ARRÊT DE LA COUR (grande chambre)
8 avril 2014 (*)

«Communications électroniques – Directive 2006/24/CE – Services de communications électroniques accessibles au public ou de réseaux publics de communications – Conservation de données générées ou traitées dans le cadre de la fourniture de tels services – Validité – Articles 7, 8 et 11 de la charte des droits fondamentaux de l'Union européenne»

Dans les affaires jointes C-293/12 et C-594/12,
ayant pour objet des demandes de décision préjudicielle au titre de l'article 267 TFUE, introduites par la High Court (Irlande) et le Verfassungsgerichtshof (Autriche), par décisions, respectivement, des 27 janvier et 28 novembre 2012, parvenues à la Cour les 11 juin et 19 décembre 2012, dans les procédures
Digital Rights Ireland Ltd (C-293/12)
contre
Minister for Communications, Marine and Natural Resources,
Minister for Justice, Equality and Law Reform,
Commissioner of the Garda Síochána,
Irlande,
The Attorney General,
en présence de:
Irish Human Rights Commission,

et

Kärntner Landesregierung (C-594/12),
Michael Seitlinger,
Christof Tschohl e.a.,

LA COUR (grande chambre),

composée de M. V. Skouris, président, M. K. Lenaerts, vice-président, M. A. Tizzano, M^me^ R. Silva de Lapuerta, MM. T. von Danwitz (rapporteur), E. Juhász, A. Borg Barthet, C. G. Fernlund et J. L. da Cruz Vilaça, présidents de chambre, MM. A. Rosas, G. Arestis, J.-C. Bonichot, A. Arabadjiev, M^me^ C. Toader et M. C. Vajda juges,
avocat général: M. P. Cruz Villalón,
greffier: M. K. Malacek, administrateur,
vu la procédure écrite et à la suite de l'audience du 9 juillet 2013,
considérant les observations présentées:

pour Digital Rights Ireland Ltd, par MM. F. Callanan, SC, et F. Crehan, BL, mandatés par M. S. McGarr, solicitor,

pour M. Seitlinger, par M^e^ G. Otto, Rechtsanwalt,

pour M. Tschohl e.a., par M^e^ E. Scheucher, Rechtsanwalt,

pour l'Irish Human Rights Commission, par M. P. Dillon Malone, BL, mandaté par M^me^ S. Lucey, solicitor,

pour l'Irlande, par M^me^ E. Creedon et M. D. McGuinness, en qualité d'agents, assistés de MM. E. Regan, SC, et D. Fennelly, JC,

pour le gouvernement autrichien, par MM. G. Hesse et G. Kunnert, en qualité d'agents,

pour le gouvernement espagnol, par M^me^ N. Díaz Abad, en qualité d'agent,

pour le gouvernement français, par MM. G. de Bergues et D. Colas ainsi que par M^me^ B. Beaupère-Manokha, en qualité d'agents,

pour le gouvernement italien, par M^me^ G. Palmieri, en qualité d'agent, assistée de M. A. De Stefano, avvocato dello Stato,

pour le gouvernement polonais, par MM. B. Majczyna et M. Szpunar, en qualité d'agents,

pour le gouvernement portugais, par M. L. Inez Fernandes et M^me^ C. Vieira Guerra, en qualité d'agents,

pour le gouvernement du Royaume-Uni, par M. L. Christie, en qualité d'agent, assisté de M^me^ S. Lee, barrister,

pour le Parlement européen, par MM. U. Rösslein et A. Caiola ainsi que par M^me^ K. Zejdová, en qualité d'agents,

pour le Conseil de l'Union européenne, par MM. J. Monteiro et E. Sitbon ainsi que par M^me^ I. Šulce, en qualité d'agents,

pour la Commission européenne, par M^me^ D. Maidani ainsi que par MM. B. Martenczuk et M. Wilderspin, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 12 décembre 2013,

rend le présent

Arrêt

Les demandes de décision préjudicielle portent sur la validité 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 L 105, p. 54).

La demande présentée par la High Court (affaire C-293/12) concerne un litige opposant Digital Rights Ireland Ltd (ci-après «Digital Rights») au Minister for Communications, Marine and Natural Resources, au Minister for Justice, Equality and Law Reform, au Commissioner of the Garda Síochána, à l'Irlande ainsi qu'à l'Attorney General au sujet de la légalité de mesures législatives et administratives nationales concernant la conservation de données relatives à des communications électroniques.

La demande présentée par le Verfassungsgerichtshof (affaire C-594/12) est relative à des recours en matière constitutionnelle introduits devant cette juridiction respectivement par la Kärntner Landesregierung (gouvernement du Land de Carinthie) ainsi que par MM. Seitlinger, Tschohl et 11 128 autres requérants au sujet de la compatibilité de la loi transposant la directive 2006/24 dans le droit interne autrichien avec la loi constitutionnelle fédérale (Bundes-Verfassungsgesetz).

Le cadre juridique

La directive 95/46/CE

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 L 281, p. 31), a, conformément à son article 1^er^, paragraphe 1, pour objet d'assurer la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel.

Quant à la sécurité des traitements de telles données, l'article 17, paragraphe 1, de ladite directive dispose:

«Les États membres prévoient que le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite.

Ces mesures doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger.»

La directive 2002/58/CE

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 L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO L 337, p. 11, ci-après la «directive 2002/58»), a pour objectif, conformément à son article 1^er^, paragraphe 1, d'harmoniser les dispositions des États membres 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, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans l'Union européenne. En vertu du paragraphe 2 du même article, les dispositions de cette directive précisent et complètent la directive 95/46 aux fins énoncées au paragraphe 1 susmentionné.

En ce qui concerne la sécurité du traitement des données, l'article 4 de la directive 2002/58 prévoit:

«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/CE, 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.

Les autorités nationales compétentes en la matière sont habilitées à vérifier les mesures prises par les fournisseurs de services de communications électroniques accessibles au public, ainsi qu'à émettre des recommandations sur les meilleures pratiques concernant le degré de sécurité que ces mesures devraient atteindre.

