Recueil de la jurisprudence

ARRÊT DE LA COUR (grande chambre)

30 avril 2024*

« Renvoi préjudiciel – Traitement des données à caractère personnel dans le secteur des communications électroniques – Confidentialité des communications – Fournisseurs de services de communications électroniques – Directive 2002/58/CE – 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 – Accès à ces données demandé par une autorité nationale compétente à des fins de poursuites d'infractions de vols avec circonstances aggravantes – Définition de la notion d'"infraction grave" dont la poursuite est susceptible de justifier une ingérence grave dans les droits fondamentaux – Compétence des États membres – Principe de proportionnalité – Étendue du contrôle préalable du juge sur les demandes d'accès aux données conservées par les fournisseurs de services de communications électroniques »

Dans l'affaire C-178/22,

ayant pour objet une demande de décision préjudicielle au titre de l'article 267 TFUE, introduite par le Giudice delle indagini preliminari presso il Tribunale di Bolzano (juge des enquêtes préliminaires du tribunal de Bolzano, Italie), par décision du 20 février 2022, parvenue à la Cour le 8 mars 2022, dans les procédures pénales contre

Inconnus,

en présence de :

Procura della Repubblica presso il Tribunale di Bolzano,

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M. L. Bay Larsen, vice-président, M. A. Arabadjiev, M^mes^ A. Prechal, K. Jürimäe, MM. T. von Danwitz et Z. Csehi, présidents de chambre, MM. J.-C. Bonichot, S. Rodin, P. G. Xuereb (rapporteur), D. Gratsias, M^me^ M. L. Arastey Sahún et M. M. Gavalec, juges,

avocat général : M. A. M. Collins,

greffier : M. C. Di Bella, administrateur,

vu la procédure écrite et à la suite de l'audience du 21 mars 2023,

* Langue de procédure : l'italien.

considérant les observations présentées :

– pour la Procura della Repubblica presso il Tribunale di Bolzano, par Mme F. Iovene, sostituto procuratore della Repubblica,

– pour le gouvernement italien, par Mme G. Palmieri, en qualité d'agent, assistée de M. S. Faraci, avvocato dello Stato,

– pour le gouvernement tchèque, par Mme A. Edelmannová, MM. O. Serdula, M. Smolek, Mme T. Suchá et M. J. Vláčil, en qualité d'agents,

– pour le gouvernement estonien, par Mme M. Kriisa, en qualité d'agent,

– pour l'Irlande, par Mme M. Browne, Chief State Solicitor, MM. A. Joyce et M. Tierney, en qualité d'agents, assistés de M. D. Fennelly, BL,

– pour le gouvernement français, par Mmes A. Daniel, A.-L. Desjonquères, MM. B. Fodda et J. Illouz, en qualité d'agents,

– pour le gouvernement chypriote, par Mme E. Neophytou, en qualité d'agent,

– pour le gouvernement hongrois, par Mme Zs. Biró-Tóth et M. M. Z. Fehér, en qualité d'agents,

– pour le gouvernement néerlandais, par Mmes M. K. Bulterman, A. Hanje et M. J. Langer, en qualité d'agents,

– pour le gouvernement autrichien, par M. A. Posch, Mmes J. Schmoll, C. Gabauer, M. K. Ibili et Mme E. Samoilova, en qualité d'agents,

– pour le gouvernement polonais, par M. B. Majczyna, Mmes D. Lutostańska et J. Sawicka, en qualité d'agents,

– pour la Commission européenne, par MM. S. L. Kalėda, H. Kranenborg, L. Malferrari et F. Wilman, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 8 juin 2023,

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 saisine du Giudice delle indagini preliminari presso il Tribunale di Bolzano (juge des enquêtes préliminaires du tribunal de Bolzano, Italie) par la Procura della Repubblica presso il Tribunale di Bolzano (parquet près le tribunal de Bolzano, Italie) (ci-après le « ministère public »), afin qu'il l'autorise à accéder à des données à caractère personnel conservées par des fournisseurs de services de communications électroniques pour identifier les auteurs de deux vols de téléphone mobile avec circonstances aggravantes.

