СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA

EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL

CVRIA
LUXEMBOURG

ARRÊT DE LA COUR (grande chambre)

21 décembre 2016 *

« Renvoi préjudiciel – Communications électroniques – Traitement des données à caractère personnel – Confidentialité des communications électroniques – Protection – Directive 2002/58/CE – Articles 5, 6 et 9 ainsi que article 15, paragraphe 1 – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et 11 ainsi que article 52, paragraphe 1 – Législation nationale – Fournisseurs de services de communications électroniques – Obligation portant sur la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation – Autorités nationales – Accès aux données – Absence de contrôle préalable par une juridiction ou une autorité administrative indépendante – Compatibilité avec le droit de l'Union »

Dans les affaires jointes C-203/15 et C-698/15,

ayant pour objet des demandes de décision préjudicielle au titre de l'article 267 TFUE, introduites par le Kammarrätten i Stockholm (cour d'appel administrative de Stockholm, Suède) et la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile), Royaume-Uni], par décisions, respectivement, du 29 avril 2015 et du 9 décembre 2015, parvenues à la Cour le 4 mai 2015 et le 28 décembre 2015, dans les procédures

Tele2 Sverige AB (C-203/15)

contre

Post- och telestyrelsen,

et

Secretary of State for the Home Department (C-698/15)

contre

Tom Watson,

* Langues de procédure : le suédois et l'anglais.

Peter Brice,

Geoffrey Lewis,

en présence de :

Open Rights Group,

Privacy International,

The Law Society of England and Wales,

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M. A. Tizzano, vice-président, M^me^ R. Silva de Lapuerta, MM. T. von Danwitz (rapporteur), J. L. da Cruz Vilaça, E. Juhász et M. Vilaras, présidents de chambre, MM. A. Borg Barthet, J. Malenovský, E. Levits, J.-C. Bonichot, A. Arabadjiev, S. Rodin, F. Biltgen et C. Lycourgos, juges,

avocat général : M. H. Saugmandsgaard Øe,

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

vu la décision du président de la Cour du 1^er^ février 2016 de soumettre l'affaire C-698/15 à la procédure accélérée prévue à l'article 105, paragraphe 1, du règlement de procédure de la Cour,

vu la procédure écrite et à la suite de l'audience du 12 avril 2016,

considérant les observations présentées :

– pour Tele2 Sverige AB, par M^es^ M. Johansson et N. Torgerzon, advokater, ainsi que par MM. E. Lagerlöf et S. Backman,

– pour M. Watson, par M. J. Welch et M^me^ E. Norton, solicitors, M^e^ I. Steele, advocate, M. B. Jaffey, barrister, ainsi que par M^me^ D. Rose, QC,

– pour MM. Brice et Lewis, par MM. A. Suterwalla et R. de Mello, barristers, R. Drabble, QC, ainsi que par S. Luke, solicitor,

– pour Open Rights Group et Privacy International, par M. D. Carey, solicitor, ainsi que par M. R. Mehta et M^me^ J. Simor, barristers,

– pour The Law Society of England and Wales, par M. T. Hickman, barrister, ainsi que par M^me^ N. Turner,

– pour le gouvernement suédois, par M^mes^ A. Falk, C. Meyer-Seitz, U. Persson et N. Otte Widgren ainsi que par M. L. Swedenborg, en qualité d'agents,

– pour le gouvernement du Royaume-Uni, par MM. S. Brandon et L. Christie ainsi que par M^me^ V. Kaye, en qualité d'agents, assistés de MM. D. Beard, G. Facenna et J. Eadie, QC, ainsi que de M^me^ S. Ford, barrister,

– pour le gouvernement belge, par MM. J.-C. Halleux et S. Vanrie ainsi que par M^me^ C. Pochet, en qualité d'agents,

– pour le gouvernement tchèque, par MM. M. Smolek et J. Vláčil, en qualité d'agents,

– pour le gouvernement danois, par M. C. Thorning et M^me^ M. Wolff, en qualité d'agents,

– pour le gouvernement allemand, par MM. T. Henze et M. Hellmann ainsi que par M^me^ J. Kemper, en qualité d'agents, assistés de M^es^ M. Kottmann et U. Karpenstein, Rechtsanwälte,

– pour le gouvernement estonien, par M^me^ K. Kraavi-Käerdi, en qualité d'agent,

– pour l'Irlande, par M^mes^ E. Creedon et L. Williams ainsi que par M. A. Joyce, en qualité d'agents, assistés de M. D. Fennelly, BL,

– pour le gouvernement espagnol, par M. A. Rubio González, en qualité d'agent,

– pour le gouvernement français, par MM. G. de Bergues, D. Colas et F.-X. Bréchot ainsi que par M^me^ C. David, en qualité d'agents,

– pour le gouvernement chypriote, par M^me^ K. Kleanthous, en qualité d'agent,

– pour le gouvernement hongrois, par MM. M. Fehér et G. Koós, en qualité d'agents,

– pour le gouvernement néerlandais, par M^mes^ M. Bulterman et M. Gijzen ainsi que par M. J. Langer, en qualité d'agents,

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

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

– pour la Commission européenne, par MM. H. Krämer, K. Simonsson, H. Kranenborg et D. Nardi ainsi que par M^mes^ P. Costa de Oliveira et J. Vondung, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 19 juillet 2016,

rend le présent

Arrêt

1 Les demandes de décision préjudicielle portent 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 et 8 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

2 Ces demandes ont été présentées dans le cadre de deux litiges opposant, pour le premier, Tele2 Sverige AB à la Post- och telestyrelsen (autorité suédoise de surveillance des postes et télécommunications, ci-après la « PTS »), au sujet d'une injonction faite par cette dernière à Tele2 Sverige de procéder à la conservation des données relatives au trafic et des données de localisation de ses abonnés et utilisateurs inscrits (affaire C-203/15), pour le second, MM. Tom Watson, Peter Brice et Geoffrey Lewis au Secretary of State for the Home Department (ministre de l'Intérieur, Royaume-Uni de Grande-Bretagne et d'Irlande du Nord), au sujet de la conformité au droit de l'Union de l'article 1er du Data Retention and Investigatory Powers Act 2014 (loi de 2014 sur la conservation des données et les pouvoirs d'enquête, ci-après la « DRIPA ») (affaire C-698/15).

Le cadre juridique

Le droit de l'Union

La directive 2002/58

3 Les considérants 2, 6, 7, 11, 21, 22, 26 et 30 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].

[...]

(6) L'Internet bouleverse les structures commerciales traditionnelles en offrant une infrastructure mondiale commune pour la fourniture de toute une série

de services de communications électroniques. Les services de communications électroniques accessibles au public sur l'Internet ouvrent de nouvelles possibilités aux utilisateurs, mais présentent aussi de nouveaux dangers pour leurs données à caractère personnel et leur vie privée.

(7) Dans le cas des réseaux publics de communications, il convient d'adopter des dispositions législatives, réglementaires et techniques spécifiques afin de protéger les droits et les libertés fondamentaux des personnes physiques et les intérêts légitimes des personnes morales, notamment eu égard à la capacité accrue de stockage et de traitement automatisés de données relatives aux abonnés et aux utilisateurs.

[...]

(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, 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.

[...]

(21) Il convient de prendre des mesures pour empêcher tout accès non autorisé aux communications afin de protéger la confidentialité des communications effectuées au moyen de réseaux publics de communications et de services de communications électroniques accessibles au public, y compris de leur contenu et de toute donnée afférente à ces communications. La législation

nationale de certains États membres interdit uniquement l'accès non autorisé intentionnel aux communications.

(22) L'interdiction du stockage des communications et des données relatives au trafic y afférentes par des personnes autres que les utilisateurs ou sans le consentement de ceux-ci ne vise pas à interdire tout stockage automatique, intermédiaire et transitoire de ces informations si ce stockage a lieu dans le seul but d'effectuer la transmission dans le réseau de communications électroniques, pour autant que les informations ne soient pas stockées pour une durée plus longue que le temps nécessaire à la transmission et à la gestion du trafic et qu'au cours de la période de stockage la confidentialité des informations reste garantie. [...]

[...]

(26) Les données relatives aux abonnés qui sont traitées dans des réseaux de communications électroniques pour établir des connexions et transmettre des informations contiennent des informations sur la vie privée des personnes physiques et touchent au droit au secret de leur correspondance ainsi qu'aux intérêts légitimes des personnes morales. Ces données ne peuvent être stockées que dans la mesure où cela est nécessaire à la fourniture du service, aux fins de la facturation et des paiements pour interconnexion, et ce, pour une durée limitée. Tout autre traitement de ces données [...] ne peut être autorisé que si l'abonné a donné son accord sur la base d'informations précises et complètes fournies par le fournisseur du service de communications électroniques accessible au public sur la nature des autres traitements qu'il envisage d'effectuer, ainsi que sur le droit de l'abonné de ne pas donner son consentement à ces traitements ou de retirer son consentement. [...]

[...]

(30) Les systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires. [...] »

4 L'article 1er de la directive 2002/58, intitulé « Champ d'application et objectif », dispose :

« 1. La présente directive prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et services de communications électroniques dans la Communauté.

2. Les dispositions de la présente directive précisent et complètent la directive [95/46] aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, 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) ou aux activités de l'État dans des domaines relevant du droit pénal. »

5 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 :

[...]

