessaires pour atteindre l'objectif de la procédure pénale. »

13 L'article 211 du même code dispose :

« (1) L'objectif de la procédure d'instruction est la collecte d'éléments de preuve et la création des autres conditions nécessaires à la tenue d'un procès.

(2) Au cours de la procédure d'instruction, l'autorité chargée de l'enquête et le ministère public vérifient les éléments à charge et les éléments à décharge recueillis contre le suspect ou la personne poursuivie. »

La loi relative au ministère public

14 L'article 1[er] de la prokuratuuriseadus (loi relative au ministère public, RT I 1998, 41, 625 ; RT I, 06.07.2018, 20), dans sa rédaction applicable aux faits au principal, prévoit :

« (1) Le ministère public est une autorité gouvernementale relevant du ministère de la Justice, qui participe à la planification des mesures de surveillance nécessaires en vue de combattre et de détecter les infractions pénales, il dirige la procédure d'instruction pénale, tout en garantissant la légalité et l'efficacité de celle–ci, il représente l'action publique lors du procès et il remplit les autres missions incombant au ministère public en vertu de la loi.

(1[1]) Le ministère public remplit de manière indépendante les missions qui lui incombent en vertu de la loi et il agit en se fondant sur la présente loi, sur d'autres lois et sur les actes adoptés en vertu de celles-ci.

[...] »

15 L'article 2, paragraphe 2, de cette loi dispose :

« Le procureur remplit ses missions de manière indépendante et il agit uniquement en vertu de la loi et selon sa conviction. »

Le litige au principal et les questions préjudicielles

16 Par décision du 6 avril 2017, H. K. a été condamnée par le Viru Maakohus (tribunal de première instance de Viru, Estonie) à une peine privative de liberté de deux ans pour avoir commis, entre le 17 janvier 2015 et le 1er février 2016, plusieurs vols de biens (d'une valeur allant de 3 à 40 euros) et d'espèces (pour des montants compris entre 5,20 et 2 100 euros), utilisé la carte bancaire d'un tiers, causant à celui-ci un préjudice de 3 941,82 euros, et exercé des actes de violence à l'égard de personnes participant à une procédure en justice la concernant.

17 Pour déclarer H. K. coupable de ces faits, le Viru Maakohus (tribunal de première instance de Viru) s'est fondé, entre autres, sur plusieurs procès-verbaux établis à partir de données relatives aux communications électroniques, au sens de l'article 111[1], paragraphe 2, de la loi relative aux communications électroniques, que l'autorité chargée de l'enquête avait recueillies auprès d'un fournisseur de services de télécommunications électroniques au cours de la procédure d'instruction, après avoir obtenu, en vertu de l'article 90[1] du code de procédure pénale, plusieurs autorisations à cet effet du Viru Ringkonnaprokuratuur (parquet du district de Viru, Estonie). Ces autorisations, accordées les 28 janvier et 2 février 2015, le 2 novembre 2015 ainsi que le 25 février 2016, portaient sur les données concernant plusieurs numéros de téléphone de H. K. et différentes identités internationales d'équipement mobile de celle-ci, au titre de la période du 1er janvier au 2 février 2015, du 21 septembre 2015, ainsi que de la période du 1er mars 2015 au 19 février 2016.

18 H. K. a interjeté appel de la décision du Viru Maakohus (tribunal de première instance de Viru) devant la Tartu Ringkonnakohus (cour d'appel de Tartu, Estonie), qui a rejeté cet appel par décision du 17 novembre 2017.

19 H. K. a introduit un pourvoi en cassation contre cette dernière décision auprès de la Riigikohus (Cour suprême, Estonie), en contestant, entre autres, la recevabilité des procès-verbaux établis à partir des données obtenues auprès du fournisseur de services de communications électroniques. Selon elle, il découlerait de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, ci-après « arrêt Tele2 », EU:C:2016:970), que les dispositions de l'article 111[1] de la loi relative aux communications électroniques prévoyant l'obligation des fournisseurs de services de conserver des données relatives aux communications ainsi que l'utilisation de ces données aux fins de sa condamnation sont contraires à 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.