Le cadre juridique

Le droit de l'Union

La directive 2002/58

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 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 [, 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 Aux termes de l'article 2 de cette directive, 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 L’article 5 de ladite directive, intitulé « Confidentialité des communications », prévoit :

« 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 même directive, 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 cette 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 communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, [TUE]. »

Le droit italien

Le décret législatif n° 196/2003

9 L'article 132, paragraphe 3, du decreto legislativo n. 196 – Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE [décret législatif n° 196, portant code en matière de protection des données à caractère personnel, portant dispositions d'adaptation du droit national au 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], du 30 juin 2003 (supplément ordinaire à la GURI n° 174, du 29 juillet 2003), dans sa rédaction applicable au litige au principal (ci-après le « décret législatif n° 196/2003 »), prévoit ce qui suit :

« Dans le délai de conservation imposé par la loi, s'il existe des indices suffisants d'infractions pour lesquelles la loi prévoit la peine de réclusion à perpétuité ou de réclusion pour une durée maximale d'au moins trois ans, déterminée conformément à l'article 4 du [codice di procedura penale (code de procédure pénale)], et d'infractions de menace et de harcèlement ou nuisance contre les personnes par téléphone, lorsque la menace, le harcèlement et la nuisance sont graves, si elles sont pertinentes pour constater les faits, les données sont recueillies sur autorisation préalable délivrée par le juge par un décret motivé, sur réquisition du ministère public ou à la demande de la défense du prévenu, de la personne faisant l'objet de l'enquête, de la victime et des autres parties privées. »

10 Le paragraphe 3 bis de cet article dispose :

« En cas d'urgence et s'il est justifié de penser que le retard pourrait porter un préjudice grave à l'enquête, le ministère public ordonne l'obtention des données par un décret motivé qui est communiqué immédiatement et en tout cas dans les 48 heures au juge compétent pour délivrer l'autorisation selon la procédure ordinaire. Dans les 48 heures suivantes, le juge se prononce sur la validation par décret motivé. »

11 Enfin, aux termes du paragraphe 3 quater, dudit article, « [l]es données recueillies en violation des dispositions figurant aux paragraphes 3 et 3 bis ne peuvent pas être utilisées ».

Le code pénal

12 L'article 624 du codice penale (code pénal), intitulé « Vol », dispose :

« Quiconque s'approprie le bien meuble d'autrui, en le soustrayant à son détenteur, dans le but d'en tirer profit pour lui-même ou pour autrui, est puni d'une peine d'emprisonnement de six mois à trois ans et d'une amende allant de 154 à 516 euros.

[...]

L'infraction est punissable sur plainte de la personne lésée, sauf si l'une ou plusieurs des conditions visées à l'article 61, paragraphe 7, et à l'article 625 sont réunies. »

13 L'article 625, premier alinéa, du code pénal, intitulé « Circonstances aggravantes », prévoit :

« Le fait visé à l'article 624 est puni d'une peine d'emprisonnement de deux à six ans et d'une amende allant de 927 à 1 500 euros :

[...]

2) si le coupable fait usage de violence à l'égard des biens ou se sert d'un quelconque moyen frauduleux ;

3) si le coupable porte sur lui des armes ou des stupéfiants, sans en faire usage ;

4) s'il est question d'un vol à la tire ;

5) si le fait est commis par trois personnes ou plus, voire par une seule, déguisée en ou qui se fait passer pour un officier public ou une personne exerçant une fonction publique ;

6) si le fait concerne les bagages de voyageurs dans n'importe quel véhicule, dans les gares, les aéroports ou sur les quais, dans les hôtels ou dans tout établissement commercialisant des aliments ou des boissons ;

7) si le fait concerne des biens présents dans des bureaux ou des établissements publics, ou confisqués ou saisis, ou exposés par nécessité ou par coutume ou par destination à la foi publique, ou destinés au service public ou à l'utilité publique, à la défense ou à la vénération ;

7 bis) si le fait concerne des composants métalliques ou d'autres matériaux retirés d'infrastructures destinées à la fourniture d'énergie, de services de transport, de télécommunications ou d'autres services publics et exploitées par des entités publiques ou privées dans le cadre d'une concession publique ;

8) si le fait concerne trois têtes de bétail ou plus réunies en troupeau, ou des bovins ou des équidés, même non réunis en troupeau ;

8 bis) si le fait est commis dans des moyens de transport public ;

8 ter) si le fait est commis à l'égard d'une personne en train d'utiliser ou qui vient d'utiliser les services d'un établissement de crédit, d'un bureau de poste ou d'un distributeur automatique de billets. »

Le code de procédure pénale

14 Aux termes de l'article 4 du code de procédure pénale, intitulé « Règles de détermination de la compétence » :

« La compétence est déterminée en fonction de la peine prévue par la loi pour chaque infraction perpétrée ou tentée. Il n'est pas tenu compte de la continuation, de la récidive ni des circonstances de l'infraction, à l'exception des circonstances aggravantes pour lesquelles la loi prévoit une peine d'une autre espèce que celle qui est prévue ordinairement pour l'infraction et des circonstances à effet spécial. »