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 ;

[...] »

6 L'article 3 de la directive 2002/58, intitulé « Services concernés », prévoit :

« La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques

accessibles au public sur les réseaux de communications publics dans la Communauté, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification. »

7 L'article 4 de cette directive, intitulé « Sécurité du traitement », est ainsi libellé :

« 1. Le fournisseur d'un service de communications électroniques accessible au public prend les mesures d'ordre technique et organisationnel appropriées afin de garantir la sécurité de ses services, le cas échéant conjointement avec le fournisseur du réseau public de communications en ce qui concerne la sécurité du réseau. Compte tenu des possibilités techniques les plus récentes et du coût de leur mise en œuvre, ces mesures garantissent un degré de sécurité adapté au risque existant.

1 bis. Sans préjudice des dispositions de la directive [95/46], les mesures visées au paragraphe 1, pour le moins :

– garantissent que seules des personnes autorisées peuvent avoir accès aux données à caractère personnel à des fins légalement autorisées,

– protègent les données à caractère personnel stockées ou transmises contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelles et le stockage, le traitement, l'accès et la divulgation non autorisés ou illicites, et

– assurent la mise en œuvre d'une politique de sécurité relative au traitement des données à caractère personnel.

[...] »

8 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. »

9 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. »

10 L'article 9 de cette directive, 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. [...] »

11 L'article 15 de ladite directive, intitulé « Application de certaines dispositions de la directive [95/46] », énonce :

« 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, du traité sur l'Union européenne.

[...]

1 ter. Les fournisseurs établissent, sur la base des dispositions nationales adoptées au titre du paragraphe 1, des procédures internes permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs. Ils mettent, sur demande, à la disposition de l'autorité nationale compétente des informations sur ces procédures, sur le nombre de demandes reçues, sur la base juridique invoquée et sur leur réponse.

2. Les dispositions du chapitre III de la directive [95/46] relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux

dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

[...] »

La directive 95/46

12 L'article 22 de la directive 95/46, figurant au chapitre III de celle-ci, est libellé comme suit :

« Sans préjudice du recours administratif qui peut être organisé, notamment devant l'autorité de contrôle visée à l'article 28, antérieurement à la saisine de l'autorité judiciaire, les États membres prévoient que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question. »

La directive 2006/24/CE

13 L'article 1er de la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54), intitulé « Objet et champ d'application », prévoyait, à son paragraphe 2 :

« La présente directive s'applique aux données relatives au trafic et aux données de localisation concernant tant les entités juridiques que les personnes physiques, ainsi qu'aux données connexes nécessaires pour identifier l'abonné ou l'utilisateur enregistré. Elle ne s'applique pas au contenu des communications électroniques, notamment aux informations consultées en utilisant un réseau de communications électroniques. »

14 Aux termes de l'article 3 de cette directive, intitulé « Obligation de conservation de données » :

« 1. Par dérogation aux articles 5, 6 et 9 de la directive [2002/58], les États membres prennent les mesures nécessaires pour que les données visées à l'article 5 de la présente directive soient conservées, conformément aux dispositions de cette dernière, dans la mesure où elles sont générées ou traitées dans le cadre de la fourniture des services de communication concernés par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans leur ressort.

2. L'obligation de conserver les données visées au paragraphe 1 inclut la conservation des données visées à l'article 5 relatives aux appels téléphoniques infructueux, lorsque ces données sont générées ou traitées, et stockées (en ce qui concerne les données de la téléphonie) ou journalisées (en ce qui concerne les

données de l'internet), dans le cadre de la fourniture des services de communication concernés, par des fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications, lorsque ces fournisseurs sont dans le ressort de l'État membre concerné. La présente directive n'impose pas la conservation des données relatives aux appels non connectés. »

Le droit suédois

15 Il ressort de la décision de renvoi dans l'affaire C-203/15 que le législateur suédois a, aux fins de transposer la directive 2006/24 en droit national, modifié la lagen (2003:389) om elektronisk kommunikation [loi (2003:389) sur les communications électroniques, ci-après la « LEK »)] et le förordningen (2003:396) om elektronisk kommunikation [règlement (2003:396) sur les communications électroniques]. L'un et l'autre de ces textes, dans leur version applicable au litige au principal, contiennent des règles portant sur la conservation des données relatives aux communications électroniques ainsi que sur l'accès à ces données par les autorités nationales.

16 L'accès auxdites données est, en outre, réglementé par la lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet [loi (2012:278) sur la communication de données relatives aux communications électroniques dans le cadre des activités de renseignement des autorités répressives, ci-après la « loi 2012:278 »] ainsi que par le rättegångsbalken (code de procédure judiciaire, ci-après le « RB »).

Sur l'obligation de conservation des données relatives aux communications électroniques

17 Selon les indications de la juridiction de renvoi dans l'affaire C-203/15, les dispositions de l'article 16 a du chapitre 6 de la LEK, lues en combinaison avec l'article 1er du chapitre 2 de cette loi, prévoient une obligation pour les fournisseurs de services de communications électroniques de conserver les données dont la conservation était prévue par la directive 2006/24. Il s'agit des données relatives aux abonnements et à toutes communications électroniques nécessaires pour retrouver et identifier la source et la destination d'une communication, pour en déterminer la date, l'heure, la durée et la nature, pour identifier le matériel de communication utilisé ainsi que pour localiser le matériel de communication mobile utilisé au début et à l'achèvement de la communication. L'obligation de conservation des données porte sur les données générées ou traitées dans le cadre d'un service de téléphonie, d'un service de téléphonie par un point de connexion mobile, d'un système de messagerie électronique, d'un service d'accès à Internet ainsi que d'un service de fourniture de capacités d'accès à Internet (mode de connexion). Cette obligation inclut également les données relatives aux communications infructueuses. Elle ne porte cependant pas sur le contenu des communications.

18 Les articles 38 à 43 du règlement (2003:396) sur les communications électroniques précisent les catégories de données qui doivent être conservées. S'agissant des services de téléphonie, doivent notamment être conservées les données relatives aux appels et aux numéros appelés ainsi que les dates et heures traçables de début et d'achèvement de la communication. S'agissant des services de téléphonie par un point de connexion mobile, des obligations supplémentaires sont imposées telles que, par exemple, la conservation des données de localisation du début et de l'achèvement de la communication. S'agissant des services de téléphonie utilisant un paquet IP, doivent notamment être conservées, outre les données mentionnées ci-dessus, celles relatives aux adresses IP de l'appelant et de l'appelé. S'agissant des systèmes de messagerie électronique, doivent, notamment, être conservées les données relatives aux numéros des émetteurs et des destinataires, les adresses IP ou toute autre adresse de messagerie. En ce qui concerne les services d'accès à Internet, doivent, par exemple, être conservées les données relatives aux adresses IP des utilisateurs ainsi que les dates et heures traçables de connexion et de déconnexion au service d'accès à Internet.

Sur la durée de conservation des données

19 Conformément à l'article 16 d du chapitre 6 de la LEK, les données visées à l'article 16 a de ce chapitre doivent être conservées par les fournisseurs de services de communications électroniques pendant six mois à compter du jour de l'achèvement de la communication. Elles doivent ensuite être immédiatement effacées, sauf dispositions contraires prévues à l'article 16 d, deuxième alinéa, dudit chapitre.

Sur l'accès aux données conservées

20 L'accès aux données conservées par les autorités nationales est régi par les dispositions de la loi 2012:278, de la LEK et du RB.

– La loi 2012:278

21 Dans le cadre des activités de renseignements, la police nationale, la Säkerhetspolisen (police de sécurité, Suède) et la Tullverket (administration des douanes, Suède) peuvent, sur le fondement de l'article 1er de la loi 2012:278, dans les conditions prescrites par cette loi et à l'insu du fournisseur d'un réseau électronique de communications ou d'un service de communications électroniques autorisé en application de la LEK, procéder à la collecte de données concernant les messages transmis dans un réseau de communications électroniques, les équipements de communication électronique présents dans une zone géographique déterminée ainsi que la ou les zones géographiques où se situe ou était situé un équipement de communication électronique.

22 Conformément aux articles 2 et 3 de la loi 2012:278, les données peuvent, en principe, être collectées si, en fonction des circonstances, la mesure est particulièrement nécessaire pour prévenir, empêcher ou constater une activité

criminelle impliquant soit une ou plusieurs infractions sanctionnées par une peine d'emprisonnement de deux ans au moins, soit l'un des actes énumérés à l'article 3 de cette loi incluant des infractions sanctionnées par une peine d'emprisonnement inférieure à deux ans. Les motifs appelant cette mesure doivent l'emporter sur les considérations relatives à l'atteinte ou au préjudice qu'elle implique pour celui qui en fait l'objet ou pour un intérêt qui s'y oppose. Conformément à l'article 5 de ladite loi, la durée de la mesure ne doit pas excéder un mois.

23 La décision de procéder à une telle mesure relève du directeur de l'autorité concernée ou d'une personne déléguée à cet effet. Elle n'est pas soumise au contrôle préalable d'une autorité judiciaire ou d'une autorité administrative indépendante.

24 En vertu de l'article 6 de la loi 2012:278, la Säkerhets och integritetsskyddsnämnden (commission de la sécurité et de la protection de l'intégrité, Suède) doit être informée de toute décision autorisant la collecte de données. Conformément à l'article 1er de la lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet [loi (2007:980) relative au contrôle de certaines activités répressives], cette autorité exerce une surveillance sur l'application de la loi par les autorités répressives.