20 Selon la juridiction de renvoi, la question se pose de savoir si les procès-verbaux établis à partir des données visées à l'article 111[1], paragraphe 2, de la loi relative aux communications électroniques peuvent être considérés comme constituant des éléments de preuve recevables. Cette juridiction fait observer que la recevabilité des procès-verbaux en cause au principal en tant qu'éléments de preuve dépend de la question de savoir dans quelle mesure la collecte des données à partir desquelles ces procès–verbaux ont été établis a été conforme à 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.

21 Ladite juridiction considère que la réponse à cette question implique de déterminer si cet article 15, paragraphe 1, lu à la lumière de la Charte, doit être interprété en ce sens que l'accès des autorités nationales à des données permettant d'identifier la source et la destination d'une communication téléphonique à partir du téléphone fixe ou mobile d'un suspect, de déterminer la date, l'heure, la durée et la nature de cette communication, d'identifier le matériel de communication utilisé ainsi que de localiser le matériel de communication mobile utilisé constitue une ingérence d'une telle gravité dans les droits fondamentaux en cause que cet accès devrait être limité à la lutte contre la criminalité grave, indépendamment de la période pour laquelle les autorités nationales ont sollicité l'accès aux données conservées.

22 La juridiction de renvoi considère toutefois que la durée de cette période est un élément essentiel pour apprécier la gravité de l'ingérence qui consiste en l'accès aux données relatives au trafic et aux données de localisation. Ainsi, lorsque ladite période est très brève ou que la quantité de données recueillies est très limitée, il conviendrait de s'interroger sur le point de savoir si l'objectif de lutte contre la criminalité en général, et pas seulement de lutte contre la criminalité grave, est susceptible de justifier une telle ingérence.

23 Enfin, la juridiction de renvoi nourrit des doutes quant à la possibilité de considérer le ministère public estonien comme une autorité administrative indépendante, au sens du point 120 de l'arrêt du 21 décembre 2016, Tele2 (C-203/15 et C-698/15, EU:C:2016:970), susceptible d'autoriser l'accès de l'autorité chargée de l'enquête à des données relatives aux communications électroniques telles que celles visées à l'article 111[1], paragraphe 2, de la loi relative aux communications électroniques.

24 Le ministère public dirigerait la procédure d'instruction, tout en garantissant la légalité et l'efficacité de celle-ci. L'objectif de cette procédure étant, notamment, la collecte de preuves, l'autorité chargée de l'enquête et le ministère public vérifieraient les éléments à charge et les éléments à décharge recueillis contre tout suspect ou personne poursuivie. Si le ministère public est convaincu que toutes les preuves nécessaires ont été recueillies, il exercerait l'action publique contre l'inculpé. Les compétences du ministère public seraient exercées en son nom par un procureur exerçant ses missions de manière indépendante, ainsi qu'il résulterait de l'article 30, paragraphes 1 et 2, du code de procédure pénale ainsi que des articles 1er et 2 de la loi relative au ministère public.

25 Dans ce contexte, la juridiction de renvoi relève que ses doutes quant à l'indépendance requise par le droit de l'Union sont principalement dus au fait que le ministère public non seulement dirige la procédure d'instruction, mais représente également l'action publique lors du procès, cette autorité étant, en vertu du droit national, partie à la procédure pénale.

26 C'est dans ces conditions que la Riigikohus (Cour suprême) a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) 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 ?

2) 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 ?

3) 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 ? »

Sur les questions préjudicielles

Sur les première et deuxième questions

27 Par ses première et deuxième questions préjudicielles, qu'il convient d'examiner conjointement, 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 qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité, de la quantité ainsi que de la nature des données disponibles pour une telle période.

