Recueil de la jurisprudence

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. HENRIK SAUGMANDSGAARD ØE
présentées le 19 juillet 2016[1]

Affaires jointes C-203/15 et C-698/15

Tele2 Sverige AB
contre
Post- och telestyrelsen (C-203/15)
et
Secretary of State for the Home Department
contre
Tom Watson,
Peter Brice,
Geoffrey Lewis (C-698/15)
en présence de
Open Rights Group,
Privacy International,
Law Society of England and Wales

[demandes de décision préjudicielle formées par le Kammarrätten i Stockholm (cour administrative d'appel de Stockholm, Suède) et la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile), Royaume-Uni]

«Renvoi préjudiciel — Directive 2002/58/CE — Traitement des données à caractère personnel et protection de la vie privée dans le secteur des communications électroniques — Législation nationale prévoyant une obligation générale de conserver les données relatives aux communications électroniques — Article 15, paragraphe 1 — charte des droits fondamentaux de l'Union européenne — Article 7 — Droit au respect de la vie privée — Article 8 — Droit à la protection des données à caractère personnel — Ingérence grave — Justification — Article 52, paragraphe 1 — Conditions — Objectif légitime de lutte contre les infractions graves — Exigence d'une base légale en droit national — Exigence de stricte nécessité — Exigence de proportionnalité dans une société démocratique»

Table des matières

I – Introduction 3

II – Le cadre juridique 5

1 — Langue originale : le français.

A – La directive 2002/58 5

B – Le droit suédois 5

1. Sur la portée de l'obligation de conservation 6

2. Sur l'accès aux données conservées 6

a) La LEK 6

b) Le RB 6

c) La loi 2012:278 7

3. Sur la durée de conservation des données 8

4. Sur la protection et la sécurité des données conservées 8

C – Le droit du Royaume-Uni 8

1. Sur la portée de l'obligation de conservation 9

2. Sur l'accès aux données conservées 9

3. Sur la durée de conservation des données 10

4. Sur la protection et la sécurité des données conservées 10

III – Les litiges au principal et les questions préjudicielles 11

A – L'affaire C-203/15 11

B – L'affaire C-698/15 12

IV – La procédure devant la Cour 13

V – Analyse des questions préjudicielles 13

A – Sur la recevabilité de la seconde question posée dans l'affaire C-698/15 14

B – Sur la compatibilité d'une obligation générale de conservation de données avec le régime établi par la directive 2002/58 16

1. Sur l'inclusion d'une obligation générale de conservation de données dans le champ d'application de la directive 2002/58 16

2. Sur la possibilité de déroger au régime établi par la directive 2002/58 en établissant une obligation générale de conservation de données 17

C – Sur l'applicabilité de la Charte à une obligation générale de conservation de données 20

D – Sur la compatibilité d'une obligation générale de conservation de données avec les exigences établies par l'article 15, paragraphe 1, de la directive 2002/58 ainsi que par les articles 7, 8 et 52, paragraphe 1, de la Charte 21

1. Sur l'exigence d'une base légale en droit national 22

2. Sur le respect du contenu essentiel des droits reconnus par les articles 7 et 8 de la Charte . 25

3. Sur l'existence d'un objectif d'intérêt général reconnu par l'Union susceptible de justifier une obligation générale de conservation de données 26

4. Sur le caractère approprié d'une obligation générale de conservation de données au regard de la lutte contre les infractions graves 28

5. Sur le caractère nécessaire d'une obligation générale de conservation de données au regard de la lutte contre les infractions graves 29

a) Sur le caractère strictement nécessaire d'une obligation générale de conservation de données 31

b) Sur le caractère impératif des garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI au regard de l'exigence de stricte nécessité 34

6. Sur le caractère proportionné, dans une société démocratique, d'une obligation générale de conservation de données au regard de l'objectif de lutte contre les infractions graves 38

VI – Conclusion 42

I – Introduction

1. En 1788, James Madison, l'un des auteurs de la Constitution des États-Unis, écrivait : « If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this : you must first enable the government to control the governed ; and in the next place oblige it to control itself» [2].