2. Lorsqu'il existe un risque particulier de violation de la sécurité du réseau, le fournisseur d'un service de communications électroniques accessible au public informe les abonnés de ce risque et, si les mesures que peut prendre le fournisseur du service ne permettent pas de l'écarter, de tout moyen éventuel d'y remédier, y compris en en indiquant le coût probable.»

Quant à la confidentialité des communications et des données relatives au trafic, l'article 5, paragraphes 1 et 3, de ladite directive dispose:

«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/CE, 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.»

Aux termes de l'article 6, paragraphe 1, de la directive 2002/58:

«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.»

L'article 15 de la directive 2002/58 dispose à son paragraphe 1:

«Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale – c'est-à-dire la sûreté de l'État – la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.»

La directive 2006/24

Après avoir lancé une consultation auprès des représentants des services répressifs, du secteur des communications électroniques et des experts en matière de protection des données, la Commission a présenté, le 21 septembre 2005, une analyse d'impact des options politiques relatives à des règles concernant la conservation des données relatives au trafic (ci-après l'«analyse d'impact»). Cette analyse a servi de base à l'élaboration de la proposition de directive du Parlement européen et du Conseil sur la conservation de données traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public, et modifiant la directive 2002/58/CE [COM(2005) 438 final, ci-après la «proposition de directive»], présentée le même jour, qui a abouti à l'adoption de la directive 2006/24 sur le fondement de l'article 95 CE.

Le considérant 4 de la directive 2006/24 énonce:

«L'article 15, paragraphe 1, de la directive 2002/58/CE énumère les conditions dans lesquelles les États membres peuvent 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 ladite directive. Toute limitation de ce type doit constituer une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour des raisons spécifiques d'ordre public, à savoir pour sauvegarder la sécurité nationale (c'est-à-dire la sûreté de l'État), la défense et la sécurité publique, ou pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées de systèmes de communications électroniques.»

Selon la première phrase du considérant 5 de la directive 2006/24, «[p]lusieurs États membres ont légiféré sur la conservation de données par les fournisseurs de services en vue de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales».

Les considérants 7 à 11 de la directive 2006/24 sont libellés comme suit:

Dans ses conclusions, le Conseil 'Justice et affaires intérieures' du 19 décembre 2002 souligne qu'en raison de l'accroissement important des possibilités qu'offrent les communications électroniques, les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile pour la prévention, la recherche, la détection et la poursuite d'infractions pénales, notamment de la criminalité organisée.

Dans sa déclaration du 25 mars 2004 sur la lutte contre le terrorisme, le Conseil européen a chargé le Conseil d'envisager des propositions en vue de l'établissement de règles relatives à la conservation, par les fournisseurs de services, des données relatives au trafic des communications.

En vertu de l'article 8 de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (CEDH) [signée à Rome le 4 novembre 1950], toute personne a droit au respect de sa vie privée et de sa correspondance. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire, entre autres, à la sécurité nationale, à la sûreté publique, à la défense de l'ordre et à la prévention des infractions pénales, ou à la protection des droits et des libertés d'autrui. Étant donné que la conservation des données s'est révélée être un outil d'investigation nécessaire et efficace pour les enquêtes menées par les services répressifs dans plusieurs États membres et, en particulier, relativement aux affaires graves telles que celles liées à la criminalité organisée et au terrorisme, il convient de veiller à ce que les données conservées soient accessibles aux services répressifs pendant un certain délai, dans les conditions prévues par la présente directive. […]

Le 13 juillet 2005, le Conseil a réaffirmé, dans sa déclaration condamnant les attentats terroristes de Londres, la nécessité d'adopter dans les meilleurs délais des mesures communes relatives à la conservation de données concernant les télécommunications.

Eu égard à l'importance des données relatives au trafic et des données de localisation pour la recherche, la détection et la poursuite d'infractions pénales, il est nécessaire, comme les travaux de recherche et l'expérience pratique de plusieurs États membres le démontrent, de garantir au niveau européen la conservation pendant un certain délai, dans les conditions prévues par la présente directive, des données traitées par les fournisseurs de communications électroniques dans le cadre de la fourniture de services de communications électroniques accessibles au public ou d'un réseau public de communications.»

Les considérants 16, 21 et 22 de ladite directive précisent:

Les obligations incombant aux prestataires de services concernant les mesures visant à garantir la qualité des données, qui résultent de l'article 6 de la directive 95/46/CE, tout comme leurs obligations concernant les mesures visant à garantir la confidentialité et la sécurité du traitement des données, qui résultent des articles 16 et 17 de ladite directive, sont pleinement applicables aux données qui sont conservées au sens de la présente directive.

Étant donné que les objectifs de la présente directive, à savoir l'harmonisation des obligations incombant aux fournisseurs de conserver certaines données et de faire en sorte que ces données soient disponibles aux fins de la recherche, de la détection et de la poursuite d'infractions graves telles que définies par chaque État membre dans son droit interne, ne peuvent pas être réalisés de manière suffisante par les États membres et peuvent donc, en raison des dimensions ou des effets de la présente directive, être mieux réalisés au niveau communautaire, la Communauté peut prendre des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité. Conformément au principe de proportionnalité, tel qu'énoncé audit article, la présente directive n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

La présente directive respecte les droits fondamentaux et observe les principes reconnus, notamment, par la charte des droits fondamentaux de l'Union européenne. La présente directive ainsi que la directive 2002/58/CE visent notamment à veiller à ce que les droits fondamentaux liés au respect de la vie privée et des communications des citoyens et à la protection des données à caractère personnel, tels que consacrés aux articles 7 et 8 de la charte, soient pleinement respectés.»

La directive 2006/24 prévoit l'obligation des fournisseurs de services de communications électroniques accessibles au public ou des réseaux publics de communications de conserver certaines données qui sont

générées ou traitées par ces fournisseurs. À cet égard, les articles 1er à 9, 11 et 13 de cette directive disposent:

«*Article premier*

Objet et champ d'application

1. La présente directive a pour objectif d'harmoniser les dispositions des États membres relatives aux obligations des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications en matière de conservation de certaines données qui sont générées ou traitées par ces fournisseurs, en vue de garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne.