– La LEK

25 En vertu de l'article 22, premier alinéa, point 2, du chapitre 6 de la LEK, tout fournisseur de services de communications électroniques doit communiquer les données relatives à un abonnement sur réquisition du Parquet, de la police nationale, de la police de sécurité ou de toute autre autorité publique répressive, si ces données se rapportent à une infraction présumée. Selon les indications de la juridiction de renvoi dans l'affaire C-203/15, il n'est pas nécessaire qu'il s'agisse d'une infraction grave.

– Le RB

26 Le RB régit la communication des données conservées aux autorités nationales dans le cadre d'enquêtes préliminaires. Conformément à l'article 19 du chapitre 27 du RB, la « mise sous surveillance de communications électroniques » à l'insu de tiers est, en principe, autorisée dans le cadre d'enquêtes préliminaires visant, notamment, des infractions sanctionnées par une peine d'emprisonnement d'au moins six mois. Par « mise sous surveillance de communications électroniques », il convient, conformément à l'article 19 du chapitre 27 du RB, d'entendre l'obtention de données à l'insu de tiers concernant un message transmis par un réseau de communications électroniques, les équipements de communication électronique présents ou ayant été présents dans une zone géographique déterminée ainsi que la ou les zones géographiques où un équipement de communication électronique déterminé est ou a été présent.

27 Selon les indications de la juridiction de renvoi dans l'affaire C-203/15, des renseignements sur le contenu d'un message ne peuvent être obtenus sur la base de l'article 19 du chapitre 27 du RB. En principe, la mise sous surveillance de communications électroniques ne peut être ordonnée, en vertu de l'article 20 du chapitre 27 du RB, qu'en présence d'indices plausibles permettant de soupçonner qu'une personne est l'auteur d'une infraction et que la mesure est particulièrement nécessaire pour les besoins de l'enquête, cette dernière devant en outre viser une infraction sanctionnée par une peine d'emprisonnement de deux ans au moins ou la tentative, la préparation ou l'entente délictueuse en vue de commettre une telle infraction. Conformément à l'article 21 du chapitre 27 du RB, le Parquet doit, sauf en cas d'urgence, demander au juge compétent l'autorisation de procéder à la mise sous surveillance de communications électroniques.

Sur la sécurité et la protection des données conservées

28 En vertu de l'article 3 a du chapitre 6 de la LEK, les fournisseurs de services de communications électroniques tenus par une obligation de conservation des données doivent prendre les mesures d'ordre technique et organisationnel appropriées pour assurer la protection des données lors de leur traitement. Selon les indications de la juridiction de renvoi dans l'affaire C-203/15, le droit suédois ne prévoit, toutefois, pas de dispositions relatives au lieu de conservation des données.

Le droit du Royaume-Uni

La DRIPA

29 L'article 1er de la DRIPA, intitulé « Pouvoirs en matière de conservation des données relatives à des communications pertinentes, moyennant des garanties », dispose :

« (1) Le [ministre de l'Intérieur] peut, aux termes d'un acte (l'"acte ordonnant la conservation") exiger d'un opérateur de télécommunications publiques de conserver des données pertinentes relatives à des communications s'il estime que cette exigence est nécessaire et proportionnée à un ou plusieurs des objectifs visés aux points (a) à (h) de la section 22, paragraphe 2, du Regulation of Investigatory Powers Act 2000 [loi de 2000 portant réglementation des pouvoirs d'enquête] (objectifs pour lesquels les données relatives à des communications peuvent être obtenues).

(2) Un acte ordonnant la conservation peut :

(a) se rapporter à un opérateur en particulier ou à toute catégorie d'opérateurs ;

(b) imposer la conservation de toutes les données ou toute catégorie de données ;

(c) préciser la période ou les périodes pendant lesquelles les données doivent être conservées ;

(d) comporter d'autres exigences ou restrictions en relation avec la conservation des données ;

(e) prévoir des dispositions différentes à des fins différentes ;

(f) concerner des données, qu'elles existent ou non à la date à laquelle l'acte ordonnant la conservation est adopté ou entre en vigueur.

(3) Le [ministre de l'Intérieur] peut, par voie de règlements, adopter davantage de dispositions relatives à la conservation des données pertinentes relatives à des communications.

(4) Ces dispositions peuvent porter, en particulier, sur :

(a) les exigences préalables à l'adoption de l'acte ordonnant la conservation ;

(b) la période maximale pendant laquelle les données doivent être conservées en application d'un acte ordonnant la conservation ;

(c) le contenu, l'adoption, l'entrée en vigueur, le réexamen, la modification ou la révocation d'un acte ordonnant la conservation ;

(d) l'intégrité, la sécurité ou la protection des données conservées en application du présent article, l'accès à ces données ainsi que leur divulgation ou leur destruction ;

(e) la mise en œuvre des exigences ou restrictions pertinentes ou la vérification de la conformité à ces exigences ou restrictions ;

(f) un code des bonnes pratiques relatives aux exigences, restrictions ou pouvoirs pertinents ;

(g) le remboursement par le [ministre de l'Intérieur] (sous certaines conditions ou non) des frais encourus par les opérateurs de télécommunications publiques pour se conformer aux exigences ou aux restrictions pertinentes ;

(h) le fait que le [Data Retention (EC Directive) Regulations 2009 (règlement de 2009 concernant la conservation des données au sens de la directive CE)] cesse d'être en vigueur et la transition vers la conservation des données en application du présent article.

(5) La période maximale prévue en application du paragraphe 4, sous b), ne doit pas excéder 12 mois à compter de la date précisée en relation avec les données concernées par les règlements visés au paragraphe 3.

[...] »

30 L'article 2 de la DRIPA définit l'expression « données pertinentes relatives à des communications » comme visant les « données pertinentes relatives à des communications du type de celles mentionnées dans l'annexe au règlement de 2009 concernant la conservation des données au sens de la directive CE, pour autant que ces données soient générées ou traitées au Royaume-Uni par des opérateurs de télécommunications publiques, dans le cadre de la fourniture des services de télécommunications concernés ».

La RIPA

31 L'article 21 de la loi de 2000 portant réglementation des pouvoirs d'enquête (ci-après la « RIPA »), figurant au chapitre II de cette loi et intitulé « Obtention et divulgation des données relatives à des communications », précise, à son paragraphe 4 :

« Dans le présent chapitre, on entend par "données relatives à des communications" l'une quelconque des notions suivantes :

(a) toute donnée relative au trafic comprise dans, ou annexée à, une communication (par l'expéditeur ou autrement) aux fins de tout service postal ou de système de télécommunication par le biais duquel elle est transmise ou peut être transmise ;

(b) toute information qui n'inclut aucun contenu d'une communication (excepté toute information relevant du point a) et qui porte sur l'utilisation effectuée par toute personne :

(i) de tout service postal ou de télécommunications ; ou

(ii) en relation avec la fourniture ou l'utilisation par toute personne de tout service de télécommunications, de toute partie d'un système de télécommunication ;

(c) toute information ne relevant pas des points a ou b, qui est détenue ou obtenue, en relation avec des personnes destinataires du service, par une personne fournissant un service postal ou un service de télécommunications ».

32 Selon les indications contenues dans la décision de renvoi dans l'affaire C-698/15, ces données incluent les « données de localisation d'un utilisateur », mais pas celles relatives au contenu d'une communication.

33 Quant à l'accès aux données conservées, l'article 22 de la RIPA dispose :

« (1) Cet article s'applique dès lors qu'une personne responsable aux fins de ce chapitre estime qu'il est nécessaire pour les raisons relevant du paragraphe 2 du présent article d'obtenir toute donnée de communication.

(2) Il est nécessaire pour des raisons relevant du présent paragraphe d'obtenir les données relatives à des communications si elles sont nécessaires :

(a) dans l'intérêt de la sûreté nationale ;

(b) à des fins de prévention ou de détection de la criminalité ou de prévention des troubles à l'ordre public ;

(c) dans l'intérêt du bien-être économique du Royaume-Uni ;

(d) dans l'intérêt de la sécurité publique ;

(e) à des fins de protection de la santé publique ;

(f) à des fins d'évaluation de l'assiette ou de collecte de toute taxe, droit, redevance ou autre imposition, contribution ou charge due à l'administration publique ;

(g) à des fins de prévention, en cas d'urgence, de décès, de blessures ou de tout préjudice pour la santé physique ou mentale d'une personne physique ou d'atténuation de toute blessure ou préjudice pour la santé physique ou mentale d'une personne physique ;

(h) à toute autre fin (ne relevant pas des points a à g) précisée dans une injonction établie par le [ministre de l'Intérieur].

(4) Sous réserve du paragraphe 5, la personne responsable peut, lorsqu'il lui semble qu'un opérateur de télécommunications ou un opérateur postal est en possession de données, pourrait l'être ou pourrait être capable de l'être, exiger par requête à l'opérateur de télécommunication ou à l'opérateur postal que cet opérateur

(a) obtienne les données, s'il ne les détient pas déjà, et

(b) divulgue, en toute hypothèse, toutes les données en sa possession ou qu'il a obtenues par la suite.

(5) La personne responsable ne doit pas donner d'autorisation conformément au paragraphe 3 ou faire une requête en vertu du paragraphe 4, sauf si elle considère que l'obtention des données en question résultant d'un comportement autorisé ou exigé en vertu d'une autorisation ou d'une requête est proportionnée avec le but recherché par l'obtention des données. »

34 Conformément à l'article 65 de la RIPA, des plaintes peuvent être déposées auprès de l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni) s'il existe une raison de penser que des données ont été obtenues de manière inappropriée.