2. Les présentes affaires nous placent au cœur de la « grande difficulté » identifiée par Madison. Elles portent sur la compatibilité avec le droit de l'Union de régimes nationaux établissant, à charge des fournisseurs de services de communications électroniques accessibles au public (ci-après les « fournisseurs »), une obligation de conservation des données relatives aux communications électroniques (ci-après les « données relatives aux communications »), portant sur l'ensemble des moyens de communication et l'ensemble des utilisateurs (ci-après l'« obligation générale de conservation de données »).

2 — « Si les hommes étaient des anges, aucun gouvernement ne serait nécessaire. Si les anges gouvernaient les hommes, aucun contrôle externe ou interne sur le gouvernement ne serait nécessaire. Dans la délimitation d'un gouvernement des hommes sur les hommes, la grande difficulté est la suivante : il faut d'abord permettre au gouvernement de contrôler les gouvernés ; et il faut ensuite l'obliger à se contrôler lui-même » : Madison, J., « Federalist No. 51 », in Hamilton, A., Madison, J. et Jay, J., ed. Genovese, M. A., *The Federalist Papers,* Palsgrave Macmillan, New York, 2009, p. 120 (traduction libre). Madison fut l'un des principaux auteurs et l'un des 39 signataires de la Constitution des États-Unis (1787). Il devint ensuite le quatrième président des États-Unis (de 1809 à 1817).

3. D'une part, la conservation des données relatives aux communications permet « au gouvernement de contrôler les gouvernés » en offrant aux autorités compétentes un moyen d'investigation pouvant revêtir une utilité certaine dans la lutte contre les infractions graves, et notamment dans la lutte contre le terrorisme. En substance, la conservation de ces données octroie aux autorités une capacité limitée de « lire le passé », en accédant aux données relatives aux communications qu'une personne a effectuées avant même d'être suspectée d'avoir un lien avec une infraction grave [3].

4. Toutefois, et d'autre part, il est impératif d'« obliger le gouvernement à se contrôler lui-même » en ce qui concerne tant la conservation que l'accès aux données conservées, eu égard aux graves risques qu'engendre l'existence de telles bases de données couvrant la totalité des communications réalisées sur le territoire national. En effet, ces bases de données d'une ampleur considérable offrent à toute personne y ayant accès le pouvoir de cataloguer instantanément l'ensemble de la population pertinente [4]. Ces risques doivent être scrupuleusement appréhendés au travers notamment de l'examen des caractères strictement nécessaire et proportionné d'une obligation générale de conservation de données, telle que celles en cause dans les litiges au principal.

5. Ainsi, dans le cadre des présentes affaires, la Cour et les juridictions de renvoi sont appelées à définir un point d'équilibre entre l'obligation incombant aux États membres d'assurer la sécurité des individus se trouvant sur leur territoire et le respect des droits fondamentaux à la vie privée et à la protection des données à caractère personnel consacrés aux articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte »).

6. C'est à la lumière de cette « grande difficulté » que j'examinerai les questions posées à la Cour dans les présentes affaires. Celles-ci concernent, plus spécifiquement, la compatibilité de régimes nationaux établissant une obligation générale de conservation de données avec la directive 2002/58/CE [5] ainsi qu'avec les articles 7 et 8 de la Charte. En vue de répondre à ces questions, la Cour devra notamment préciser l'interprétation qu'il convient d'apporter dans un contexte national à l'arrêt Digital Rights Ireland e.a. (ci-après « l'arrêt DRI ») [6], dans lequel la grande chambre de la Cour a invalidé la directive 2006/24/CE [7].