15 L'article 269, paragraphe 2, de ce code prévoit :

« [...] les enregistrements sont conservés jusqu'à ce qu'un jugement définitif soit rendu. Toutefois, afin de protéger la confidentialité, les intéressés peuvent, lorsque les documents ne sont pas nécessaires aux fins de la procédure, solliciter auprès du juge qui a autorisé ou validé l'interception la destruction des enregistrements. »

Le litige au principal et la question préjudicielle

16 À la suite de deux plaintes déposées pour des faits de vols de téléphone mobile commis, respectivement, les 27 octobre et 20 novembre 2021, le ministère public a engagé, en application des articles 624 et 625 du code pénal, deux procédures pénales contre des auteurs inconnus pour des infractions de vol avec circonstances aggravantes.

17 Afin d'identifier les auteurs de ces vols, le ministère public a, sur le fondement de l'article 132, paragraphe 3, du décret législatif n° 196/2003, demandé, respectivement les 7 décembre et 30 décembre 2021, au Giudice delle indagini preliminari presso il Tribunale di Bolzano (juge des enquêtes préliminaires du tribunal de Bolzano), la juridiction de renvoi, l'autorisation de recueillir auprès de toutes les compagnies téléphoniques les relevés téléphoniques des téléphones volés. Ces demandes visaient « toutes les données [en la possession des compagnies téléphoniques], suivant une méthode de traçage et de localisation (plus particulièrement les abonnés et le cas échéant les codes [relatifs à l'identité internationale d'équipement mobile (IMEI) des appareils] appelés ou appelants, les sites visités et atteints, le moment et la durée de l'appel ou de la connexion et l'indication des parties de réseaux ou répétiteurs concernés, les abonnés et les codes IMEI [des appareils] expéditeurs et destinataires des SMS ou MMS et, si possible, les données d'identité des titulaires respectifs) des conversations et communications téléphoniques et des connexions effectuées, y compris en itinérance, entrantes ou sortantes même si les appels ne sont pas facturés (simple sonnerie sans réponse) depuis la date du vol jusqu'à la date de rédaction de la demande ».

18 La juridiction de renvoi a des doutes quant à la compatibilité de l'article 132, paragraphe 3, du décret législatif n° 196/2003 avec l'article 15, paragraphe 1, de la directive 2002/58, tel qu'interprété par la Cour dans son arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152).

19 Elle rappelle que, en vertu du point 45 de cet arrêt, des dispositions nationales permettant l'accès d'autorités publiques à des relevés téléphoniques, comportant un ensemble de données relatives au trafic ou de données de localisation susceptibles de permettre de tirer des conclusions précises sur la vie privée de l'utilisateur concerné, ne sont justifiables, compte tenu du principe de

proportionnalité prévu à l'article 52, paragraphe 1, de la Charte et de la gravité de l'ingérence dans les droits fondamentaux à la vie privée, à la protection des données à caractère personnel et à la liberté d'expression et d'information, tels que garantis, respectivement, aux articles 7, 8 et 11 de la Charte, que si elles sont destinées à poursuivre des infractions graves, telles que les menaces graves contre la sécurité publique, entendue comme celle de l'État, et d'autres formes de criminalité grave.

20 À cet égard, la juridiction de renvoi indique que, dans son arrêt nº 33116 du 7 septembre 2021, la Corte suprema di cassazione (Cour de cassation, Italie) a considéré que, eu égard à la marge d'interprétation entourant la détermination des infractions constituant des menaces graves contre la sécurité publique ou d'autres formes de criminalité grave au sens de la jurisprudence de la Cour, cette jurisprudence ne présentait pas les caractéristiques requises pour être appliquée directement par les juridictions nationales. En conséquence, le législateur italien aurait modifié l'article 132, paragraphe 3, du décret législatif nº 196/2003 afin de qualifier d'infractions graves, pour lesquelles les relevés téléphoniques peuvent être obtenus, les infractions que la loi punit d'une peine de réclusion maximale « d'au moins trois ans ».

21 Selon la juridiction de renvoi, ce seuil de trois ans à partir duquel la peine de réclusion maximale dont est punie une infraction justifie que cette infraction puisse donner lieu à la communication de relevés téléphoniques aux autorités publiques est tel que ces relevés pourraient être communiqués à celles-ci pour poursuivre des infractions qui ne causent qu'un trouble social limité et qui ne sont punies que sur plainte d'un particulier, notamment les vols de faible valeur comme les vols de téléphone mobile ou de bicyclette.