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.

Article 2

Définitions

1. Aux fins de la présente directive, les définitions contenues dans la directive 95/46/CE, 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 services de communications électroniques (directive 'cadre') [...], ainsi que dans la directive 2002/58/CE s'appliquent.

2. Aux fins de la présente directive, on entend par:

'données', les données relatives au trafic et les données de localisation, ainsi que les données connexes nécessaires pour identifier l'abonné ou l'utilisateur;

'utilisateur', toute entité juridique ou personne physique qui utilise un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service;

'service téléphonique', les appels téléphoniques (notamment les appels vocaux, la messagerie vocale, la téléconférence et la communication de données), les services supplémentaires (notamment le renvoi et le transfert d'appels), les services de messagerie et multimédias (notamment les services de messages brefs, les services de médias améliorés et les services multimédias);

'numéro d'identifiant', le numéro d'identification exclusif attribué aux personnes qui s'abonnent ou s'inscrivent à un service d'accès à l'internet ou à un service de communication par l'internet;

'identifiant cellulaire', le numéro d'identification de la cellule où un appel de téléphonie mobile a commencé ou a pris fin;

'appel téléphonique infructueux', toute communication au cours de laquelle un appel téléphonique a été transmis mais est resté sans réponse ou a fait l'objet d'une intervention de la part du gestionnaire du réseau.

Article 3

Obligation de conservation de données

1. Par dérogation aux articles 5, 6 et 9 de la directive 2002/58/CE, 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.

Article 4

Accès aux données

Les États membres prennent les mesures nécessaires pour veiller à ce que les données conservées conformément à la présente directive ne soient transmises qu'aux autorités nationales compétentes, dans des cas précis et conformément au droit interne. La procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité sont arrêtées par chaque État membre dans son droit interne, sous réserve des dispositions du droit de l'Union européenne ou du droit international public applicables en la matière, en particulier la CEDH telle qu'interprétée par la Cour européenne des droits de l'homme.

Article 5

Catégories de données à conserver

1. Les États membres veillent à ce que soient conservées en application de la présente directive les catégories de données suivantes:

les données nécessaires pour retrouver et identifier la source d'une communication:

en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile:

e numéro de téléphone de l'appelant;

les nom et adresse de l'abonné ou de l'utilisateur inscrit;

en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet:

e(s) numéro(s) d'identifiant attribué(s);

le numéro d'identifiant et le numéro de téléphone attribués à toute communication entrant dans le réseau téléphonique public;

les nom et adresse de l'abonné ou de l'utilisateur inscrit à qui une adresse IP (protocole internet), un numéro d'identifiant ou un numéro de téléphone a été attribué au moment de la communication;

les données nécessaires pour identifier la destination d'une communication:

en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile:

le(s) numéro(s) composé(s) [le(s) numéro(s) de téléphone appelé(s)] et, dans les cas faisant intervenir des services complémentaires tels que le renvoi ou le transfert d'appels, le(s) numéro(s) vers le(s)quel(s) l'appel est réacheminé;

les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s);

en ce qui concerne le courrier électronique par l'internet et la téléphonie par l'internet:

le numéro d'identifiant ou le numéro de téléphone du (des) destinataire(s) prévu(s) d'un appel téléphonique par l'internet;

les nom et adresse de l'abonné (des abonnés) ou de l'utilisateur (des utilisateurs) inscrit(s) et le numéro d'identifiant du destinataire prévu de la communication;

les données nécessaires pour déterminer la date, l'heure et la durée d'une communication:

en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile, la date et l'heure de début et de fin de la communication;

en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet:

la date et l'heure de l'ouverture et de la fermeture de la session du service d'accès à l'internet dans un fuseau horaire déterminé, ainsi que l'adresse IP (protocole internet), qu'elle soit dynamique ou statique, attribuée à une communication par le fournisseur d'accès à l'internet, ainsi que le numéro d'identifiant de l'abonné ou de l'utilisateur inscrit;

la date et l'heure de l'ouverture et de la fermeture de la session du service de courrier électronique par l'internet ou de téléphonie par l'internet dans un fuseau horaire déterminé;

les données nécessaires pour déterminer le type de communication:

en ce qui concerne la téléphonie fixe en réseau et la téléphonie mobile, le service téléphonique utilisé;

en ce qui concerne le courrier électronique par l'internet et la téléphonie par l'internet, le service internet utilisé;

les données nécessaires pour identifier le matériel de communication des utilisateurs ou ce qui est censé être leur matériel:

en ce qui concerne la téléphonie fixe en réseau, le numéro de téléphone de l'appelant et le numéro appelé;

en ce qui concerne la téléphonie mobile:

e numéro de téléphone de l'appelant et le numéro appelé;

l'identité internationale d'abonné mobile (IMSI) de l'appelant;

l'identité internationale d'équipement mobile (IMEI) de l'appelant;

l'IMSI de l'appelé;

l'IMEI de l'appelé;

dans le cas des services anonymes à prépaiement, la date et l'heure de la première activation du service ainsi que l'identité de localisation (identifiant cellulaire) d'où le service a été activé;

en ce qui concerne l'accès à l'internet, le courrier électronique par l'internet et la téléphonie par l'internet:

e numéro de téléphone de l'appelant pour l'accès commuté;

la ligne d'abonné numérique (DSL) ou tout autre point terminal de l'auteur de la communication;

les données nécessaires pour localiser le matériel de communication mobile:

l'identité de localisation (identifiant cellulaire) au début de la communication;

les données permettant d'établir la localisation géographique des cellules, en se référant à leur identité de localisation (identifiant cellulaire), pendant la période au cours de laquelle les données de communication sont conservées.

2. Aucune donnée révélant le contenu de la communication ne peut être conservée au titre de la présente directive.

Article 6

Durées de conservation

Les États membres veillent à ce que les catégories de données visées à l'article 5 soient conservées pour une

durée minimale de six mois et maximale de deux ans à compter de la date de la communication.