7. Pour les motifs que j'exposerai ci-après, j'ai le sentiment qu'une obligation générale de conservation de données imposée par un État membre peut être compatible avec les droits fondamentaux consacrés par le droit de l'Union à condition d'être strictement encadrée par une série de garanties que j'identifierai au cours de mon exposé.

3 — Cette capacité limitée de « lire le passé » peut notamment s'avérer d'une grande utilité aux fins de l'identification d'éventuels complices : voir points 178 à 184 des présentes conclusions.

4 — Voir points 252 à 261 des présentes conclusions.

5 — Directive 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).

6 — Arrêt du 8 avril 2014 (C-293/12 et C-594/12, EU:C:2014:238).

7 — Directive 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).

II – Le cadre juridique

A – *La directive 2002/58*

8. 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 [l'Union européenne].

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 [TFUE], telles que celles visées dans les titres V et VI du [TUE], 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. »

9. L'article 15, paragraphe 1, de la directive 2002/58, intitulé « Application de certaines dispositions de la directive [95/46] », est libellé comme suit :

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

B – *Le droit suédois*

10. La directive 2006/24, aujourd'hui invalidée, a été transposée en droit suédois par des modifications apportées à la lagen (2003:389) om elektronisk kommunikation (loi suédoise 2003:389 sur les communications électroniques, ci-après la « LEK ») et au förordningen (2003:396) om elektronisk kommunikation (règlement 2003:396 sur les communications électroniques, ci-après le « FEK »), textes entrés en vigueur le 1er mai 2012.

1. Sur la portée de l'obligation de conservation

11. Il ressort des dispositions de l'article 16 a du chapitre 6 de la LEK que les fournisseurs sont tenus de conserver les données relatives aux communications nécessaires pour 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 au terme de la communication. Les types de données devant être conservées font l'objet de dispositions plus détaillées aux articles 38 à 43 du FEK.

12. Cette obligation de conservation concerne les données 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.

13. Les données à conserver incluent non seulement toutes celles qui devaient être conservées dans le cadre de la directive 2006/24, mais également celles relatives à des communications infructueuses ainsi que celles relatives à la localisation au terme d'une communication par téléphonie mobile. À l'image du régime qui était prévu par cette directive, les données à conserver n'incluent pas le contenu des communications.

2. Sur l'accès aux données conservées

14. L'accès aux données conservées est encadré par trois textes, à savoir la LEK, le rättegångsbalken (code de procédure judiciaire, ci-après le « RB ») et la lagen (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet (loi suédoise 2012:278 sur la communication de données relatives à des communications électroniques dans le cadre des activités de renseignement des autorités répressives).

a) La LEK

15. Suivant les dispositions de l'article 22, premier alinéa, 2°, du chapitre 6 de la LEK, tout fournisseur doit communiquer les données relatives à un abonnement sur réquisition du parquet, de la police, de la Säkerhetspolisen (sûreté suédoise, ci-après la « Säpo ») ou de toute autre autorité publique répressive, si lesdites données se rapportent à une infraction présumée. Suivant ces dispositions, il n'est pas nécessaire qu'il s'agisse d'une infraction grave.

16. Par données relatives à un abonnement, il faut en substance comprendre les données relatives au nom, au titre, à l'adresse postale, au numéro et à l'adresse IP de l'abonné.

17. En vertu de la LEK, la communication de données relatives à un abonnement n'est pas subordonnée à un contrôle préalable, mais peut faire l'objet d'un contrôle administratif postérieur. Par ailleurs, le nombre d'autorités susceptibles d'avoir accès aux données n'est pas limité.

b) Le RB

18. Le RB réglemente la mise sous surveillance de communications électroniques dans le cadre d'enquêtes préliminaires.

19. En substance, la mise sous surveillance de communications électroniques ne peut être ordonnée que lorsqu'une personne déterminée est raisonnablement soupçonnée d'être l'auteur d'une infraction sanctionnée par une peine d'emprisonnement d'au moins six mois ou d'autres infractions spécifiquement énumérées, si cette mesure est particulièrement nécessaire pour les besoins de l'enquête.