22 La disposition nationale en cause méconnaîtrait ainsi le principe de proportionnalité prévu à l'article 52, paragraphe 1, de la Charte, qui exige que la gravité de l'infraction poursuivie soit mise en balance avec les droits fondamentaux auxquels il est porté atteinte pour la poursuivre. Ce principe s'opposerait en effet à ce qu'une atteinte aux droits fondamentaux garantis par les articles 7, 8 et 11 de la Charte soit justifiée par la poursuite d'une infraction telle que le vol.

23 La juridiction de renvoi précise que les juridictions italiennes disposent d'une marge d'appréciation très restreinte pour refuser l'autorisation d'obtenir des relevés téléphoniques puisque, en vertu de la disposition en cause, l'autorisation doit être accordée s'il existe des « indices suffisants d'infractions » et si les données sollicitées sont « pertinentes pour constater les faits ». Les juridictions italiennes ne disposeraient donc d'aucune marge d'appréciation quant à la gravité concrète de l'infraction faisant l'objet de l'enquête. Cette appréciation aurait été effectuée à titre définitif par le législateur italien lorsqu'il a prévu que l'autorisation d'obtenir les données devait être accordée, notamment, pour toutes les infractions punies d'une peine de réclusion maximale d'au moins trois ans.

24 Dans ces conditions, le Giudice delle indagini preliminari presso il Tribunale di Bolzano (juge des enquêtes préliminaires du tribunal de Bolzano) a décidé de surseoir à statuer et de poser à la Cour la question préjudicielle suivante :

« L'article 15, paragraphe 1, de la directive [2002/58] s'oppose-t-il à la législation nationale figurant à l'article 132[, paragraphe 3,] du décret législatif [n° 196/2003], [...] qui [...] dispose ce qui suit :

"3. Dans le délai de conservation imposé par la loi, s'il existe des indices suffisants d'infractions pour lesquelles la loi prévoit la peine de réclusion à perpétuité ou de réclusion pour une durée maximale d'au moins trois ans, déterminée conformément à l'article 4 du code de procédure pénale, et d'infractions de menace et de harcèlement ou nuisance contre les personnes par téléphone, lorsque la menace, le harcèlement et la nuisance sont graves, si elles sont pertinentes pour constater les faits, les données sont recueillies sur autorisation préalable délivrée par le juge par un décret motivé, sur réquisition du ministère public ou à la demande de la défense du prévenu, de la personne faisant l'objet de l'enquête, de la victime et des autres parties privées" ? »

Sur la recevabilité de la demande de décision préjudicielle

25 Le gouvernement italien et l'Irlande estiment que la demande de décision préjudicielle est partiellement irrecevable. Ils relèvent que les demandes d'accès aux données conservées par les fournisseurs de services de communications électroniques ont été présentées par le ministère public, sur le fondement de l'article 132, paragraphe 3, du décret législatif n° 196/2003, afin de poursuivre des infractions de vols avec circonstances aggravantes de téléphone mobile. Or, par sa question préjudicielle, la juridiction de renvoi demanderait également à la Cour si l'article 15, paragraphe 1, de la directive 2002/58 s'oppose à une disposition nationale qui permet d'obtenir l'accès à des données conservées par les fournisseurs de services de communications électroniques afin de poursuivre d'autres infractions relevant de l'article 132, paragraphe 3, du décret législatif n° 196/2003 que celles en cause au principal, telles que le vol simple ou le harcèlement grave par téléphone. Partant, la demande de décision préjudicielle présenterait un caractère hypothétique en ce qu'elle viserait ces autres infractions.

26 À cet égard, il convient de rappeler que, selon une jurisprudence constante, dans le cadre de la coopération entre la Cour et les juridictions nationales instituée à l'article 267 TFUE, il appartient au seul juge national qui est saisi du litige et qui doit assumer la responsabilité de la décision juridictionnelle à intervenir d'apprécier, au regard des particularités de l'affaire, tant la nécessité d'une décision préjudicielle pour être en mesure de rendre son jugement que la pertinence des questions qu'il pose à la Cour. En conséquence, lorsque les questions posées portent sur l'interprétation du droit de l'Union, la Cour est, en principe, tenue de statuer [arrêt du 21 mars 2023, Mercedes-Benz Group (Responsabilité des constructeurs de véhicules munis de dispositifs d'invalidation), C-100/21, EU:C:2023:229, point 52 et jurisprudence citée].