Article 7

Protection et sécurité des données

Sans préjudice des dispositions adoptées en application des directives 95/46/CE et 2002/58/CE, chaque État membre veille à ce que les fournisseurs de services de communications électroniques accessibles au public ou d'un réseau public de communications respectent, au minimum, les principes suivants en matière de sécurité des données, pour ce qui concerne les données conservées conformément à la présente directive:

les données conservées doivent être de la même qualité et soumises aux mêmes exigences de sécurité et de protection que les données sur le réseau;

les données font l'objet de mesures techniques et organisationnelles appropriées afin de les protéger contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle, ou le stockage, le traitement, l'accès ou la divulgation non autorisés ou illicites;

les données font l'objet de mesures techniques et organisationnelles appropriées afin de garantir que l'accès aux données n'est effectué que par un personnel spécifiquement autorisé;

et

les données sont détruites lorsque leur durée de conservation prend fin, à l'exception des données auxquelles on a pu accéder et qui ont été préservées.

Article 8

Conditions à observer pour le stockage des données conservées

Les États membres veillent à ce que les données visées à l'article 5 soient conservées conformément à la présente directive de manière à ce que les données conservées et toute autre information nécessaire concernant ces données puissent, à leur demande, être transmises sans délai aux autorités compétentes.

Article 9

Autorité de contrôle

1. Chaque État membre désigne une ou plusieurs autorités publiques qui sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de l'article 7 pour ce qui concerne la sécurité des données conservées. Ces autorités peuvent être les mêmes que celles visées à l'article 28 de la directive 95/46/CE.

2. Les autorités visées au paragraphe 1 exercent en toute indépendance la surveillance visée audit paragraphe.

[...]

Article 11

Modification de la directive 2002/58/CE

À l'article 15 de la directive 2002/58/CE, le paragraphe suivant est inséré:

'1 *bis*. Le paragraphe 1 n'est pas applicable aux données dont la conservation est spécifiquement exigée par la [directive 2006/24] aux fins visées à l'article 1er, paragraphe 1, de ladite directive.'

Article 13

Recours, responsabilité et sanctions

1. Chaque État membre prend les mesures nécessaires pour veiller à ce que les mesures nationales mettant en œuvre le chapitre III de la directive 95/46/CE, relatif aux recours juridictionnels, à la responsabilité et aux sanctions, soient intégralement appliquées au traitement des données effectué au titre de la présente directive.

2 Chaque État membre prend, en particulier, les mesures nécessaires pour faire en sorte que l'accès intentionnel aux données conservées conformément à la présente directive ou le transfert de ces données qui ne sont pas autorisés par le droit interne adopté en application de la présente directive soient passibles de sanctions, y compris de sanctions administratives ou pénales, qui sont efficaces, proportionnées et dissuasives.»

Les litiges au principal et les questions préjudicielles

L'affaire C-293/12

Digital Rights a introduit le 11 août 2006 un recours devant la High Court dans le cadre duquel elle soutient qu'elle est propriétaire d'un téléphone portable qui a été enregistré le 3 juin 2006 et qu'elle utilise celui-ci depuis cette date. Elle met en cause la légalité de mesures législatives et administratives nationales concernant la conservation de données relatives à des communications électroniques et demande, notamment, à la juridiction de renvoi de constater la nullité de la directive 2006/24 et de la septième partie de la loi de 2005 sur la justice pénale (infractions terroristes) [Criminal Justice (Terrorist Offences) Act 2005] prévoyant que les fournisseurs de services de communications téléphoniques doivent conserver les données afférentes à ces dernières relatives au trafic et à la localisation pour une période déterminée par la loi, afin de prévenir et de détecter les infractions, d'enquêter sur celles-ci et de les poursuivre ainsi que de garantir la sécurité de l'État.

La High Court, considérant qu'elle n'est pas en mesure de trancher les questions relatives au droit national dont elle est saisie sans que la validité de la directive 2006/24 ait été examinée a décidé de surseoir à statuer

et de poser à la Cour les questions préjudicielles suivantes:

La restriction faite aux droits de la partie requérante en matière d'utilisation de téléphonie mobile qui découle des exigences des articles 3, 4 et 6 de la directive 2006/24 est-elle incompatible avec l'article 5, paragraphe 4, TUE, en ce qu'elle est disproportionnée et qu'elle n'est pas nécessaire ou qu'elle est inappropriée pour atteindre les objectifs légitimes tels que:

permettre que certaines données soient disponibles aux fins des enquêtes sur les infractions graves et aux fins de la détection et de la poursuite de ces dernières,

et/ou

garantir le bon fonctionnement du marché intérieur de l'Union européenne?

En particulier,

La directive 2006/24 est-elle compatible avec le droit des citoyens à circuler et à résider librement sur le territoire des États membres, consacré à l'article 21 TFUE?

La directive 2006/24 est-elle compatible avec le droit au respect de la vie privée consacré par l'article 7 de la [charte des droits fondamentaux de l'Union européenne (ci-après la «Charte»)] et par l'article 8 de la [CEDH]?

La directive 2006/24 est-elle compatible avec le droit à la protection des données à caractère personnel qui figure à l'article 8 de la Charte?

La directive 2006/24 est-elle compatible avec le droit à la liberté d'expression consacré par l'article 11 de la Charte et par l'article 10 de la [CEDH]?

La directive 2006/24 est-elle compatible avec le droit à une bonne administration consacré par l'article 41 de la Charte?

Dans quelle mesure les traités, et en particulier le principe de coopération loyale consacré à l'article 4, paragraphe 3, TUE, exigent-ils qu'une juridiction nationale examine et évalue la compatibilité des mesures nationales transposant la directive 2006/24 avec les garanties prévues par la [Charte], y compris son article 7 (tel que repris de l'article 8 de la [CEDH])?»

L'affaire C-594/12

À l'origine de la demande de décision préjudicielle dans l'affaire C-594/12 se trouvent plusieurs recours introduits devant le Verfassungsgerichtshof, formés respectivement par la Kärntner Landesregierung ainsi que par MM. Seitlinger, Tschohl et 11 128 autres requérants demandant l'annulation de l'article 102 bis de la loi de 2003 sur les télécommunications (Telekommunikationsgesetz 2003), qui a été introduit dans cette loi par la loi fédérale modifiant celle-ci (Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird, BGBl. I, 27/2011) aux fins de la transposition de la directive 2006/24 dans le droit interne autrichien. Ces parties considèrent, notamment, que cet article 102 bis viole le droit fondamental des particuliers à la protection de leurs données.