Le Data Retention Regulations 2014

35 Le Data Retention Regulations 2014 (règlement de 2014 sur la conservation de données), adopté sur le fondement de la DRIPA, est divisé en trois parties, la deuxième d'entre elles comprenant les articles 2 à 14 de ce règlement. L'article 4, intitulé « Requêtes en matière de conservation », prévoit :

« (1) les requêtes en matière de conservation doivent préciser :

(a) l'opérateur public de télécommunications (ou la description des opérateurs) à qui elles s'adressent,

(b) les données relatives à des communications pertinentes qui doivent être conservées,

(c) la période ou les périodes pendant lesquelles les données doivent être conservées,

(d) toute autre exigence ou restriction en lien avec la conservation des données.

(2) Une requête en matière de conservation ne peut pas exiger qu'une donnée soit conservée pendant plus de 12 mois à partir :

(a) dans le cas des données de trafic ou des données relatives à l'utilisation du service, du jour de la communication concernée et

(b) dans le cas des données relatives aux abonnés, du jour où la personne concernée met un terme au service de communication en cause ou du jour où la donnée est modifiée (si celui-ci est antérieur).

[...] »

36 Selon l'article 7 de ce règlement, intitulé « Intégrité et sécurité des données » :

« (1) Un opérateur public de télécommunications qui conserve des données en application de l'article 1er de la [DRIPA] doit :

(a) s'assurer que les données sont de la même intégrité et soumises au moins au même niveau de sécurité et de protection que les données des systèmes dont elles proviennent,

(b) s'assurer, par des mesures techniques et organisationnelles appropriées, que seul le personnel spécialement autorisé peut avoir accès aux données, et

(c) protéger, par des mesures techniques et organisationnelles appropriées, les données contre la destruction illicite, les pertes ou les dégâts d'origine accidentelle, ou contre la conservation, le traitement, l'accès ou la divulgation illicites ou non autorisés.

(2) Un opérateur public de télécommunications qui conserve des données relatives à des communications en vertu de l'article 1er de la [DRIPA] doit détruire les données si la conservation des données cesse d'être autorisée par cet article et n'est pas autrement autorisée par la loi.

(3) L'exigence visée au paragraphe 2 de détruire les données est une exigence consistant à effacer les données de manière à rendre l'accès à ces données impossible.

(4) Il est suffisant pour l'opérateur de prendre des dispositions afin que l'effacement des données intervienne de manière mensuelle ou à des intervalles plus courts selon les possibilités de l'opérateur en pratique. »

37 L'article 8 dudit règlement, intitulé « Divulgation des données conservées », dispose :

« (1) Un opérateur public de télécommunications doit mettre en place des systèmes de sécurité adéquats (comprenant des mesures techniques et organisationnelles) déterminant l'accès aux données relatives à des communications conservées en vertu de l'article 1er de la [DRIPA] afin de prévenir toute divulgation ne relevant pas de l'article 1er, paragraphe 6, sous a, de la [DRIPA].

(2) Un opérateur public de télécommunications qui conserve des données en vertu de l'article 1er de la [DRIPA] doit conserver les données de manière à pouvoir les transmettre, sans délai injustifié, en réponse à des requêtes. »

38 L'article 9 de ce même règlement, intitulé « Contrôle du commissaire chargé de l'information », énonce :

« Le commissaire chargé de l'information doit contrôler le respect des exigences ou restrictions, prévues dans cette partie, en lien avec l'intégrité, la sécurité et la destruction des données conservées en vertu de l'article 1 de la [DRIPA]. »

Le code des pratiques

39 L'Acquisition and Disclosure of Communications Data Code of Practice (code des bonnes pratiques relatives à l'obtention et à la divulgation des données relatives à

des communications, ci-après le « code des pratiques ») contient, à ses paragraphes 2.5 à 2.9 et 2.36 à 2.45, des orientations sur la nécessité et la proportionnalité de l'obtention des données relatives à des communications. Selon les explications de la juridiction de renvoi dans l'affaire C-698/15, une attention particulière doit, conformément aux paragraphes 3.72 à 3.77 de ce code, être accordée à la nécessité et à la proportionnalité lorsque les données relatives à des communications demandées se rapportent à une personne qui est membre d'une profession bénéficiant d'informations protégées par le secret professionnel ou autrement confidentielles.

40 En vertu des paragraphes 3.78 à 3.84 dudit code, une ordonnance judiciaire est requise dans le cas particulier d'une demande portant sur des données relatives à des communications, effectuée en vue d'identifier la source de journalistes. Selon les paragraphes 3.85 à 3.87 de ce même code, une approbation judiciaire est requise en cas de demande d'accès formulée par des autorités locales. Aucune autorisation judiciaire ou émanant d'une entité indépendante n'est, en revanche, nécessaire en ce qui concerne l'accès à des données relatives à des communications protégées par un secret professionnel légal ou se rapportant à des docteurs en médecine, à des membres du Parlement ou à des ministres des cultes.

41 Le paragraphe 7.1 du code des pratiques prévoit que les données relatives à des communications acquises ou obtenues en vertu des dispositions de la RIPA ainsi que tous les extraits, résumés et copies de ces données doivent être traités et stockés de manière sûre. En outre, les exigences figurant dans le Data Protection Act (loi relative à la protection des données) doivent être respectées.

42 Conformément au paragraphe 7.18 du code des pratiques, lorsqu'une autorité publique du Royaume-Uni envisage la possible divulgation à des autorités étrangères de données relatives à des communications, elle doit, notamment, examiner si ces données vont être protégées de manière adéquate. Toutefois, il ressort du paragraphe 7.22 de ce code qu'un transfert des données vers des pays tiers peut avoir lieu lorsque ce transfert est nécessaire pour des raisons liées à un intérêt public important, même lorsque le pays tiers n'assure pas un niveau de protection adéquat. Selon les indications de la juridiction de renvoi dans l'affaire C-698/15, le ministre de l'Intérieur peut établir un certificat de sécurité nationale qui exonère certaines données du respect des dispositions prévues par la législation.

43 Au paragraphe 8.1 dudit code, il est rappelé que la RIPA a institué l'Interception of Communications Commissioner (commissaire à l'interception des communications, Royaume-Uni), dont le rôle est, notamment, de superviser de manière indépendante l'exercice et la mise en œuvre des pouvoirs et des devoirs énoncés au chapitre II de la partie I de la RIPA. Ainsi qu'il ressort du paragraphe 8.3 de ce même code, ce commissaire est autorisé, lorsqu'il peut « établir qu'un individu a été lésé par un manquement intentionnel ou par imprudence », à informer cet individu qu'un usage illicite de compétences est soupçonné.

Les litiges au principal et les questions préjudicielles

L'affaire C-203/15

44 Le 9 avril 2014, Tele2 Sverige, fournisseur de services de communications électroniques établi en Suède, a notifié à la PTS que, à la suite de l'invalidation de la directive 2006/24 par l'arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, ci-après l'« arrêt Digital Rights », EU:C:2014:238), elle cesserait, à compter du 14 avril 2014, de conserver les données relatives aux communications électroniques, visées par la LEK, et qu'elle procéderait à la suppression des données conservées jusqu'à cette date.

45 Le 15 avril 2014, la Rikspolisstyrelsen (direction générale de la police nationale, Suède) a saisi la PTS d'une plainte en raison du fait que Tele2 Sverige avait cessé de lui communiquer les données en cause.

46 Le 29 avril 2014, le justitieminister (ministre de la Justice, Suède) a désigné un rapporteur spécial chargé d'analyser la réglementation suédoise en cause au regard de l'arrêt Digital Rights. Dans un rapport du 13 juin 2014, intitulé « Datalagring, EU-rätten och svensk rätt, n° Ds 2014:23 » (Conservation de données, droit de l'Union et droit suédois, ci-après le « rapport de 2014 »), le rapporteur spécial a conclu que la réglementation nationale relative à la conservation des données, telle que prévue aux articles 16 a à 16 f de la LEK, n'était contraire ni au droit de l'Union ni à la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après la « CEDH »). Le rapporteur spécial a souligné que l'arrêt Digital Rights ne pouvait être interprété en ce sens qu'il aurait censuré le principe même d'une conservation généralisée et indifférenciée des données. De son point de vue, l'arrêt Digital Rights ne devait pas non plus être compris en ce sens que la Cour y aurait établi une série de critères devant tous être satisfaits pour qu'une réglementation puisse être considérée comme proportionnée. Il conviendrait d'apprécier toutes les circonstances afin de déterminer la conformité de la réglementation suédoise au droit de l'Union, telle que l'ampleur de la conservation des données au regard des dispositions sur l'accès aux données, sur la durée de leur conservation, sur leur protection ainsi que sur leur sécurité.

47 Sur cette base, la PTS a, le 19 juin 2014, informé Tele2 Sverige que celle-ci manquait aux obligations prévues par la réglementation nationale en ne conservant pas les données visées par la LEK pendant six mois à des fins de lutte contre la criminalité. Par injonction du 27 juin 2014, la PTS lui a ensuite ordonné de procéder, au plus tard le 25 juillet 2014, à la conservation de ces données.

48 Considérant que le rapport de 2014 reposait sur une interprétation erronée de l'arrêt Digital Rights et que l'obligation de conservation des données était contraire aux droits fondamentaux garantis par la Charte, Tele2 Sverige a introduit un recours devant le Förvaltningsrätten i Stockholm (tribunal administratif de

Stockholm, Suède) contre l'injonction du 27 juin 2014. Cette juridiction ayant rejeté le recours par jugement du 13 octobre 2014, Tele2 Sverige a interjeté appel de ce jugement devant la juridiction de renvoi.