20. Outre ces cas de figure, il peut être procédé à une telle mise sous surveillance aux fins d'enquêter sur une infraction sanctionnée par une peine d'emprisonnement d'au moins deux ans en vue de déterminer qui pourrait être raisonnablement soupçonné d'en être l'auteur, si cette mesure est particulièrement nécessaire pour les besoins de l'enquête.

21. En application de l'article 21 du chapitre 27 du RB, le parquet doit normalement obtenir l'autorisation du juge compétent avant de procéder à la mise sous surveillance de communications électroniques.

22. Néanmoins, si le fait de saisir le juge compétent avant de procéder à la mise sous surveillance de communications électroniques, mesure d'une impérieuse nécessité pour les besoins de l'enquête, paraît incompatible avec l'urgence de sa mise en œuvre ou créerait des obstacles, l'autorisation est accordée par le parquet dans l'attente de la décision du juge compétent. Ce dernier doit immédiatement en être informé par écrit par le parquet. Le juge compétent doit alors faire diligence pour examiner si la mesure est justifiée.

c) La loi 2012:278

23. Dans le cadre de la recherche de renseignements et en application de l'article 1er de la loi 2012:278, la police nationale, la Säpo et la Tullverket (administration suédoise des douanes) peuvent, dans les conditions prescrites par cette loi et à l'insu du fournisseur, procéder à la collecte de données relatives aux communications.

24. Suivant les articles 2 et 3 de la loi 2012:278, les données peuvent 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 (comprenant notamment différentes formes de sabotage et d'espionnage).

25. La décision de procéder à une telle mesure relève du directeur de l'autorité concernée ou d'une personne déléguée à cet effet.

26. La décision doit indiquer l'activité criminelle, la période concernée ainsi que le numéro de téléphone, toute autre adresse, l'équipement de communication électronique ou la zone géographique visés. La durée de l'autorisation ne doit pas se prolonger au-delà du nécessaire et, s'agissant de la période courant après la date de la décision d'autorisation, celle-ci ne doit pas excéder une durée d'un mois.

27. Ce type de mesure n'est pas soumis à un contrôle préalable. Toutefois, en application 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 d'autorisation de procéder à la collecte de données. En application de l'article 1er de la lagen (2007:980) om tillsyn över viss brottsbekämpande verksamhet (loi 2007:980 relative au contrôle de certaines activités répressives), cet organisme doit exercer une surveillance sur l'application de la loi par les autorités répressives.

3. Sur la durée de conservation des données

28. Il ressort des dispositions de l'article 16 d du chapitre 6 de la LEK que les données visées à l'article 16 a du même chapitre doivent être conservées pendant six mois à compter du jour de l'achèvement de la communication. Elles doivent ensuite être immédiatement effacées, sauf dispositions contraires de l'article 16 d, deuxième alinéa, (du chapitre 6) de la LEK. En application de ces dernières dispositions, les données dont la communication a été demandée avant l'expiration du délai de conservation mais qui n'ont pas encore été communiquées doivent être effacées dès cette communication.

4. Sur la protection et la sécurité des données conservées

29. L'article 20, premier alinéa, du chapitre 6 de la LEK interdit à quiconque de diffuser ou d'utiliser de manière non autorisée des données relatives aux communications.

30. Suivant les dispositions de l'article 3 a du chapitre 6 de la LEK, les fournisseurs doivent prendre les mesures d'ordre technique et organisationnel appropriées pour assurer la protection des données lors du traitement. Il ressort des travaux préparatoires relatifs à ces dispositions qu'il n'est pas permis de déterminer le niveau de protection sur la base d'un arbitrage entre les considérations d'ordre technique, des coûts et des risques de piratage et d'intrusion.