Le Verfassungsgerichtshof se demande, notamment, si la directive 2006/24 est compatible avec la Charte en ce qu'elle permet le stockage d'une masse de types de données à l'égard d'un nombre illimité de personnes pour une longue durée. La conservation des données toucherait presque exclusivement des personnes dont le comportement ne justifie aucunement la conservation des données les concernant. Ces personnes seraient exposées à un risque accru de voir les autorités rechercher leurs données, prendre connaissance de leur contenu, s'informer de leur vie privée et utiliser ces données à de multiples fins, compte tenu, notamment, du nombre incommensurable de personnes ayant accès aux données pendant une période de six mois au minimum. Selon la juridiction de renvoi, il existe des doutes, d'une part, quant au fait que cette directive serait en mesure d'atteindre les objectifs qu'elle poursuit et, d'autre part, quant au caractère proportionné de l'ingérence dans les droits fondamentaux concernés.

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

Sur la validité d'actes d'institutions de l'Union:

Les articles 3 à 9 de la directive 2006/24 sont-ils compatibles avec les articles 7, 8 et 11 de la [Charte]?

Sur l'interprétation des traités:

Au vu des explications sur l'article 8 de la Charte, lesquelles ont été élaborées, aux termes de l'article 52, paragraphe 7, de la Charte, en vue de guider l'interprétation de [celle-ci] et sont dûment prises en considération par le Verfassungsgerichtshof, la directive 95/46 et le règlement (CE) n° 45/2001 du Parlement européen et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données [(JO 2001, L 8, p. 1),] doivent-ils être considérés au même titre que les conditions fixées à l'article 8, paragraphe 2, et à l'article 52, paragraphe 1, de la Charte pour apprécier la licéité d'empiètements?

Dans quel rapport se trouvent le 'droit de l'Union' visé à l'article 52, paragraphe 3, dernière phrase, de la Charte et les directives en matière de droit à la protection des données?

Au vu des conditions et restrictions apportées par la directive 95/46 et le règlement [...] n° 45/2001 à la sauvegarde du droit fondamental à la protection des données inscrit dans la Charte, faut-il prendre en considération, dans l'interprétation de l'article 8 de [celle-ci], des changements découlant du droit dérivé

ultérieur?

Compte tenu de l'article 52, paragraphe 4, de la Charte, le principe de la prévalence du niveau supérieur de protection inscrit à l'article 53 de la Charte a-t-il pour conséquence que les limites assignées par [cette dernière] aux restrictions que peut valablement apporter le droit dérivé doivent être tracées plus étroitement?

Au regard de l'article 52, paragraphe 3, de la Charte, du cinquième alinéa du préambule et des explications sur l'article 7 de [celle-ci], indiquant que les droits garantis à l'article 7 correspondent à ceux qui sont garantis par l'article 8 de la CEDH, la jurisprudence que la Cour européenne des droits de l'homme a consacrée à l'article 8 de la CEDH peut-elle donner des indications dans l'interprétation de l'article 8 de la Charte qui rejaillissent sur l'interprétation de ce dernier article?»

Par décision du président de la Cour du 11 juin 2013, les affaires C-293/12 et C-594/12 ont été jointes aux fins de la procédure orale et de l'arrêt.

Sur les questions préjudicielles

Sur la deuxième question, sous b) à d), dans l'affaire C-293/12 et la première question dans l'affaire C-594/12

Par la deuxième question, sous b) à d), dans l'affaire C-293/12 et la première question dans l'affaire C-594/12, qu'il convient d'examiner ensemble, les juridictions de renvoi demandent en substance à la Cour d'examiner la validité de la directive 2006/24 à la lumière des articles 7, 8 et 11 de la Charte.

Sur la pertinence des articles 7, 8 et 11 de la Charte au regard de la question de la validité de la directive 2006/24

Il résulte de l'article 1er ainsi que des considérants 4, 5, 7 à 11, 21 et 22 de la directive 2006/24 que celle-ci a pour objectif principal d'harmoniser les dispositions des États membres relatives à la conservation, par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication, de certaines données générées ou traitées par ces fournisseurs en vue de garantir la disponibilité de ces données à des fins de prévention, de recherche, de détection et de poursuite des infractions graves, telles que celles liées à la criminalité organisée et au terrorisme, dans le respect des droits consacrés aux articles 7 et 8 de la Charte.

L'obligation des fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, prévue à l'article 3 de la directive 2006/24, de conserver les données énumérées à l'article 5 de celle-ci aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives à la protection tant de la vie privée que des communications consacrée à l'article 7 de la Charte à la protection des données à caractère personnel prévue à l'article 8 de celle-ci ainsi qu'au respect de la liberté d'expression garantie par l'article 11 de la Charte.

À cet égard, il convient de relever que les données que doivent conserver les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, au titre des articles 3 et 5 de la directive 2006/24, sont, notamment, les données nécessaires pour retrouver et identifier la source d'une communication et la destination de celle-ci, pour déterminer la date, l'heure, la durée et le type d'une communication, le matériel de communication des utilisateurs, ainsi que pour localiser le matériel de communication mobile, données au nombre desquelles 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, notamment, 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.

Ces données, prises dans leur ensemble, 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.

Dans de telles circonstances, même si la directive 2006/24 n'autorise pas, ainsi qu'il découle de ses articles 1er, paragraphe 2, et 5, paragraphe 2, la conservation du contenu de la communication et des informations consultées en utilisant un réseau de communications électroniques, il n'est pas exclu que la conservation des données en cause puisse avoir une incidence sur l'utilisation, par les abonnés ou les utilisateurs inscrits, des moyens de communication visés par cette directive et, en conséquence, sur l'exercice par ces derniers de leur liberté d'expression, garantie par l'article 11 de la Charte.