49 Selon la juridiction de renvoi, la compatibilité de la réglementation suédoise avec le droit de l'Union doit être appréciée à la lumière de l'article 15, paragraphe 1, de la directive 2002/58. En effet, alors que cette directive poserait le principe selon lequel les données relatives au trafic et les données de localisation doivent être effacées ou rendues anonymes lorsqu'elles ne sont plus nécessaires pour la transmission d'une communication, l'article 15, paragraphe 1, de ladite directive introduirait une dérogation à ce principe puisqu'il autoriserait les États membres, lorsque cela est justifié par un des motifs qu'il énonce, à limiter cette obligation d'effacement ou d'anonymisation ou encore à prévoir la conservation de données. Ainsi, le droit de l'Union permettrait, dans certaines situations, la conservation des données relatives aux communications électroniques.

50 La juridiction de renvoi se demande néanmoins si une obligation généralisée et indifférenciée de conservation des données relatives aux communications électroniques, telle que celle en cause au principal, est compatible, compte tenu de l'arrêt Digital Rights, avec l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte. Eu égard aux avis divergents des parties à cet égard, il conviendrait que la Cour se prononce de manière univoque sur la question de savoir si, ainsi que le considère Tele2 Sverige, la conservation généralisée et indifférenciée des données relatives aux communications électroniques est en elle-même incompatible avec les articles 7 et 8 ainsi qu'avec l'article 52, paragraphe 1, de la Charte, ou si, comme il ressortirait du rapport de 2014, la compatibilité d'une telle conservation de données doit être appréciée au regard des dispositions relatives à l'accès aux données, à leur protection et à leur sécurité ainsi qu'à la durée de leur conservation.

51 C'est dans ces conditions que la juridiction de renvoi a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) Une obligation générale de conservation de données, relative à toute personne et à tous les moyens de communication électronique et portant sur l'ensemble des données relatives au trafic, sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif de lutte contre la criminalité [...], est-elle compatible avec l'article 15, paragraphe 1, de la directive 2002/58 compte tenu des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte ?

2) S'il est répondu par la négative à la première question, une telle obligation de conservation peut-elle néanmoins être admise :

a) si l'accès par les autorités nationales aux données conservées est encadré de la manière précisée aux points 19 à 36 [de la décision de renvoi], et

b) si les exigences de protection et de sécurité des données sont régies de la manière précisée aux points 38 à 43 [de la décision de renvoi], et que

c) toutes les données en question doivent être conservées pendant six mois à compter du jour de l'achèvement de la communication avant d'être effacées, comme il est exposé au point 37 [de la décision de renvoi] ? »

L'affaire C-698/15

52 MM. Watson, Brice et Lewis ont chacun introduit, devant la High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) [Haute Cour de justice (Angleterre et pays de Galles), division du Queens' Bench (chambre divisionnaire), Royaume-Uni], un recours juridictionnel tendant au contrôle de la légalité de l'article 1er de la DRIPA, en invoquant notamment l'incompatibilité de cet article avec les articles 7 et 8 de la Charte ainsi qu'avec l'article 8 de la CEDH.

53 Par arrêt du 17 juillet 2015, la High Court of Justice (England & Wales), Queens' Bench Division (Divisional Court) [Haute Cour de justice (Angleterre et pays de Galles), division du Queens' Bench (chambre divisionnaire)] a constaté que l'arrêt Digital Rights énonçait des « exigences impératives en droit de l'Union » applicables aux réglementations des États membres en matière de conservation des données relatives à des communications ainsi qu'à l'accès à de telles données. Selon cette juridiction, puisque la Cour a, dans cet arrêt, considéré que la directive 2006/24 était incompatible avec le principe de proportionnalité, une réglementation nationale au contenu identique à celui de cette directive ne pourrait pas non plus être compatible avec ce principe. Il ressortirait de la logique sous-tendant l'arrêt Digital Rights qu'une législation établissant un régime généralisé de conservation des données relatives à des communications viole les droits garantis aux articles 7 et 8 de la Charte, à moins que cette législation ne soit complétée par un régime d'accès aux données, défini par le droit national, qui prévoit des garanties suffisantes pour la sauvegarde de ces droits. Ainsi, l'article 1er de la DRIPA ne serait pas compatible avec les articles 7 et 8 de la Charte dans la mesure où il n'établirait pas de règles claires et précises relatives à l'accès et à l'utilisation des données conservées et où il ne subordonnerait pas l'accès à ces données à un contrôle préalable effectué par une juridiction ou une entité administrative indépendante.

54 Le ministre de l'Intérieur a interjeté appel de cet arrêt devant la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile), Royaume-Uni].

55 Cette juridiction relève que l'article 1er, paragraphe 1, de la DRIPA habilite le ministre de l'Intérieur à adopter, en l'absence de toute autorisation préalable d'une juridiction ou d'une entité administrative indépendante, un régime général imposant aux opérateurs de télécommunications publiques de conserver toutes les données portant sur tout service postal ou tout service de télécommunications pendant une durée maximale de douze mois pour autant qu'il estime qu'une telle exigence est nécessaire et proportionnée afin de poursuivre les fins énoncées dans la réglementation du Royaume-Uni. Même si ces données ne comprennent pas le contenu d'une communication, elles pourraient avoir un caractère particulièrement intrusif dans la vie privée des utilisateurs de services de communications.

56 Dans la décision de renvoi et dans son arrêt du 20 novembre 2015, rendu dans le cadre de la procédure d'appel et par lequel elle a décidé de soumettre à la Cour la présente demande de décision préjudicielle, la juridiction de renvoi considère que les règles nationales relatives à la conservation des données relèvent nécessairement de l'article 15, paragraphe 1, de la directive 2002/58 et doivent donc respecter les exigences découlant de la Charte. Cependant, conformément à l'article 1er, paragraphe 3, de cette directive, le législateur de l'Union n'aurait pas harmonisé les règles portant sur l'accès aux données conservées.

57 S'agissant de l'incidence de l'arrêt Digital Rights sur les questions soulevées dans le litige au principal, la juridiction de renvoi relève que, dans l'affaire ayant conduit à cet arrêt, la Cour avait été saisie de la validité de la directive 2006/24 et non de celle d'une réglementation nationale. Eu égard notamment au rapport étroit existant entre la conservation des données et l'accès à ces données, il aurait été indispensable que cette directive s'accompagnât d'une série de garanties et que l'arrêt Digital Rights analysât, lors de l'examen de la légalité du régime de conservation des données établi par ladite directive, les règles relatives à l'accès à ces données. La Cour n'aurait donc pas envisagé d'énoncer, dans cet arrêt, des exigences impératives s'appliquant aux réglementations nationales relatives à l'accès aux données ne mettant pas en œuvre le droit de l'Union. En outre, le raisonnement de la Cour aurait été étroitement lié à l'objectif poursuivi par cette même directive. Toutefois, une réglementation nationale devrait être appréciée au regard des objectifs poursuivis par celle-ci et de son contexte.

58 S'agissant de la nécessité de saisir la Cour d'un renvoi préjudiciel, la juridiction de renvoi met en exergue le fait que, à la date d'adoption de la décision de renvoi, six juridictions d'autres États membres, dont cinq de dernière instance, avaient annulé des législations nationales en se fondant sur l'arrêt Digital Rights. La réponse aux questions soulevées ne serait donc pas évidente, alors qu'elle serait nécessaire pour juger les affaires dont cette juridiction est saisie.

59 Dans ces conditions, la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile)] a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) L'arrêt Digital Rights (y compris, notamment, ses points 60 à 62) établit-il des exigences impératives en droit de l'Union, applicables au régime national d'un État membre régissant l'accès aux données conservées conformément à la législation nationale, afin de se conformer aux articles 7 et 8 de la Charte ?

2) L'arrêt Digital Rights étend-il la portée des articles 7 et/ou 8 de la Charte au-delà de celle de l'article 8 de la CEDH, telle qu'établie par la jurisprudence de la Cour européenne des droits de l'homme ? »

Sur la procédure devant la Cour

60 Par ordonnance du 1er février 2016, Davis e.a. (C-698/15, non publiée, EU:C:2016:70), le président de la Cour a décidé de faire droit à la demande de la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile)] tendant à ce que l'affaire C-698/15 soit soumise à la procédure accélérée prévue à l'article 105, paragraphe 1, du règlement de procédure de la Cour.

61 Par décision du président de la Cour du 10 mars 2016, les affaires C-203/15 et C-698/15 ont été jointes aux fins de la procédure orale et de l'arrêt.

Sur les questions préjudicielles

Sur la première question dans l'affaire C-203/15

62 Par la première question dans l'affaire C-203/15, le Kammarrätten i Stockholm (cour d'appel administrative de Stockholm) demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 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 telle que celle en cause au principal prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique.

63 Cette question trouve son origine, notamment, dans le fait que la directive 2006/24, que la réglementation nationale en cause au principal a eu pour objet de transposer, a été déclarée invalide par l'arrêt Digital Rights, mais que les parties divergent sur la portée de cet arrêt et sur son incidence sur cette réglementation, celle-ci régissant la conservation des données relatives au trafic et des données de localisation ainsi que l'accès à ces données par les autorités nationales.

64 Il convient d'examiner au préalable si une réglementation nationale telle que celle en cause au principal relève du champ d'application du droit de l'Union.