31. D'autres prescriptions sur la protection des données figurent à l'article 37 du FEK ainsi que dans les instructions et les lignes directrices de la Post- och telestyrelsen (autorité suédoise de surveillance des postes et télécommunications, ci-après la « PTS ») sur les mesures de protection dans le cadre de la conservation et du traitement de données aux fins de la lutte contre la criminalité (PTSFS nº 2012:4). De ces textes, il ressort notamment que les fournisseurs doivent prendre des mesures de protection des données contre la destruction non intentionnelle ou non autorisée, contre la conservation, le traitement et l'accès non autorisés, ainsi que contre la divulgation non autorisée. Le fournisseur doit également veiller en permanence et systématiquement à la sécurité des données en tenant compte des risques spéciaux engendrés par l'obligation de conservation.

32. Le droit suédois ne renferme aucune disposition concernant le lieu où les données doivent être conservées.

33. En application du chapitre 7 de la LEK, l'autorité de surveillance a le pouvoir, en cas de manquement par un fournisseur à ses obligations, d'adresser des mesures d'injonction et d'interdiction, éventuellement assorties d'astreintes, ainsi que d'ordonner une cessation totale ou partielle d'activité.

C – *Le droit du Royaume-Uni*

34. Les dispositions régissant la conservation des données figurent dans la Data Retention and Investigatory Powers Act 2014 (loi de 2014 sur la conservation des données et les pouvoirs d'enquête, ci-après la « DRIPA »), dans le Data Retention Regulations 2014 (SI 2014/2042) (règlement de 2014 relatif à la conservation des données, ci-après le « règlement de 2014 ») ainsi que dans le Retention of Communications Data Code of Practice (code des bonnes pratiques relatif à la conservation des données).

35. Les dispositions régissant l'accès aux données se trouvent dans le chapitre 2 de la partie 1 de la Regulation of Investigatory Powers Act 2000 (loi de 2000 portant réglementation des pouvoirs d'enquête, ci-après la « RIPA »), le Regulation of Investigatory Powers (Communication Data) Order 2010 (SI 2010/480) (ordonnance de 2015 portant réglementation des pouvoirs d'enquête en matière

de données relatives aux communications, telle que modifiée par le Regulation of Investigatory Powers (Communications Data) (Amendement) Order 2015 (SI 2015/228) ainsi que le Acquisition and Disclosure of Communications Data Code of Practice (code des bonnes pratiques relatif à l'obtention et à la divulgation des données relatives aux communications, ci-après le « code relatif à l'obtention des données »).

1. Sur la portée de l'obligation de conservation

36. En vertu de la section 1 de la DRIPA, le Secretary of State for the Home Department (Ministre de l'Intérieur, Royaume-Uni, ci-après le « Ministre ») peut imposer aux fournisseurs une obligation de conserver toutes les données relatives aux communications. En substance, cette obligation est susceptible de concerner l'ensemble des données générées à l'occasion d'une communication acheminée par un service postal ou un système de télécommunication, à l'exception du contenu de la communication. Ces données incluent notamment le lieu où se trouve l'utilisateur du service ainsi que les données permettant de déterminer l'adresse IP (protocole Internet) ou tout autre identifiant appartenant à l'expéditeur ou au destinataire d'une communication.

37. Les objectifs pouvant justifier l'adoption d'une telle mesure de conservation incluent les intérêts de la sûreté nationale, la prévention ou la détection de la criminalité ou la prévention des troubles à l'ordre public, les intérêts du bien-être économique du Royaume-Uni pour autant que ces intérêts soient également pertinents pour les intérêts de la sûreté nationale, les intérêts de la sécurité publique, la protection de la santé publique, l'évaluation de l'assiette ou la collecte de toute taxe, de toute contribution ou de tout autre montant dû à l'administration publique, la prévention de préjudices pour la santé physique ou mentale dans les cas d'urgence, l'assistance dans les enquêtes sur les cas d'erreurs judiciaires, l'identification d'une personne qui est décédée ou qui n'est pas en mesure de s'identifier elle-même autrement qu'à la suite d'un crime ou délit (comme en cas de catastrophe naturelle ou d'accident), l'exercice de fonctions relatives à la réglementation des services et des marchés financiers ou de la stabilité financière ainsi que toute autre fin précisée dans une injonction établie par le Ministre en vertu de la section 22(2) de la DRIPA.