28 À cet égard, il ressort de la demande de décision préjudicielle que, comme l'a confirmé le gouvernement estonien lors de l'audience, les données auxquelles l'autorité nationale chargée de l'enquête a eu accès dans l'affaire au principal sont celles retenues en vertu de l'article 111[1], paragraphes 2 et 4, de la loi relative aux communications électroniques imposant aux fournisseurs de services de communications électroniques une obligation de conserver de manière généralisée et indifférenciée les données relatives au trafic et les données de localisation en ce qui concerne la téléphonie fixe et mobile, pendant un an. Ces données permettent, notamment, de retrouver et d'identifier la source et la destination d'une communication à partir du téléphone fixe ou mobile d'une personne, de déterminer la date, l'heure, la durée et la nature de cette communication, d'identifier le matériel de communication utilisé ainsi que de localiser le téléphone mobile sans qu'une communication soit nécessairement acheminée. En outre, elles offrent la possibilité de déterminer la fréquence des communications de l'utilisateur avec certaines personnes pendant une période donnée. Par ailleurs, comme l'a confirmé le gouvernement estonien lors de l'audience, l'accès auxdites données peut, en matière de lutte contre la criminalité, être sollicité pour tout type d'infraction pénale.

29 S'agissant des conditions dans lesquelles l'accès aux données relatives au trafic et aux données de localisation conservées par les fournisseurs de services de communications électroniques peut, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, être accordé à des autorités publiques, en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58, la Cour a jugé qu'un tel accès ne peut être octroyé que pour autant que ces données aient été conservées par ces fournisseurs d'une manière conforme audit article 15, paragraphe 1 (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 167).

30 À cet égard, la Cour a également jugé que ledit article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, s'oppose à des mesures législatives prévoyant, à de telles fins, à titre préventif, la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 168).

31 Quant aux objectifs susceptibles de justifier un accès des autorités publiques aux données conservées par les fournisseurs de services de communications électroniques en application d'une mesure conforme à ces dispositions, il ressort, d'une part, de la jurisprudence de la Cour qu'un tel accès ne peut être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs de services (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 166).

32 D'autre part, la Cour a jugé que la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 131 ainsi que jurisprudence citée).

33 En ce qui concerne l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, poursuivi par la réglementation en cause au principal, conformément au principe de proportionnalité, seule la lutte contre la criminalité grave et la prévention de menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation, qu'elle soit généralisée et indifférenciée ou ciblée. Dès lors, seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif, poursuivi par la réglementation en cause au principal, de prévention, de recherche, de détection et de poursuite d'infractions pénales en général (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 140 ainsi que 146).

34 À cet égard, il a notamment été jugé que les mesures législatives visant le traitement des données relatives à l'identité civile des utilisateurs des moyens de communications électroniques en tant que telles, notamment leur conservation et l'accès à celles-ci, à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58. En effet, ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées des utilisateurs des moyens de communications électroniques, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une mesure visant ces données ne saurait, en principe, être qualifiée de grave (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 157 et 158 ainsi que jurisprudence citée).

35 Dans ces conditions, seuls les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique sont de nature à justifier l'accès des autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et permettant de tirer des conclusions précises sur la vie privée des personnes concernées (voir, en ce sens, arrêt du 2 octobre 2018,

Ministerio Fiscal, C-207/16, EU:C:2018:788, point 54), sans que d'autres facteurs tenant à la proportionnalité d'une demande d'accès, tels que la durée de la période pour laquelle l'accès est sollicité à de telles données, puissent avoir pour effet que l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général soit susceptible de justifier un tel accès.

36 Il y a lieu de relever que l'accès à un ensemble de données relatives au trafic ou de données de localisation, telles que celles conservées en vertu de l'article 111[1] de la loi relative aux communications électroniques, est effectivement susceptible de permettre de tirer des conclusions précises, voire très précises, concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 117).