Sur le champ d'application de la directive 2002/58

65 Les États membres ayant soumis des observations écrites à la Cour ont exprimé des avis divergents quant à la question de savoir si et dans quelle mesure des réglementations nationales portant sur la conservation des données relatives au trafic et des données de localisation ainsi que sur l'accès à ces données par les autorités nationales, à des fins de lutte contre la criminalité, relèvent du champ d'application de la directive 2002/58. En effet, tandis que, notamment, les gouvernements belge, danois, allemand, estonien et l'Irlande ainsi que le gouvernement néerlandais ont exprimé l'avis qu'une telle question appelle une réponse positive, le gouvernement tchèque a proposé qu'il soit répondu par la négative à cette question, faisant observer que ces réglementations ont pour seul objectif la lutte contre la criminalité. Quant au gouvernement du Royaume-Uni, il a fait valoir que ne relèvent du champ d'application de cette directive que les réglementations portant sur la conservation des données et non celles portant sur l'accès à ces données par les autorités nationales compétentes en matière de répression.

66 S'agissant, enfin, de la Commission, si celle-ci a soutenu, dans ses observations écrites soumises à la Cour dans l'affaire C-203/15, que la réglementation nationale en cause au principal relève du champ d'application de la directive 2002/58, elle a avancé, dans ses observations écrites dans l'affaire C-698/15, que seules les règles nationales relatives à la conservation des données, et non celles relatives à l'accès des autorités nationales à ces données, relèvent du champ d'application de cette directive. Ces dernières règles devraient néanmoins, selon elle, être prises en considération afin d'évaluer si une réglementation nationale régissant la conservation des données par les fournisseurs de services de communications électroniques constitue une ingérence proportionnée dans les droits fondamentaux garantis aux articles 7 et 8 de la Charte.

67 À cet égard, il convient de relever que l'étendue du champ d'application de la directive 2002/58 doit être appréciée en tenant compte notamment de l'économie générale de cette dernière.

68 Aux termes de son article 1er, paragraphe 1, la directive 2002/58 prévoit, notamment, l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et des libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques.

69 L'article 1er, paragraphe 3, de cette directive exclut du champ d'application de celle-ci les « activités de l'État » dans les domaines qui y sont visés, à savoir, notamment, les activités de l'État dans le domaine pénal et celles concernant la sécurité publique, la défense, 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 (voir, par

analogie, en ce qui concerne l'article 3, paragraphe 2, premier tiret, de la directive 95/46, arrêts du 6 novembre 2003, Lindqvist, C-101/01, EU:C:2003:596, point 43, ainsi que du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 41).

70 Quant à l'article 3 de la directive 2002/58, il énonce que cette directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans l'Union, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification (ci-après les « services de communications électroniques »). Partant, ladite directive doit être regardée comme régissant les activités des fournisseurs de tels services.

71 L'article 15, paragraphe 1, de la directive 2002/58 autorise les États membres à adopter, dans le respect des conditions qu'il prévoit, 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 [cette] directive ». L'article 15, paragraphe 1, deuxième phrase, de ladite directive identifie, à titre d'exemples de mesures susceptibles d'être ainsi adoptées par les États membres, les mesures « prévoyant la conservation de données ».

72 Certes, les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 se rapportent à des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 51). En outre, les finalités auxquelles, en vertu de cette disposition, de telles mesures doivent répondre, en l'occurrence la sauvegarde de la sécurité nationale, de la défense et de la sécurité publique ainsi que la mise en œuvre de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, recoupent substantiellement les finalités poursuivies par les activités visées à l'article 1er, paragraphe 3, de cette directive.

73 Toutefois, eu égard à l'économie générale de la directive 2002/58, les éléments relevés au point précédent du présent arrêt n'autorisent pas à conclure que les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 seraient exclues du champ d'application de cette directive, sauf à priver cette disposition de tout effet utile. En effet, ladite disposition présuppose nécessairement que les mesures nationales qui y sont visées, telles que celles relatives à la conservation de données à des fins de lutte contre la criminalité, relèvent du champ d'application de cette même directive, puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit.

74 En outre, les mesures législatives qui sont visées à l'article 15, paragraphe 1, de la directive 2002/58 régissent, aux fins mentionnées à cette disposition, l'activité des fournisseurs de services de communications électroniques. Partant, cet article 15, paragraphe 1, lu en combinaison avec l'article 3 de ladite directive, doit être interprété en ce sens que de telles mesures législatives relèvent du champ d'application de cette même directive.

75 Relève, en particulier, de ce champ d'application une mesure législative, telle que celle en cause au principal, qui impose à ces fournisseurs de conserver les données relatives au trafic et les données de localisation, puisqu'une telle activité implique nécessairement un traitement, par ceux-ci, de données à caractère personnel.

76 Relève également dudit champ d'application une mesure législative portant, comme dans l'affaire au principal, sur l'accès des autorités nationales aux données conservées par les fournisseurs de services de communications électroniques.

77 En effet, la protection de la confidentialité des communications électroniques et des données relatives au trafic y afférentes, garantie à l'article 5, paragraphe 1, de la directive 2002/58, s'applique aux mesures prises par toutes les personnes autres que les utilisateurs, qu'il s'agisse de personnes ou d'entités privées ou d'entités étatiques. Comme le confirme le considérant 21 de cette directive, celle-ci vise à empêcher « tout accès » non autorisé aux communications, y compris à « toute donnée afférente à ces communications », afin de protéger la confidentialité des communications électroniques.

78 Dans ces conditions, une mesure législative par laquelle un État membre impose, sur le fondement de l'article 15, paragraphe 1, de la directive 2002/58, aux fournisseurs de services de communications électroniques, aux fins mentionnées par cette disposition, d'accorder aux autorités nationales, dans les conditions prévues par une telle mesure, l'accès aux données conservées par lesdits fournisseurs porte sur des traitements de données à caractère personnel par ces derniers, traitements qui relèvent du champ d'application de cette directive.

79 En outre, dès lors que la conservation de données n'intervient qu'aux seules fins de rendre, le cas échéant, les données accessibles aux autorités nationales compétentes, une réglementation nationale prévoyant la conservation de données implique, en principe, nécessairement l'existence de dispositions relatives à l'accès des autorités nationales compétentes aux données conservées par les fournisseurs de services de communications électroniques.

80 Cette interprétation est corroborée par l'article 15, paragraphe 1 ter, de la directive 2002/58, selon lequel les fournisseurs établissent, sur la base des dispositions nationales adoptées au titre de l'article 15, paragraphe 1, de cette directive, des procédures internes permettant de répondre aux demandes d'accès aux données à caractère personnel concernant les utilisateurs.

81 Il résulte de ce qui précède qu'une réglementation nationale, telle que celle en cause au principal dans les affaires C-203/15 et C-698/15, relève du champ d'application de la directive 2002/58.

Sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, au regard des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte

82 Il convient de relever que, conformément à l'article 1er, paragraphe 2, de la directive 2002/58, les dispositions de celle-ci « précisent et complètent » la directive 95/46. Ainsi que l'énonce son considérant 2, la directive 2002/58 vise à garantir, en particulier, le plein respect des droits énoncés aux articles 7 et 8 de la Charte. À cet égard, il ressort de l'exposé des motifs de la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [COM (2000) 385 final], à l'origine de la directive 2002/58, que le législateur de l'Union a entendu « faire en sorte qu'un niveau élevé de protection des données à caractère personnel et de la vie privée continue à être garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée ».

83 À cette fin, la directive 2002/58 contient des dispositions spécifiques visant, ainsi qu'il ressort notamment de ses considérants 6 et 7, à protéger les utilisateurs des services de communications électroniques contre les dangers pour les données à caractère personnel et la vie privée résultant des nouvelles technologies et de la capacité accrue de stockage et de traitement automatisés de données.

84 En particulier, l'article 5, paragraphe 1, de cette directive prévoit que les États membres doivent garantir, par leur 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.

85 Le principe de confidentialité des communications instauré par la directive 2002/58 implique, entre autres, ainsi qu'il ressort de l'article 5, paragraphe 1, deuxième phrase, de celle-ci, une interdiction faite, en principe, à toute autre personne que les utilisateurs de stocker, sans le consentement de ceux-ci, les données relatives au trafic afférentes aux communications électroniques. Font seuls l'objet d'exceptions les personnes légalement autorisées conformément à l'article 15, paragraphe 1, de cette directive et le stockage technique nécessaire à l'acheminement d'une communication (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 47).

86 Ainsi, et comme le confirment les considérants 22 et 26 de la directive 2002/58, le traitement et le stockage des données relatives au trafic ne sont autorisés, en vertu de l'article 6 de cette directive, que dans la mesure et pour la durée nécessaires à la facturation des services, à la commercialisation de ceux-ci et à la fourniture de

services à valeur ajoutée (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, points 47 et 48). S'agissant, en particulier, de la facturation des services, 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. Une fois cette durée expirée, les données ayant été traitées et stockées doivent être effacées ou rendues anonymes. S'agissant des données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de ladite directive prévoit que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés.

87 La portée des dispositions des articles 5 et 6 et de l'article 9, paragraphe 1, de la directive 2002/58, qui visent à garantir la confidentialité des communications et des données y afférentes ainsi qu'à minimiser les risques d'abus, doit en outre être appréciée à la lumière du considérant 30 de cette directive, aux termes duquel « [l]es systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires ».

88 Certes, l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 50).

89 Néanmoins, en ce que l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres de limiter la portée de l'obligation de principe d'assurer la confidentialité des communications et des données relatives au trafic y afférentes, il est, conformément à la jurisprudence constante de la Cour, d'interprétation stricte (voir, par analogie, arrêt du 22 novembre 2012, Probst, C-119/12, EU:C:2012:748, point 23). Une telle disposition ne saurait donc justifier que la dérogation à cette obligation de principe et, en particulier, à l'interdiction de stocker ces données, prévue à l'article 5 de cette directive, devienne la règle, sauf à vider largement cette dernière disposition de sa portée.