38. La législation nationale n'exige pas que l'adoption d'un acte ordonnant la conservation soit préalablement soumise à une autorisation judiciaire ou d'une entité indépendante. Le Ministre doit vérifier que l'obligation de conservation est « nécessaire et proportionnée » aux fins d'un ou de plusieurs objectifs pour lesquels les données pertinentes relatives aux communications peuvent être conservées.

2. Sur l'accès aux données conservées

39. En vertu de la section 22(4) de la RIPA, les autorités publiques peuvent, aux termes d'un acte, exiger des fournisseurs qu'ils leur divulguent des données relatives aux communications. La forme et le contenu de ces actes sont régis par la section 23(2) de la RIPA. Un tel acte est limité dans le temps par des dispositions relatives à son annulation et à son renouvellement.

40. L'obtention des données relatives aux communications doit être nécessaire et proportionnée à un ou à plusieurs des objectifs figurant à la section 22 de la RIPA, lesquels correspondent aux objectifs susceptibles de justifier la conservation des données décrits au point 37 des présentes conclusions.

41. Il ressort du code relatif à l'obtention des données que l'ordonnance d'une juridiction est requise dans le cas d'une demande d'accès effectuée en vue d'identifier la source de journalistes ainsi qu'en cas de demande d'accès formulée par des autorités locales.

42. En dehors de ces hypothèses, l'accès des autorités publiques est subordonné à l'obtention d'une autorisation accordée par les personnes désignées à cet effet au sein de l'autorité publique concernée. Une personne désignée à cet effet est une personne qui détient une fonction, un grade ou un poste établi au sein de l'autorité publique concernée et qui a été désignée aux fins de l'obtention des données relatives aux communications conformément à l'ordonnance de 2015 portant réglementation des pouvoirs d'enquête en matière de données relatives aux communications, telle que modifiée.

43. Aucune autorisation judiciaire ou d'une entité indépendante n'est spécifiquement exigée en ce qui concerne l'accès à des données relatives aux communications protégées par un secret professionnel légal ou à des données relatives aux communications se rapportant à des docteurs en médecine, à des membres du Parlement ou à des ministres des cultes. Le code relatif à l'obtention des données précise seulement qu'une attention particulière doit être accordée quant à la nécessité et à la proportionnalité d'une demande d'accès à de telles données.

3. Sur la durée de conservation des données

44. La section 1(5) de la DRIPA et la disposition 4(2) du règlement de 2014 prévoient une période maximale de conservation des données de douze mois. Selon le code des bonnes pratiques relatif à la conservation des données, la période doit seulement être aussi longue que nécessaire et proportionnée. La disposition 6 du règlement de 2014 exige du Ministre qu'il réexamine un acte ordonnant la conservation.

4. Sur la protection et la sécurité des données conservées

45. En application de la section 1 de la DRIPA, les fournisseurs ont l'interdiction de divulguer les données conservées à moins que cette divulgation ne soit conforme au chapitre 2 de la partie 1 de la RIPA, à une décision de justice ou à tous autres autorisation ou mandat judiciaire, ou encore à un règlement adopté par le Ministre en application de la section 1 de la DRIPA.