27 Il s'ensuit que les questions portant sur le droit de l'Union bénéficient d'une présomption de pertinence. Le refus de la Cour de statuer sur une question préjudicielle posée par une juridiction nationale n'est possible que s'il apparaît de manière manifeste que l'interprétation sollicitée du droit de l'Union n'a aucun rapport avec la réalité ou l'objet du litige au principal, lorsque le problème est de nature hypothétique ou encore lorsque la Cour ne dispose pas des éléments de

fait et de droit nécessaires pour répondre de façon utile aux questions qui lui sont posées [arrêt du 21 mars 2023, Mercedes-Benz Group (Responsabilité des constructeurs de véhicules munis de dispositifs d'invalidation), C-100/21, EU:C:2023:229, point 53 et jurisprudence citée].

28 Or, en reproduisant intégralement l'article 132, paragraphe 3, du décret législatif nº 196/2003, la question préjudicielle, même si elle ne distingue pas les types d'infractions auxquelles cette disposition s'applique, couvre nécessairement les infractions de vols avec circonstances aggravantes pour lesquelles les demandes d'autorisation d'accès aux données à caractère personnel ont été présentées dans l'affaire au principal.

29 Partant, cette question ne présente pas un caractère hypothétique et est donc recevable.

Sur la question préjudicielle

30 Ainsi que l'a relevé le gouvernement français dans ses observations écrites, la question posée par la juridiction de renvoi, telle qu'elle est formulée, invite la Cour à se prononcer sur la compatibilité de l'article 132, paragraphe 3, du décret législatif nº 196/2003 avec l'article 15, paragraphe 1, de la directive 2002/58.

31 À cet égard, il convient de rappeler que, dans le cadre de la procédure instituée à l'article 267 TFUE, la Cour n'est compétente pour se prononcer ni sur l'interprétation de dispositions législatives ou réglementaires nationales ni sur la conformité de telles dispositions au droit de l'Union. En effet, il ressort d'une jurisprudence constante que, dans le cadre d'un renvoi préjudiciel au titre de l'article 267 TFUE, la Cour peut uniquement interpréter le droit de l'Union dans les limites des compétences attribuées à l'Union [arrêt du 14 décembre 2023, Getin Noble Bank (Délai de prescription des actions en restitution), C-28/22, EU:C:2023:992, point 53 et jurisprudence citée].

32 Cela étant, il ressort d'une jurisprudence constante que, en présence de questions formulées de manière impropre ou dépassant le cadre des fonctions qui sont dévolues à la Cour par l'article 267 TFUE, il appartient à celle-ci d'extraire de l'ensemble des éléments fournis par la juridiction nationale, et notamment de la motivation de la décision de renvoi, les éléments du droit de l'Union qui appellent une interprétation compte tenu de l'objet du litige. Dans cette optique, il incombe, le cas échéant, à la Cour de reformuler les questions qui lui sont soumises (arrêt du 14 décembre 2023, Sparkasse Südpfalz, C-206/22, EU:C:2023:984, point 20 et jurisprudence citée).

33 En outre, la Cour peut être amenée à prendre en considération des normes du droit de l'Union auxquelles le juge national n'a pas fait référence dans l'énoncé de sa question (arrêt du 17 novembre 2022, Harman International Industries, C-175/21, EU:C:2022:895, point 31 et jurisprudence citée).

34 Eu égard à ce qui précède, il y a lieu de considérer que, par sa question, 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 disposition nationale qui impose au juge national, intervenant dans le cadre d'un contrôle préalable effectué à la suite d'une demande motivée d'accès à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de permettre de tirer des conclusions précises sur la vie privée d'un utilisateur d'un moyen de communication

électronique, conservées par les fournisseurs de services de communications électroniques, présentée par une autorité nationale compétente dans le cadre d'une enquête pénale, d'autoriser cet accès si celui-ci est demandé aux fins de la recherche d'infractions pénales punies, par le droit national, d'une peine de réclusion maximale d'au moins trois ans, sous réserve qu'il existe des indices suffisants de telles infractions et que ces données soient pertinentes pour constater les faits.

35 À titre liminaire, il convient de rappeler que, 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 législative 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 conformément à cette directive [voir, en ce sens, arrêt de ce jour, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, point 65 ainsi que jurisprudence citée]. Elle a également jugé que cet 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 [arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 30 et jurisprudence citée].

36 Il convient également de rappeler la jurisprudence de la Cour selon laquelle 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'ingérence grave dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, découlant de 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, 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 à de telles données est sollicité, 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 [voir, en ce sens, arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 35 et jurisprudence citée].

37 Par sa question préjudicielle, la juridiction de renvoi cherche, en substance, à savoir si une telle ingérence grave peut être autorisée pour des infractions telles que celles visées par la réglementation nationale en cause au principal.