90 Il convient, à cet égard, de relever que l'article 15, paragraphe 1, première phrase, de la directive 2002/58 prévoit que les mesures législatives qu'il vise et qui dérogent au principe de confidentialité des communications et des données relatives au trafic y afférentes doivent avoir pour objectif de « sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou [d']assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques », ou doivent poursuivre un des autres objectifs visés à l'article 13, paragraphe 1, de la directive 95/46, auquel renvoie l'article 15, paragraphe 1, première phrase, de la directive 2002/58 (voir, en ce sens, arrêt du

29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 53). Une telle énumération d'objectifs revêt un caractère exhaustif ainsi qu'il ressort de l'article 15, paragraphe 1, deuxième phrase, de cette dernière directive, aux termes duquel les mesures législatives doivent être justifiées par « un des motifs énoncés » à l'article 15, paragraphe 1, première phrase, de ladite directive. Partant, les États membres ne sauraient adopter de telles mesures à d'autres fins que celles énumérées à cette dernière disposition.

91 En outre, l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 dispose que « [t]outes les mesures visées [à l'article 15, paragraphe 1, de cette directive] 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, [UE] », parmi lesquels figurent les principes généraux et les droits fondamentaux qui sont désormais garantis par la Charte. L'article 15, paragraphe 1, de la directive 2002/58 doit ainsi être interprété à la lumière des droits fondamentaux garantis par la Charte (voir, par analogie, en ce qui concerne la directive 95/46, arrêts du 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 68 ; du 13 mai 2014, Google Spain et Google, C-131/12, EU:C:2014:317, point 68, ainsi que du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 38).

92 À cet égard, il importe de souligner que l'obligation faite aux fournisseurs de services de communications électroniques, par une réglementation nationale telle que celle en cause au principal, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, qui sont explicitement mentionnés dans les questions préjudicielles, mais également de la liberté d'expression garantie à l'article 11 de la Charte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, points 25 et 70).

93 Ainsi, l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour (voir, en ce sens, arrêt du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 39 et jurisprudence citée), doit être prise en compte lors de l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58. Il en va de même du droit à la liberté d'expression eu égard à l'importance particulière que revêt cette liberté dans toute société démocratique. Ce droit fondamental, garanti à l'article 11 de la Charte, constitue l'un des fondements essentiels d'une société démocratique et pluraliste, faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 12 juin 2003, Schmidberger, C-112/00, EU:C:2003:333, point 79, et du 6 septembre 2011, Patriciello, C-163/10, EU:C:2011:543, point 31).

94 À cet égard, il convient de rappeler que, conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et des libertés reconnus par celle-ci doit être prévue par la loi et respecter leur contenu essentiel. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à l'exercice de ces droits et de ces libertés que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui (arrêt du 15 février 2016, N., C-601/15 PPU, EU:C:2016:84, point 50).

95 À ce dernier égard, l'article 15, paragraphe 1, première phrase, de la directive 2002/58 prévoit que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'elle est « nécessaire, appropriée et proportionnée, au sein d'une société démocratique », au regard des objectifs que cette disposition énonce. Quant au considérant 11 de cette directive, il précise qu'une mesure de cette nature doit être « rigoureusement » proportionnée au but poursuivi. En ce qui concerne, en particulier, la conservation de données, l'article 15, paragraphe 1, deuxième phrase, de ladite directive exige que celle-ci n'ait lieu que « pendant une durée limitée » et « lorsque cela est justifié » par un des objectifs visés à l'article 15, paragraphe 1, première phrase, de cette même directive.

96 Le respect du principe de proportionnalité découle également de la jurisprudence constante de la Cour selon laquelle la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire (arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 56 ; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 77 ; Digital Rights, point 52, ainsi que du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 92).

97 S'agissant de la question de savoir si une réglementation nationale, telle que celle en cause dans l'affaire C-203/15, satisfait à ces conditions, il convient de relever que celle-ci prévoit une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, et qu'elle oblige les fournisseurs de services de communications électroniques à conserver ces données de manière systématique et continue, et ce sans aucune exception. Ainsi qu'il ressort de la décision de renvoi, les catégories de données visées par cette réglementation correspondent, en substance, à celles dont la conservation était prévue par la directive 2006/24.

98 Les données que doivent ainsi conserver les fournisseurs de services de communications électroniques permettent de retrouver et d'identifier la source d'une communication et la destination de celle-ci, de déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des

utilisateurs, ainsi que de localiser le matériel de communication mobile. Au nombre de ces données figurent, notamment, le nom et l'adresse de l'abonné ou de l'utilisateur inscrit, le numéro de téléphone de l'appelant et le numéro appelé ainsi qu'une adresse IP pour les services Internet. Ces données permettent, en particulier, de savoir quelle est la personne avec laquelle un abonné ou un utilisateur inscrit a communiqué et par quel moyen, tout comme de déterminer le temps de la communication ainsi que l'endroit à partir duquel celle-ci a eu lieu. En outre, elles permettent de connaître la fréquence des communications de l'abonné ou de l'utilisateur inscrit avec certaines personnes pendant une période donnée (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 26).

99 Prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions 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, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 27). En particulier, ces données fournissent les moyens d'établir, ainsi que l'a relevé M. l'avocat général aux points 253, 254 et 257 à 259 de ses conclusions, le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications.

100 L'ingérence que comporte une telle réglementation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance que la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 37).

101 Même si une telle réglementation n'autorise pas la conservation du contenu d'une communication et, partant, n'est pas de nature à porter atteinte au contenu essentiel desdits droits (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 39), la conservation des données relatives au trafic et des données de localisation pourrait toutefois avoir une incidence sur l'utilisation des moyens de communication électronique et, en conséquence, sur l'exercice par les utilisateurs de ces moyens de leur liberté d'expression, garantie à l'article 11 de la Charte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 28).

102 Eu égard à la gravité de l'ingérence dans les droits fondamentaux en cause que constitue une réglementation nationale prévoyant, aux fins de la lutte contre la criminalité, la conservation de données relatives au trafic et de données de

localisation, seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure (voir, par analogie, à propos de la directive 2006/24, arrêt Digital Rights, point 60).

103 En outre, si l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 51).

104 À cet égard, il convient de relever, d'une part, qu'une telle réglementation a pour effet, eu égard à ses caractéristiques décrites au point 97 du présent arrêt, que la conservation des données relatives au trafic et des données de localisation est la règle, alors que le système mis en place par la directive 2002/58 exige que cette conservation des données soit l'exception.

105 D'autre part, une réglementation nationale telle que celle en cause au principal, qui couvre de manière généralisée tous les abonnés et utilisateurs inscrits et vise tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic, ne prévoit aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi. Elle concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves. En outre, elle ne prévoit aucune exception, de telle sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, points 57 et 58).

106 Une telle réglementation ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 59).

107 Une réglementation nationale telle que celle en cause au principal excède donc les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige 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.

108 En revanche, 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, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, la conservation ciblée des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave, à condition que la conservation des données soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire.

109 Pour satisfaire aux exigences énoncées au point précédent du présent arrêt, cette réglementation nationale doit, en premier lieu, prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et imposant un minimum d'exigences, de telle sorte que les personnes dont les données ont été conservées disposent de garanties suffisantes permettant de protéger efficacement leurs données à caractère personnel contre les risques d'abus. Elle doit en particulier indiquer en quelles circonstances et sous quelles conditions une mesure de conservation des données peut, à titre préventif, être prise, garantissant ainsi qu'une telle mesure soit limitée au strict nécessaire (voir, par analogie, à propos de la directive 2006/24, arrêt Digital Rights, point 54 et jurisprudence citée).

110 En second lieu, s'agissant des conditions matérielles auxquelles doit satisfaire une réglementation nationale permettant, dans le cadre de la lutte contre la criminalité, la conservation, à titre préventif, des données relatives au trafic et des données de localisation, afin de garantir qu'elle soit limitée au strict nécessaire, il convient de relever que, si ces conditions peuvent varier en fonction des mesures prises aux fins de la prévention, de la recherche, de la détection et de la poursuite de la criminalité grave, la conservation des données n'en doit pas moins toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi. En particulier, de telles conditions doivent s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné.

111 S'agissant de la délimitation d'une telle mesure quant au public et aux situations potentiellement concernés, la réglementation nationale doit être fondée sur des éléments objectifs permettant de viser un public dont les données sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique. Une telle délimitation peut être assurée au moyen d'un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs, qu'il existe, dans une ou plusieurs zones géographiques, un risque élevé de préparation ou de commission de tels actes.

112 Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la première question dans l'affaire C-203/15 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 prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique.

Sur la seconde question dans l'affaire C-203/15 et la première question dans l'affaire C-698/15

113 Il y a lieu de relever à titre liminaire que le Kammarrätten i Stockholm (cour d'appel administrative de Stockholm) n'a posé la seconde question dans l'affaire C-203/15 que dans le cas de figure d'une réponse négative à la première question dans ladite affaire. Toutefois, cette seconde question est indépendante du caractère généralisé ou ciblé d'une conservation des données, au sens envisagé aux points 108 à 111 du présent arrêt. Partant, il convient de répondre conjointement à la seconde question dans l'affaire C-203/15 et à la première question dans l'affaire C-698/15, laquelle est posée indépendamment de l'étendue de l'obligation de conservation de données qui serait imposée aux fournisseurs de services de communications électroniques.