37 Certes, ainsi que le suggère la juridiction de renvoi, plus la durée de la période pour laquelle l'accès est sollicité est longue, plus importante est, en principe, la quantité de données susceptibles d'être conservées par les fournisseurs de services de communications électroniques, concernant les communications électroniques passées, les lieux de séjour fréquentés ainsi que les déplacements effectués par l'utilisateur d'un moyen de communication électronique, permettant ainsi de tirer, à partir des données consultées, un plus grand nombre de conclusions sur la vie privée de cet utilisateur. Un constat analogue peut être tiré en ce qui concerne les catégories de données sollicitées.

38 C'est donc pour satisfaire à l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 130 ainsi que jurisprudence citée), qu'il appartient aux autorités nationales compétentes d'assurer, dans chaque cas d'espèce, que tant la ou les catégories de données visées que la durée pour laquelle l'accès à celles-ci est sollicité soient, en fonction des circonstances de l'espèce, limitées à ce qui est strictement nécessaire aux fins de l'enquête en cause.

39 Toutefois, l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte l'accès, par une autorité publique, à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise, présente en tout état de cause un caractère grave indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période, lorsque, comme dans l'affaire au principal, cet ensemble de données est susceptible de permettre de tirer des conclusions précises sur la vie privée de la ou des personnes concernées.

40 À cet égard, même l'accès à une quantité limitée de données relatives au trafic ou de données de localisation ou l'accès à des données pour une courte période peut être susceptible de fournir des informations précises sur la vie privée d'un utilisateur d'un moyen de communication électronique. En outre, la quantité des données disponibles et les informations concrètes sur la vie privée de la personne concernée en découlant sont des circonstances qui ne peuvent être appréciées qu'après la consultation desdites données. Or, l'autorisation d'accès accordée par la juridiction ou l'autorité indépendante compétente intervient nécessairement avant que les données et les informations en découlant puissent être consultées. Ainsi, l'appréciation de la gravité de l'ingérence que constitue l'accès s'effectue nécessairement en fonction du risque généralement afférent à la catégorie de données sollicitées pour la vie privée des personnes concernées, sans qu'il importe, par ailleurs, de savoir si les informations relatives à la vie privée en découlant présentent ou non, concrètement, un caractère sensible.

41 Enfin, compte tenu du fait que la juridiction de renvoi est saisie d'une demande concluant à l'irrecevabilité des procès-verbaux établis à partir des données relatives au trafic et des données de localisation, au motif que les dispositions de l'article 111[1] de la loi relative aux communications électroniques seraient contraires à l'article 15, paragraphe 1, de la directive 2002/58 tant en ce qui concerne la conservation des données que l'accès à celles-ci, il y a lieu de rappeler que, en l'état actuel du droit de l'Union, il appartient, en principe, au seul droit national de déterminer les règles relatives à l'admissibilité et à l'appréciation, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, d'informations et d'éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée de ces données, contraire au droit de l'Union (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 222), ou encore par un accès des autorités nationales auxdites données, contraire à ce droit.

42 En effet, il est de jurisprudence constante que, en l'absence de règles de l'Union en la matière, il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe d'autonomie procédurale, de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas moins favorables que celles régissant des situations similaires soumises au droit interne (principe d'équivalence) et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union (principe d'effectivité) (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 223 ainsi que jurisprudence citée).

43 Pour ce qui est plus particulièrement du principe d'effectivité, il convient de rappeler que les règles nationales relatives à l'admissibilité et à l'exploitation des informations et des éléments de preuve ont pour objectif, en vertu des choix opérés par le droit national, d'éviter que des informations et des éléments de preuve qui ont été obtenus de manière illégale portent indûment préjudice à une personne soupçonnée d'avoir commis des infractions pénales. Or, cet objectif peut, selon le droit national, être atteint non seulement par une interdiction d'exploiter de telles informations et de tels éléments de preuve, mais également par des règles et des pratiques nationales régissant l'appréciation et la pondération des informations et des éléments de preuve, voire par une prise en considération de leur caractère illégal dans le cadre de la détermination de la peine (arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 225).