38 S'agissant, tout d'abord, de la question de savoir si les accès tels que ceux en cause peuvent être qualifiés d'ingérence grave dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte, il y a lieu de relever que, afin d'identifier les auteurs des vols présumés qui sont à l'origine de ce litige, le ministère public, pour chacun des téléphones mobiles concernés, a demandé à la juridiction de renvoi, sur le fondement de l'article 132, paragraphe 3, du décret législatif n° 196/2003, l'autorisation de recueillir toutes les données en la possession des compagnies téléphoniques, obtenues au moyen d'une méthode de traçage et de localisation des conversations et communications téléphoniques et des connexions effectuées avec ces téléphones. Ces demandes concernaient, plus particulièrement, les abonnés et les codes IMEI des appareils

appelés ou appelants, les sites visités et atteints, le moment et la durée des appels et des connexions, l'indication des parties de réseaux ou répétiteurs concernés ainsi que les abonnés et les codes IMEI des appareils expéditeurs et destinataires des SMS ou MMS.

39 L'accès à un tel ensemble de données relatives au trafic ou de données de localisation paraît susceptible de permettre de tirer des conclusions 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 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, point 36 et jurisprudence citée]. L'ingérence dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte causée par l'accès à de telles données paraît donc susceptible d'être qualifiée de grave.

40 Ainsi qu'il ressort du point 39 de l'arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques) (C-746/18, EU:C:2021:152), cette appréciation ne saurait être écartée du seul fait que les deux demandes d'accès aux données relatives au trafic ou aux données de localisation en cause ne concernaient que de courtes périodes, de moins de deux mois, allant des dates des vols présumés des téléphones mobiles aux dates auxquelles ces demandes ont été rédigées, dès lors que lesdites demandes portaient sur un ensemble de ces données susceptible de fournir des informations précises sur la vie privée des personnes utilisant les téléphones mobiles concernés.

41 De même, est dépourvue de pertinence, aux fins d'apprécier l'existence d'une ingérence grave dans les droits garantis aux articles 7 et 8 de la Charte, la circonstance que les données auxquelles le ministère public a demandé l'accès ne seraient pas celles des propriétaires des téléphones mobiles en cause mais celles des personnes ayant communiqué les unes avec les autres en utilisant ces téléphones après leurs vols présumés. En effet, il ressort de l'article 5, paragraphe 1, de la directive 2002/58 que l'obligation de principe de garantir la confidentialité des communications électroniques 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, vise les communications effectuées par les utilisateurs de ce réseau. Or, l'article 2, sous a), de cette directive définit la notion d'« utilisateur » comme 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.

42 Par conséquent, eu égard à la jurisprudence citée au point 36 du présent arrêt, dès lors que les ingérences dans les droits fondamentaux causées par l'accès aux données, telles que celles en cause dans l'affaire au principal, sont susceptibles d'être considérées comme étant graves, elles ne peuvent être justifiées que par les objectifs de lutte contre la criminalité grave ou de prévention de menaces graves pour la sécurité publique.

43 Ensuite, s'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, une telle réglementation doit prévoir des règles claires et précises régissant la portée et les conditions d'application d'un tel accès. Celui-ci ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées d'être impliquées dans une infraction grave. Aux fins de garantir, en pratique, le plein respect de ces conditions garantissant que l'ingérence soit limitée au strict nécessaire, il est essentiel que l'accès des autorités nationales

compétentes aux données conservées soit subordonné, sauf en cas d'urgence dûment justifiée, à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante [voir, en ce sens, arrêt du 2 mars 2021, Prokuratuur (Conditions d'accès aux données relatives aux communications électroniques), C-746/18, EU:C:2021:152, points 48 à 51].

44 En ce qui concerne, enfin, la définition de la notion d'« infraction grave », il ressort de la jurisprudence que, pour autant que l'Union n'ait pas légiféré en la matière, la législation pénale et les règles de la procédure pénale relèvent de la compétence des États membres. Ceux-ci doivent toutefois exercer cette compétence dans le respect du droit de l'Union (voir, en ce sens, arrêt du 26 février 2019, Rimšēvičs et BCE/Lettonie, C-202/18 et C-238/18, EU:C:2019:139, point 57 ainsi que jurisprudence citée).

45 À cet égard, il faut observer que la définition des infractions pénales, des circonstances atténuantes et aggravantes et des sanctions reflète tant les réalités sociales que les traditions juridiques qui varient non seulement entre les États membres, mais aussi dans le temps. Or, ces réalités et traditions revêtent une importance certaine pour déterminer les infractions considérées comme présentant un caractère grave.