114 Par la seconde question dans l'affaire C-203/15 et la première question dans l'affaire C-698/15, les juridictions de renvoi demandent, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 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 régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union.

115 S'agissant des objectifs susceptibles de justifier une réglementation nationale dérogeant au principe de confidentialité des communications électroniques, il convient de rappeler que, dans la mesure où, ainsi qu'il a été constaté aux points 90 et 102 du présent arrêt, l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de la directive 2002/58 revêt un caractère exhaustif, l'accès aux données conservées doit répondre effectivement et strictement à l'un de ces objectifs. En outre, dès lors que l'objectif poursuivi par cette réglementation doit être en relation avec la gravité de l'ingérence dans les droits fondamentaux qu'entraîne cet accès, il s'ensuit que, en matière de prévention, de recherche, de détection et de poursuite d'infractions pénales, seule

la lutte contre la criminalité grave est susceptible de justifier un tel accès aux données conservées.

116 En ce qui concerne le respect du principe de proportionnalité, une réglementation nationale régissant les conditions dans lesquelles les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données conservées doit assurer, conformément à ce qui a été constaté aux points 95 et 96 du présent arrêt, qu'un tel accès n'ait lieu que dans les limites du strict nécessaire.

117 En outre, les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 devant, conformément au considérant 11 de cette directive, « être subordonnées à des garanties appropriées », une telle mesure doit, ainsi qu'il résulte de la jurisprudence citée au point 109 du présent arrêt, prévoir des règles claires et précises indiquant en quelles circonstances et sous quelles conditions les fournisseurs de services de communications électroniques doivent accorder aux autorités nationales compétentes l'accès aux données. De même, une mesure de cette nature doit être légalement contraignante en droit interne.

118 Afin de garantir que l'accès des autorités nationales compétentes aux données conservées soit limité au strict nécessaire, il appartient, certes, au droit national de déterminer les conditions dans lesquelles les fournisseurs de services de communications électroniques doivent accorder un tel accès. Toutefois, la réglementation nationale concernée ne saurait se limiter à exiger que l'accès réponde à l'un des objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, fût-ce la lutte contre la criminalité grave. En effet, une telle réglementation nationale doit également prévoir les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données conservées (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 61).

119 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 saurait être considéré comme 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 des abonnés ou des utilisateurs inscrits. À cet égard, un 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 (voir, par analogie, Cour EDH, 4 décembre 2015, Zakharov c. Russie, CE:ECHR:2015:1204JUD004714306, § 260). 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.

120 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, en principe, sauf cas d'urgence dûment justifiés, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités présentée, notamment, dans le cadre de procédures de prévention, de détection ou de poursuites pénales (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 62 ; voir également, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 12 janvier 2016, Szabó et Vissy c. Hongrie, CE:ECHR:2016:0112JUD003713814, §§ 77 et 80).

121 De même, il importe que les autorités nationales compétentes auxquelles l'accès aux données conservées a été accordé, en informent les personnes concernées, dans le cadre des procédures nationales applicables, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités. En effet, cette information est, de fait, nécessaire pour permettre à celles-ci d'exercer, notamment, le droit de recours, explicitement prévu à l'article 15, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 22 de la directive 95/46, en cas de violation de leurs droits (voir, par analogie, arrêts du 7 mai 2009, Rijkeboer, C-553/07, EU:C:2009:293, point 52, ainsi que du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, point 95).

122 En ce qui concerne les règles visant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques, il convient de constater que l'article 15, paragraphe 1, de la directive 2002/58 ne permet pas aux États membres de déroger à l'article 4, paragraphe 1, ainsi qu'à l'article 4, paragraphe 1 bis, de celle-ci. Ces dernières dispositions exigent que ces fournisseurs prennent les mesures d'ordre technique et organisationnel appropriées permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès illicite à ces données. Compte tenu de la quantité de données conservées, du caractère sensible de ces données ainsi que du risque d'accès illicite à celles-ci, les fournisseurs de services de communications électroniques doivent, aux fins d'assurer la pleine intégrité et la confidentialité desdites données, garantir un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles appropriées. En particulier, la réglementation nationale doit prévoir la conservation sur le territoire de l'Union ainsi que la destruction irrémédiable des données au terme de la durée de conservation de celles-ci (voir, par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, points 66 à 68).

123 En tout état de cause, les États membres doivent garantir le contrôle, par une autorité indépendante, du respect du niveau de protection garanti par le droit de l'Union en matière de protection des personnes physiques à l'égard du traitement des données à caractère personnel, un tel contrôle étant explicitement exigé à l'article 8, paragraphe 3, de la Charte et constituant, conformément à la jurisprudence constante de la Cour, un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel. S'il en était autrement, les personnes dont les données à caractère personnel ont été conservées seraient privées du droit, garanti à l'article 8, paragraphes 1 et 3, de la Charte, de saisir les autorités nationales de contrôle d'une demande aux fins de la protection de leurs données (voir, en ce sens, arrêts Digital Rights, point 68, ainsi que du 6 octobre 2015, Schrems, C-362/14, EU:C:2015:650, points 41 et 58).

124 Il appartient aux juridictions de renvoi de vérifier si et dans quelle mesure les réglementations nationales en cause au principal respectent les exigences découlant de 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, telles qu'explicitées aux points 115 à 123 du présent arrêt, en ce qui concerne tant l'accès des autorités nationales compétentes aux données conservées que la protection et le niveau de sécurité de ces données.

125 Eu égard à l'ensemble des considérations qui précèdent, il convient de répondre à la seconde question dans l'affaire C-203/15 et à la première question dans l'affaire C-698/15 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 régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union.

Sur la seconde question dans l'affaire C-698/15

126 Par la seconde question dans l'affaire C-698/15, la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile)] demande en substance si, dans l'arrêt Digital Rights, la Cour a interprété les articles 7 et/ou 8 de la Charte dans un sens allant au-delà de celui conféré à l'article 8 de la CEDH par la Cour européenne des droits de l'homme.

127 À titre liminaire, il convient de rappeler que, si, comme le confirme l'article 6, paragraphe 3, TUE, les droits fondamentaux reconnus par la CEDH font partie du droit de l'Union en tant que principes généraux, ladite convention ne constitue

pas, tant que l'Union n'y a pas adhéré, un instrument juridique formellement intégré à l'ordre juridique de l'Union (voir, en ce sens, arrêt du 15 février 2016, N., C-601/15 PPU, EU:C:2016:84, point 45 et jurisprudence citée).

128 Ainsi, l'interprétation de la directive 2002/58, en cause en l'occurrence, doit être opérée au regard uniquement des droits fondamentaux garantis par la Charte (voir, en ce sens, arrêt du 15 février 2016, N., C-601/15 PPU, EU:C:2016:84, point 46 et jurisprudence citée).

129 En outre, il convient de rappeler que les explications afférentes à l'article 52 de la Charte indiquent que l'article 52, paragraphe 3, de celle-ci vise à assurer la cohérence nécessaire entre la Charte et la CEDH, « sans que cela porte atteinte à l'autonomie du droit de l'Union et de la Cour de justice de l'Union européenne » (arrêt du 15 février 2016, N., C-601/15 PPU, EU:C:2016:84, point 47). En particulier, ainsi que le prévoit expressément l'article 52, paragraphe 3, seconde phrase, de la Charte, l'article 52, paragraphe 3, première phrase, de celle-ci ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue que la CEDH. À cela s'ajoute enfin le fait que l'article 8 de la Charte concerne un droit fondamental distinct de celui consacré à l'article 7 de celle-ci et qui n'a pas d'équivalent dans la CEDH.

130 Or, selon une jurisprudence constante de la Cour, la justification d'une demande de décision préjudicielle est non pas la formulation d'opinions consultatives sur des questions générales ou hypothétiques, mais le besoin inhérent à la solution effective d'un litige portant sur le droit de l'Union (voir, en ce sens, arrêts du 24 avril 2012, Kamberaj, C-571/10, EU:C:2012:233, point 41 ; du 26 février 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, point 42, ainsi que du 27 février 2014, Pohotovosť, C-470/12, EU:C:2014:101, point 29).

131 En l'occurrence, eu égard aux considérations figurant notamment aux points 128 et 129 du présent arrêt, la question de savoir si la protection conférée aux articles 7 et 8 de la Charte va au-delà de celle garantie à l'article 8 de la CEDH n'est pas de nature à influer sur l'interprétation de la directive 2002/58, lue à la lumière de la Charte, qui est en cause dans le litige au principal dans l'affaire C-698/15.

132 Ainsi, il n'apparaît pas qu'une réponse à la seconde question dans l'affaire C-698/15 puisse apporter des éléments d'interprétation du droit de l'Union qui soient nécessaires à la solution, au regard de ce droit, dudit litige.

133 Il s'ensuit que la seconde question dans l'affaire C-698/15 est irrecevable.

Sur les dépens

134 La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant les juridictions de renvoi, il appartient à celles-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 prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique.**

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 régissant la protection et la sécurité des données relatives au trafic et des données de localisation, en particulier l'accès des autorités nationales compétentes aux données conservées, sans limiter, dans le cadre de la lutte contre la criminalité, cet accès aux seules fins de lutte contre la criminalité grave, sans soumettre ledit accès à un contrôle préalable par une juridiction ou une autorité administrative indépendante, et sans exiger que les données en cause soient conservées sur le territoire de l'Union.**

3) **La seconde question posée par la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile), Royaume-Uni] est irrecevable.**

Signatures