44 La nécessité d'exclure des informations et des éléments de preuve obtenus en méconnaissance des prescriptions du droit de l'Union doit être appréciée au regard, notamment, du risque que l'admissibilité de tels informations et éléments de preuve comporte pour le respect du principe du contradictoire et, partant, du droit à un procès équitable. Or, une juridiction qui considère qu'une partie n'est pas en mesure de commenter efficacement un moyen de preuve qui ressortit à un domaine échappant à la connaissance des juges et qui est susceptible d'influencer de manière prépondérante l'appréciation des faits doit constater une violation du droit à un procès équitable et exclure ce moyen de preuve afin d'éviter une telle violation. Partant, le principe d'effectivité impose au juge pénal national 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 connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, points 226 et 227).

45 Eu égard aux considérations qui précèdent, il convient de répondre aux première et deuxième questions que 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 qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période.

Sur la troisième question

46 Par sa troisième question préjudicielle, 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 qu'il s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale.

47 La juridiction de renvoi précise à cet égard que, si le ministère public estonien est, conformément au droit national, tenu d'agir de manière indépendante, est uniquement soumis à la loi et doit examiner les éléments à charge et à décharge lors de la procédure d'instruction, l'objectif de cette procédure n'en reste pas moins la collecte d'éléments de preuve ainsi que la réunion des autres conditions nécessaires à la tenue d'un procès. Ce serait cette même autorité qui représente l'action publique lors du procès et elle serait donc également partie à la procédure. En outre, il ressort du dossier dont dispose la Cour, comme l'ont également confirmé le gouvernement estonien et le Prokuratuur lors de l'audience, que le ministère public estonien est organisé de manière hiérarchique et que les demandes d'accès aux données relatives au trafic et aux données de localisation ne sont pas soumises à une exigence de forme particulière et peuvent être introduites par le procureur lui-même. Enfin, les personnes aux données desquelles l'accès peut être accordé ne seraient pas seulement celles soupçonnées d'être impliquées dans une infraction pénale.

48 Il est vrai, ainsi que la Cour l'a déjà jugé, qu'il appartient au droit national de déterminer les conditions dans lesquelles les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données dont ils disposent. Toutefois, pour satisfaire à l'exigence de proportionnalité, une telle réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire (voir, en ce sens, arrêts du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 117 et 118 ; du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790, point 68, ainsi que du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 132 et jurisprudence citée).

49 En particulier, une réglementation nationale régissant l'accès des autorités compétentes à des données relatives au trafic et à des données de localisation conservées, adoptée au titre de l'article 15, paragraphe 1, de la directive 2002/58, ne saurait se limiter à exiger que l'accès des autorités aux

données réponde à la finalité poursuivie par cette réglementation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation (arrêts du 6 octobre 2020, Privacy International, C-623/17, EU:C:2020:790, point 77, ainsi que du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 176 et jurisprudence citée).

50 Ainsi, et dès lors qu'un accès général à toutes les données conservées, indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne peut être considéré comme étant limité au strict nécessaire, la réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données en cause. À cet égard, un tel accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction. Toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités (voir, en ce sens, arrêts du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 119, ainsi que du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 188).

51 Aux fins de garantir, en pratique, le plein respect de ces conditions, il est essentiel que l'accès des autorités nationales compétentes aux données conservées soit 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. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais (voir, en ce sens, arrêt du 6 octobre 2020, La Quadrature du Net e.a., C-511/18, C-512/18 et C-520/18, EU:C:2020:791, point 189 ainsi que jurisprudence citée).

52 Ce contrôle préalable requiert entre autres, ainsi que l'a relevé, en substance, M. l'avocat général au point 105 de ses conclusions, que la juridiction ou l'entité chargée d'effectuer ledit contrôle préalable dispose de toutes les attributions et présente 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 des personnes dont les données sont concernées par l'accès.

53 Lorsque ce contrôle est effectué non par une juridiction mais par une entité administrative indépendante, celle-ci doit jouir d'un statut lui permettant d'agir lors de l'exercice de ses missions de manière objective et impartiale et doit être, à cet effet, à l'abri de toute influence extérieure [voir, en ce sens, arrêt du 9 mars 2010, Commission/Allemagne, C-518/07, EU:C:2010:125, point 25, ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 229 et 230].