46 Partant, compte tenu de la répartition des compétences entre l'Union et les États membres en vertu du traité FUE et des différences importantes qui existent entre les systèmes juridiques des États membres dans le domaine pénal, il y a lieu de considérer qu'il incombe aux États membres de définir les « infractions graves » aux fins de l'application de l'article 15, paragraphe 1, de la directive 2002/58.

47 Toutefois, la définition des « infractions graves », opérée par les États membres, doit respecter les exigences qui découlent de cet 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.

48 Il convient de rappeler, à cet égard, que, en ce qu'il permet aux États membres d'adopter des mesures législatives visant à « limiter la portée » des droits et des obligations prévus notamment aux articles 5, 6 et 9 de la directive 2002/58, tels que ceux découlant des principes de confidentialité des communications et de l'interdiction du stockage des données y afférentes, l'article 15, paragraphe 1, de cette directive énonce une exception à la règle générale prévue notamment à ces articles 5, 6 et 9 et doit ainsi, conformément à une jurisprudence constante, faire l'objet d'une interprétation stricte. Une telle disposition ne saurait donc justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes devienne la règle, sauf à vider largement l'article 5 de ladite directive de sa portée (voir, ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 40).

49 En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les mesures prises par les États membres au titre de cette disposition doivent respecter les principes généraux de l'Union, parmi lesquels figure le principe de proportionnalité, et assurer le respect des droits fondamentaux garantis par les articles 7, 8 et 11 de la Charte (voir, en ce sens, arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 42).

50 Il s'ensuit que les États membres ne sauraient dénaturer la notion d'« infraction grave » et, par extension, celle de « criminalité grave », en y incluant, aux fins de l'application de cet article 15, paragraphe 1, des infractions qui ne sont manifestement pas graves, au regard des conditions sociétales prévalant dans l'État membre concerné, alors même que le législateur de cet État membre a prévu de les punir d'une peine maximale de réclusion de trois ans.

51 C'est notamment en vue de vérifier l'absence d'une telle dénaturation qu'il est essentiel que, lorsque l'accès des autorités nationales compétentes aux données conservées comporte le risque d'une ingérence grave dans les droits fondamentaux de la personne concernée, cet accès soit subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante [voir, en ce sens, arrêt de ce jour, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, points 124 à 131].

52 En l'occurrence, il ressort de la décision de renvoi que l'article 132, paragraphe 3, du décret législatif n° 196/2003 fixe les conditions dans lesquelles l'accès à des données conservées par les fournisseurs de services de communications électroniques peut être octroyé par un juge saisi d'une demande motivée d'une autorité publique. Cette disposition définit les infractions, pour la poursuite desquelles l'accès à des données conservées par les fournisseurs de services de communications électroniques peut être octroyé, par référence à une peine de réclusion maximale d'au moins trois ans. Elle subordonne cet accès à la double condition qu'il existe des « indices suffisants d'infraction » et que ces données soient « pertinentes pour constater les faits ».

53 La juridiction de renvoi se demande cependant si la définition, résultant de cette disposition, des « infractions graves », pour la poursuite desquelles l'accès aux données peut être octroyé, n'est pas trop large dès lors qu'elle couvre des infractions qui ne causent qu'un trouble social limité.

54 À cet égard, il y a lieu de relever, premièrement, qu'une définition, selon laquelle les « infractions graves », pour la poursuite desquelles l'accès peut être octroyé, sont celles pour lesquelles la peine de réclusion maximale est au moins égale à une durée que la loi détermine, est fondée sur un critère objectif. Cela est conforme à l'exigence selon laquelle la législation 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 (arrêt du 5 avril 2022, Commissioner of An Garda Síochána e.a., C-140/20, EU:C:2022:258, point 105 ainsi que jurisprudence citée).

55 Deuxièmement, il découle de la jurisprudence citée au point 48 du présent arrêt que la définition donnée, en droit national, des « infractions graves » pouvant permettre un accès aux données conservées par les fournisseurs de services de communications électroniques, permettant de tirer des conclusions précises sur la vie privée des personnes concernées, ne doit pas être à ce point large que l'accès à ces données devienne la règle plutôt que l'exception. Ainsi, elle ne saurait couvrir la grande majorité des infractions pénales, ce qui serait le cas si le seuil au-delà duquel la peine de réclusion maximale dont est punie une infraction justifie que celle-ci soit qualifiée d'infraction grave était fixé à un niveau excessivement bas.

56 Or, un seuil fixé par référence à une peine maximale de réclusion de trois ans n'apparaît pas, à cet égard, comme étant excessivement bas (voir, en ce sens, arrêt du 21 juin 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, point 150).