La conservation des données aux fins de leur accès éventuel par les autorités nationales compétentes, telle que prévue par la directive 2006/24, concerne de manière directe et spécifique la vie privée et, ainsi, les droits garantis par l'article 7 de la Charte. En outre, une telle conservation des données relève également de l'article 8 de celle-ci en raison du fait qu'elle constitue un traitement des données à caractère personnel au sens de cet article et doit, ainsi, nécessairement satisfaire aux exigences de protection des données découlant de cet article (arrêt Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 47).

Si les renvois préjudiciels dans les présentes affaires soulèvent notamment la question de principe de savoir si

les données des abonnés et des utilisateurs inscrits peuvent ou non, au regard de l'article 7 de la Charte, être conservées, ils concernent également celle de savoir si la directive 2006/24 répond aux exigences de protection des données à caractère personnel découlant de l'article 8 de la Charte.

Eu égard aux considérations qui précèdent, il convient, aux fins de répondre à la deuxième question, sous b) à d), dans l'affaire C-293/12 et à la première question dans l'affaire C-594/12, d'examiner la validité de la directive au regard des articles 7 et 8 de la Charte.

Sur l'existence d'une ingérence dans les droits consacrés par les articles 7 et 8 de la Charte

En imposant la conservation des données énumérées à l'article 5, paragraphe 1, de la directive 2006/24 et en permettant l'accès des autorités nationales compétentes à celles-ci, cette directive déroge, ainsi que l'a relevé M. l'avocat général notamment aux points 39 et 40 de ses conclusions, au régime de protection du droit au respect de la vie privée, instauré par les directives 95/46 et 2002/58, à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques, ces dernières directives ayant prévu la confidentialité des communications et des données relatives au trafic ainsi que l'obligation d'effacer ou de rendre anonymes ces données lorsqu'elles ne sont plus nécessaires à la transmission d'une communication, hormis si elles sont nécessaires à la facturation et uniquement tant que cette nécessité perdure.

Pour établir l'existence d'une ingérence dans le droit fondamental au respect de la vie privée, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence (voir, en ce sens, arrêt Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 75).

Il en résulte que l'obligation imposée par les articles 3 et 6 de la directive 2006/24 aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communication de conserver pendant une certaine durée des données relatives à la vie privée d'une personne et à ses communications, telles que celles visées à l'article 5 de cette directive, constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte.

En outre, l'accès des autorités nationales compétentes aux données constitue une ingérence supplémentaire dans ce droit fondamental (voir, en ce qui concerne l'article 8 de la CEDH, arrêts Cour EDH, Leander c. Suède, 26 mars 1987, série A n°116, § 48; Rotaru c. Roumanie [GC], n° 28341/95, § 46, CEDH 2000-V, ainsi que Weber et Saravia c. Allemagne (déc.), n° 54934/00, § 79, CEDH 2006-XI). Ainsi, les articles 4 et 8 de la directive 2006/24 prévoyant des règles relatives à l'accès des autorités nationales compétentes aux données sont également constitutifs d'une ingérence dans les droits garantis par l'article 7 de la Charte.

De même, la directive 2006/24 est constitutive d'une ingérence dans le droit fondamental à la protection des données à caractère personnel garanti par l'article 8 de la Charte puisqu'elle prévoit un traitement des données à caractère personnel.

Force est de constater que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère, ainsi que l'a également relevé M. l'avocat général notamment aux points 77 et 80 de ses conclusions, d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave. En outre, la circonstance que la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soient informés est susceptible de générer dans l'esprit des personnes concernées, ainsi que l'a relevé M. l'avocat général aux points 52 et 72 de ses conclusions, le sentiment que leur vie privée fait l'objet d'une surveillance constante.

Sur la justification de l'ingérence dans les droits garantis par les articles 7 et 8 de la Charte

Conformément à l'article 52, paragraphe 1, de la Charte, toute limitation de l'exercice des droits et des libertés consacrés par celle-ci doit être prévue par la loi, respecter leur contenu essentiel et, dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées à ces droits et 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 libertés d'autrui.

En ce qui concerne le contenu essentiel du droit fondamental au respect de la vie privée et des autres droits consacrés à l'article 7 de la Charte, il convient de constater que, même si la conservation des données imposée par la directive 2006/24 constitue une ingérence particulièrement grave dans ces droits, elle n'est pas de nature à porter atteinte audit contenu étant donné que, ainsi qu'il découle de son article 1er, paragraphe 2, cette directive ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel.

Cette conservation des données n'est pas non plus de nature à porter atteinte au contenu essentiel du droit fondamental à la protection des données à caractère personnel, consacré à l'article 8 de la Charte, en raison du fait que la directive 2006/24 prévoit, à son article 7, une règle relative à la protection et à la sécurité des données selon laquelle, sans préjudice des dispositions adoptées en application des directives 95/46 et 2002/58, certains principes de protection et de sécurité des données doivent être respectés par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, principes selon lesquels les États membres veillent à l'adoption de mesures techniques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données.

Quant à la question de savoir si ladite ingérence répond à un objectif d'intérêt général, il convient de relever

que, si la directive 2006/24 est destinée à harmoniser les dispositions des États membres relatives aux obligations desdits fournisseurs en matière de conservation de certaines données qui sont générées ou traitées par ces derniers, l'objectif matériel de cette directive vise, ainsi qu'il découle de son article 1er, paragraphe 1, à garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne. L'objectif matériel de cette directive est, dès lors, de contribuer à la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique.

Il ressort de la jurisprudence de la Cour que constitue un objectif d'intérêt général de l'Union la lutte contre le terrorisme international en vue du maintien de la paix et de la sécurité internationales (voir, en ce sens, arrêts Kadi et Al Barakaat International Foundation/Conseil et Commission, C-402/05 P et C-415/05 P, EU:C:2008:461, point 363, ainsi que Al-Aqsa/Conseil, C-539/10 P et C-550/10 P, EU:C:2012:711, point 130). Il en va de même de la lutte contre la criminalité grave afin de garantir la sécurité publique (voir, en ce sens, arrêt Tsakouridis, C-145/09, EU:C:2010:708, points 46 et 47). Par ailleurs, il convient de relever, à cet égard, que l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté.