54 Il résulte des considérations qui précèdent que l'exigence d'indépendance à laquelle doit satisfaire l'autorité chargée d'exercer le contrôle préalable, rappelé au point 51 du présent arrêt, impose que cette autorité ait la qualité de tiers par rapport à celle qui demande l'accès aux données, de sorte que la première soit en mesure d'exercer ce contrôle de manière objective et impartiale à l'abri de toute influence extérieure. En particulier, dans le domaine pénal, l'exigence d'indépendance implique, ainsi que l'a relevé M. l'avocat général en substance au point 126 de ses conclusions, que l'autorité chargée de ce contrôle préalable, d'une part, ne soit pas impliquée dans la conduite de l'enquête pénale en cause et, d'autre part, ait une position de neutralité vis-à-vis des parties à la procédure pénale.

55 Tel n'est pas le cas d'un ministère public qui dirige la procédure d'enquête et exerce, le cas échéant, l'action publique. En effet, le ministère public a pour mission non pas de trancher en toute indépendance un litige, mais de le soumettre, le cas échéant, à la juridiction compétente, en tant que partie au procès exerçant l'action pénale.

56 La circonstance que le ministère public soit, conformément aux règles régissant ses compétences et son statut, tenu de vérifier les éléments à charge et à décharge, de garantir la légalité de la procédure d'instruction et d'agir uniquement en vertu de la loi et de sa conviction ne saurait suffire à lui conférer le statut de tiers par rapport aux intérêts en cause au sens décrit au point 52 du présent arrêt.

57 Il s'ensuit que le ministère public n'est pas en mesure d'effectuer le contrôle préalable visé au point 51 du présent arrêt.

58 La juridiction de renvoi ayant soulevé, par ailleurs, la question de savoir s'il peut être suppléé à l'absence de contrôle effectué par une autorité indépendante par un contrôle ultérieur exercé par une juridiction de la légalité de l'accès d'une autorité nationale aux données relatives au trafic et aux données de localisation, il importe de relever que le contrôle indépendant doit intervenir, ainsi que l'exige la jurisprudence rappelée au point 51 du présent arrêt, préalablement à tout accès, sauf cas d'urgence dûment justifiée, auquel cas le contrôle doit intervenir dans de brefs délais. Ainsi que l'a relevé M. l'avocat général au point 128 de ses conclusions, un tel contrôle ultérieur ne permettrait pas de répondre à l'objectif d'un contrôle préalable, consistant à empêcher que soit autorisé un accès aux données en cause qui dépasse les limites du strict nécessaire.

59 Dans ces conditions, il convient de répondre à la troisième question préjudicielle que 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 qu'il s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale.

Sur les dépens

60 La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant la juridiction de renvoi, il appartient à celle-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (grande chambre) dit pour droit :

1) **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), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale permettant l'accès d'autorités publiques à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de fournir des informations sur les communications effectuées par un utilisateur d'un moyen de communication électronique ou sur la localisation des équipements terminaux qu'il utilise et de permettre de tirer des conclusions précises sur sa vie privée, à des fins de prévention, de recherche, de détection et de**

poursuite d'infractions pénales, sans que cet accès soit circonscrit à des procédures visant à la lutte contre la criminalité grave ou à la prévention de menaces graves contre la sécurité publique, ce indépendamment de la durée de la période pour laquelle l'accès auxdites données est sollicité et de la quantité ou de la nature des données disponibles pour une telle période.

2) **L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale donnant compétence au ministère public, dont la mission est de diriger la procédure d'instruction pénale et d'exercer, le cas échéant, l'action publique lors d'une procédure ultérieure, pour autoriser l'accès d'une autorité publique aux données relatives au trafic et aux données de localisation aux fins d'une instruction pénale.**

Signatures