57 Certes, dès lors que la définition des « infractions graves », pour lesquelles l'accès aux données conservées par les fournisseurs de services de communications électroniques peut être demandé, est établie par référence non pas à une peine minimale applicable mais à une peine maximale applicable, il n'est pas exclu qu'un accès à des données, constitutif d'une ingérence grave dans les droits fondamentaux, puisse être demandé à des fins de poursuites d'infractions ne relevant pas, en réalité, de la criminalité grave (voir, par analogie, arrêt du 21 juin 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, point 151).

58 La fixation d'un seuil à partir duquel la peine de réclusion maximale dont est punie une infraction justifie que celle-ci soit qualifiée d'infraction grave n'est toutefois pas nécessairement contraire au principe de proportionnalité.

59 D'une part, tel paraît être le cas d'une disposition telle que celle en cause au principal puisqu'elle vise, ainsi que cela ressort de la décision de renvoi, de manière générale, l'accès aux données conservées par les fournisseurs de services de communications électroniques, sans préciser la nature de ces données. Ainsi, cette disposition paraît couvrir notamment des cas dans lesquels l'accès ne peut être qualifié d'ingérence grave, car ne visant pas un ensemble de données susceptible de permettre de tirer des conclusions précises sur la vie privée des personnes concernées.

60 D'autre part, la juridiction ou l'entité administrative indépendante, intervenant dans le cadre d'un contrôle préalable effectué à la suite d'une demande d'accès motivée, doit être habilitée à refuser ou à restreindre cet accès lorsqu'elle constate que l'ingérence dans les droits fondamentaux que constituerait un tel accès est grave alors qu'il est manifeste que l'infraction en cause ne relève pas effectivement de la criminalité grave (voir, par analogie, arrêt du 21 juin 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, point 152).

61 En effet, la juridiction ou l'entité chargée du contrôle doit être en mesure d'assurer un juste équilibre entre, d'une part, les intérêts légitimes 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 [arrêt de ce jour, La Quadrature du Net e.a. (Données personnelles et lutte contre la contrefaçon), C-470/21, point 125 ainsi que jurisprudence citée].

62 En particulier, dans le cadre de son examen de la proportionnalité de l'ingérence causée dans les droits fondamentaux de la personne concernée par la demande d'accès, cette juridiction ou cette entité doit être en mesure d'exclure un tel accès lorsque ce dernier est sollicité dans le cadre de poursuites pour une infraction qui n'est manifestement pas grave, au sens du point 50 du présent arrêt.

63 Il résulte de ce qui précède qu'il convient de répondre à la 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 ne s'oppose pas à une disposition nationale qui impose au juge national, intervenant dans le cadre d'un contrôle préalable effectué à la suite d'une demande motivée d'accès à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de permettre de tirer des conclusions précises sur la vie privée d'un utilisateur d'un moyen de communication électronique, conservées par les fournisseurs de services de communications électroniques, présentée par une autorité nationale compétente dans le cadre d'une enquête pénale, d'autoriser cet accès si celui-ci est demandé aux fins de la recherche d'infractions pénales punies, par le droit national, d'une peine

de réclusion maximale d'au moins trois ans, sous réserve qu'il existe des indices suffisants de telles infractions et que ces données soient pertinentes pour constater les faits, à condition, toutefois, que ce juge soit habilité à refuser ledit accès si ce dernier est sollicité dans le cadre d'une enquête portant sur une infraction qui n'est manifestement pas grave, au regard des conditions sociétales prévalant dans l'État membre concerné.

Sur les dépens

64 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 :

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 que :

il ne s'oppose pas à une disposition nationale qui impose au juge national, intervenant dans le cadre d'un contrôle préalable effectué à la suite d'une demande motivée d'accès à un ensemble de données relatives au trafic ou de données de localisation, susceptibles de permettre de tirer des conclusions précises sur la vie privée d'un utilisateur d'un moyen de communication électronique, conservées par les fournisseurs de services de communications électroniques, présentée par une autorité nationale compétente dans le cadre d'une enquête pénale, d'autoriser cet accès si celui-ci est demandé aux fins de la recherche d'infractions pénales punies, par le droit national, d'une peine de réclusion maximale d'au moins trois ans, sous réserve qu'il existe des indices suffisants de telles infractions et que ces données soient pertinentes pour constater les faits, à condition, toutefois, que ce juge soit habilité à refuser ledit accès si ce dernier est sollicité dans le cadre d'une enquête portant sur une infraction qui n'est manifestement pas grave, au regard des conditions sociétales prévalant dans l'État membre concerné.

Signatures