À cet égard, il ressort du considérant 7 de la directive 2006/24 que, en raison de l'accroissement important des possibilités offertes par les communications électroniques, le Conseil «Justice et affaires intérieures» du 19 décembre 2002 a considéré que les données relatives à l'utilisation de celles-ci sont particulièrement importantes et constituent donc un instrument utile dans la prévention des infractions et la lutte contre la criminalité, notamment la criminalité organisée.

Force est donc de constater que la conservation des données aux fins de permettre aux autorités nationales compétentes de disposer d'un accès éventuel à celles-ci, telle qu'imposée par la directive 2006/24, répond effectivement à un objectif d'intérêt général.

Dans ces conditions, il y a lieu de vérifier la proportionnalité de l'ingérence constatée.

À cet égard, il convient de rappeler que le principe de proportionnalité exige, selon une jurisprudence constante de la Cour, que les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs (voir, en ce sens, arrêts Afton Chemical, C-343/09, EU:C:2010:419, point 45; Volker und Markus Schecke et Eifert, EU:C:2010:662, point 74; Nelson e.a., C-581/10 et C-629/10, EU:C:2012:657, point 71; Sky Österreich, C-283/11, EU:C:2013:28, point 50, ainsi que Schaible, C-101/12, EU:C:2013:661, point 29).

En ce qui concerne le contrôle juridictionnel du respect de ces conditions, dès lors que des ingérences dans des droits fondamentaux sont en cause, l'étendue du pouvoir d'appréciation du législateur de l'Union peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels figurent, notamment, le domaine concerné, la nature du droit en cause garanti par la Charte, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, arrêt Cour EDH, S et Marper c. Royaume-Uni [GC], nos 30562/04 et 30566/04, § 102, CEDH 2008-V).

En l'espèce, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict.

En ce qui concerne la question de savoir si la conservation des données est apte à réaliser l'objectif poursuivi par la directive 2006/24, il convient de constater que, eu égard à l'importance croissante des moyens de communication électronique, les données qui doivent être conservées en application de cette directive permettent aux autorités nationales compétentes en matière de poursuites pénales de disposer de possibilités supplémentaires d'élucidation des infractions graves et, à cet égard, elles constituent donc un instrument utile pour les enquêtes pénales. Ainsi, la conservation de telles données peut être considérée comme apte à réaliser l'objectif poursuivi par ladite directive.

Cette appréciation ne saurait être remise en cause par la circonstance, invoquée notamment par MM. Tschohl et Seitlinger ainsi que par le gouvernement portugais dans leurs observations écrites soumises à la Cour, qu'il existe plusieurs modalités de communications électroniques qui ne relèvent pas du champ d'application de la directive 2006/24 ou qui permettent une communication anonyme. Si, certes, cette circonstance est de nature à limiter l'aptitude de la mesure de conservation des données à atteindre l'objectif poursuivi, elle n'est toutefois pas de nature à rendre cette mesure inapte, ainsi que l'a relevé M. l'avocat général au point 137 de ses conclusions.

En ce qui concerne le caractère nécessaire de la conservation des données imposée par la directive 2006/24, il convient de constater que, certes, la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête. Toutefois, un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte.

S’agissant du droit au respect de la vie privée, la protection de ce droit fondamental exige, selon la jurisprudence constante de la Cour, en tout état de cause, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s’opérer dans les limites du strict nécessaire (arrêt IPI, C-473/12, EU:C:2013:715, point 39 et jurisprudence citée).

À cet égard, il convient de rappeler que la protection des données à caractère personnel, résultant de l’obligation explicite prévue à l’article 8, paragraphe 1, de la Charte, revêt une importance particulière pour le droit au respect de la vie privée consacré à l’article 7 de celle-ci.

Ainsi, la réglementation de l’Union en cause doit prévoir des règles claires et précises régissant la portée et l’application de la mesure en cause et imposant un minimum d’exigences de 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 ainsi que contre tout accès et toute utilisation illicites de ces données (voir, par analogie, en ce qui concerne l’article 8 de la CEDH, arrêts Cour EDH, Liberty et autres c. Royaume-Uni, n° 58243/00, § 62 et 63, du 1er juillet 2008; Rotaru c. Roumanie, précité, § 57 à 59, ainsi que S et Marper c. Royaume-Uni, précité, § 99).

La nécessité de disposer de telles garanties est d’autant plus importante lorsque, comme le prévoit la directive 2006/24, les données à caractère personnel sont soumises à un traitement automatique et qu’il existe un risque important d’accès illicite à ces données (voir, par analogie, en ce qui concerne l’article 8 de la CEDH, arrêts Cour EDH, S et Marper c. Royaume-Uni, précité, § 103, ainsi que M. K. c. France, n° 19522/09, § 35, du 18 avril 2013).

Quant à la question de savoir si l’ingérence que comporte la directive 2006/24 est limitée au strict nécessaire, il convient de relever que cette directive impose, conformément à son article 3 lu en combinaison avec son article 5, paragraphe 1, la conservation de toutes les données relatives au trafic concernant la téléphonie fixe, la téléphonie mobile, l’accès à l’internet, le courrier électronique par Internet ainsi que la téléphonie par l’internet. Ainsi, elle vise tous les moyens de communication électronique dont l’utilisation est très répandue et d’une importance croissante dans la vie quotidienne de chacun. En outre, conformément à son article 3, ladite directive couvre tous les abonnés et utilisateurs inscrits. Elle comporte donc une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne.

À cet égard, il importe de constater, en premier lieu, que la directive 2006/24 couvre de manière généralisée toute personne et tous les moyens de communication électronique ainsi que l’ensemble des données relatives au trafic sans qu’aucune différenciation, limitation ni exception soient opérées en fonction de l’objectif de lutte contre les infractions graves.

En effet, d’une part, la directive 2006/24 concerne de manière globale l’ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées 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 graves. En outre, elle ne prévoit aucune exception, de sorte qu’elle s’applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel.

D’autre part, tout en visant à contribuer à la lutte contre la criminalité grave, ladite directive ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique et, notamment, elle n’est pas limitée à une conservation portant soit sur des données afférentes à une période temporelle et/ou une zone géographique déterminée et/ou sur un cercle de personnes données 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 prévention, à la détection ou à la poursuite d’infractions graves.

En deuxième lieu, à cette absence générale de limites s’ajoute le fait que la directive 2006/24 ne prévoit aucun critère objectif permettant de délimiter l’accès des autorités nationales compétentes aux données et leur utilisation ultérieure à des fins de prévention, de détection ou de poursuites pénales concernant des infractions pouvant, au regard de l’ampleur et de la gravité de l’ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, être considérées comme suffisamment graves pour justifier une telle ingérence. Au contraire, la directive 2006/24 se borne à renvoyer, à son article 1er, paragraphe 1, de manière générale aux infractions graves telles qu’elles sont définies par chaque État membre dans son droit interne.

En outre, quant à l’accès des autorités nationales compétentes aux données et à leur utilisation ultérieure, la directive 2006/24 ne contient pas les conditions matérielles et procédurales y afférentes. L’article 4 de cette directive, qui régit l’accès de ces autorités aux données conservées, ne dispose pas expressément que cet accès et l’utilisation ultérieure des données en cause doivent être strictement restreints à des fins de prévention et de détection d’infractions graves précisément délimitées ou de poursuites pénales afférentes à celles-ci, mais il se borne à prévoir que chaque État membre arrête la procédure à suivre et les conditions à remplir pour avoir accès aux données conservées dans le respect des exigences de nécessité et de proportionnalité.

En particulier, la directive 2006/24 ne prévoit aucun critère objectif permettant de limiter le nombre de

personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données conservées au strict nécessaire au regard de l'objectif poursuivi. Surtout, l'accès aux données conservées par les autorités nationales compétentes n'est pas subordonné à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante dont la décision vise à limiter l'accès aux données et leur utilisation à ce qui est strictement nécessaire aux fins d'atteindre l'objectif poursuivi et intervient à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales. Il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles limitations.

En troisième lieu, s'agissant de la durée de conservation des données, la directive 2006/24 impose, à son article 6, la conservation de celles-ci pendant une période d'au moins six mois sans que soit opérée une quelconque distinction entre les catégories de données prévues à l'article 5 de cette directive en fonction de leur utilité éventuelle aux fins de l'objectif poursuivi ou selon les personnes concernées.

Cette durée se situe, en outre, entre six mois au minimum et vingt-quatre mois au maximum, sans qu'il soit précisé que la détermination de la durée de conservation doit être fondée sur des critères objectifs afin de garantir que celle-ci est limitée au strict nécessaire.

Il résulte de ce qui précède que la directive 2006/24 ne prévoit pas de règles claires et précises régissant la portée de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Force est donc de constater que cette directive comporte une ingérence dans ces droits fondamentaux d'une vaste ampleur et d'une gravité particulière dans l'ordre juridique de l'Union sans qu'une telle ingérence soit précisément encadrée par des dispositions permettant de garantir qu'elle est effectivement limitée au strict nécessaire.

De surcroît, en ce qui concerne les règles visant la sécurité et la protection des données conservées par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, il convient de constater que la directive 2006/24 ne prévoit pas des garanties suffisantes, telles que requises par l'article 8 de la Charte, permettant d'assurer une protection efficace des données conservées contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données. En effet, en premier lieu, l'article 7 de la directive 2006/24 ne prévoit pas de règles spécifiques et adaptées à la vaste quantité des données dont la conservation est imposée par cette directive, au caractère sensible de ces données ainsi qu'au risque d'accès illicite à celles-ci, règles qui seraient destinées notamment à régir de manière claire et stricte la protection et la sécurité des données en cause, afin de garantir leur pleine intégrité et confidentialité. En outre, il n'a pas non plus été prévu une obligation précise des États membres visant à établir de telles règles.

L'article 7 de la directive 2006/24, lu en combinaison avec les articles 4, paragraphe 1, de la directive 2002/58 et 17, paragraphe 1, second alinéa, de la directive 95/46, ne garantit pas que soit appliqué par lesdits fournisseurs un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles, mais autorise notamment ces fournisseurs à tenir compte de considérations économiques lors de la détermination du niveau de sécurité qu'ils appliquent, en ce qui concerne les coûts de mise en œuvre des mesures de sécurité. En particulier, la directive 2006/24 ne garantit pas la destruction irrémédiable des données au terme de la durée de conservation de celles-ci.

En second lieu, il convient d'ajouter que ladite directive n'impose pas que les données en cause soient conservées sur le territoire de l'Union, de sorte qu'il ne saurait être considéré qu'est pleinement garanti le contrôle par une autorité indépendante, explicitement exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité, telles que visées aux deux points précédents. Or, un tel contrôle, effectué sur la base du droit de l'Union, constitue un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel (voir, en ce sens, arrêt Commission/Autriche, C-614/10, EU:C:2012:631, point 37).

Eu égard à l'ensemble des considérations qui précèdent, il convient de considérer que, en adoptant la directive 2006/24, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité au regard des articles 7, 8 et 52, paragraphe 1, de la Charte.

Dans ces conditions, il n'y a pas lieu d'examiner la validité de la directive 2006/24 au regard de l'article 11 de la Charte.

En conséquence, il y a lieu de répondre à la deuxième question, sous b) à d), dans l'affaire C-293/12 et à la première question dans l'affaire C-594/12 que la directive 2006/24 est invalide.

Sur la première question et la deuxième question, sous a) et e), ainsi que sur la troisième question dans l'affaire C-293/12 et sur la seconde question dans l'affaire C-594/12

Il résulte de ce qui a été jugé au point précédent qu'il n'y a pas lieu de répondre à la première question, à la deuxième question, sous a) et e), et à la troisième question dans l'affaire C-293/12 non plus qu'à la deuxième question dans l'affaire C-594/12.

Sur les dépens

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:

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, est invalide.

Signatures

---

* Langues de procédure: l'anglais et l'allemand.