46. En vertu des dispositions 7 et 8 du règlement de 2014, les fournisseurs doivent assurer l'intégrité et la sécurité des données conservées ; les protéger d'une destruction accidentelle ou illicite, d'une perte ou d'une altération accidentelle, ou d'une conservation, d'un traitement, d'un accès ou d'une divulgation non autorisés ou illicites ; détruire les données de sorte qu'il soit impossible d'y accéder si la conservation des données cesse d'être autorisée ; et instaurer des systèmes de sécurité. La disposition 9 du règlement de 2014 confie à l'Information Commissioner (commissaire chargé de l'information) le devoir de vérifier le respect de ces obligations par les fournisseurs.

47. Les autorités auxquelles les fournisseurs communiquent des données relatives aux communications doivent traiter et conserver ces données, ainsi que toute copie, tout extrait ou tout résumé de celles-ci, de manière sûre. En application du code relatif à l'obtention des données, les exigences figurant dans la loi relative à la protection des données (Data Protection Act, ci-après le « DPA »), qui a transposé la directive 95/46, doivent être respectées.

48. La RIPA institue un Interception of Communications Commissioner (commissaire chargé de l'interception des communications, ci-après le « commissaire chargé de l'interception ») qui est chargé de superviser de manière indépendante l'exercice et la mise en œuvre des pouvoirs et devoirs figurant au chapitre II de la partie I de la RIPA. Le commissaire chargé de l'interception ne supervise pas le recours à la section 1 de la DRIPA. Il doit fournir régulièrement des rapports destinés au public et au Parlement [section 57(2) et section 58 de la RIPA] et faire état de ce qui est conservé et rapporté par les autorités publiques (code relatif à l'obtention des données, paragraphes 6.1 à 6.8). Des plaintes peuvent également être déposées auprès de l'Investigatory Powers Tribunal (Tribunal chargé des pouvoirs d'enquête) s'il existe une raison de penser que des données ont été obtenues de manière inappropriée (section 65 de la RIPA).

49. Il ressort du code relatif à l'obtention des données que le commissaire chargé de l'interception n'a pas le pouvoir de renvoyer une affaire devant ce Tribunal. Il est simplement autorisé à informer une personne qu'un usage illicite de compétences est soupçonné s'il peut « établir qu'un individu a été lésé par un manquement intentionnel ou par imprudence ». Cependant, il n'est pas autorisé à procéder à une divulgation si la sécurité nationale est menacée par une telle divulgation, même s'il considère qu'il y a eu un manquement intentionnel ou par imprudence.

III – Les litiges au principal et les questions préjudicielles

A – *L'affaire C-203/15*

50. Le 9 avril 2014, soit le lendemain du prononcé de l'arrêt DRI, Tele2 Sverige a notifié à la PTS sa décision de cesser de procéder à la conservation des données visées par le chapitre 6 de la LEK. Tele2 Sverige allait également procéder à l'effacement des données conservées jusqu'alors en application de ce chapitre. Tele2 Sverige considérait que la législation suédoise transposant la directive 2006/24 n'était pas conforme à la Charte.

51. Le 15 avril 2014, la Rikspolisstyrelsen (direction générale de la police nationale, Suède, ci-après la « RPS ») a saisi la PTS d'une plainte au motif que Tele2 Sverige avait cessé de communiquer à ses services les données relatives à certaines communications électroniques. Dans sa plainte, la RPS exposait que le refus de Tele2 Sverige entraînait des conséquences sérieuses sur les activités répressives de la police.

52. Par injonction du 27 juin 2014, la PTS a ordonné à Tele2 Sverige de procéder à la conservation des données, en application de l'article 16 a du chapitre 6 de la LEK et des articles 37 à 43 du FEK, au plus tard le 25 juillet 2014.

53. Tele2 Sverige a saisi le Förvaltningsrätten i Stockholm (tribunal administratif de Stockholm, Suède) d'un recours contre la décision de la PTS. Par jugement du 13 octobre 2014, le Förvaltningsrätten i Stockholm a rejeté ce recours.

54. Tele2 Sverige a interjeté appel du jugement du Förvaltningsrätten i Stockholm devant la juridiction de renvoi en vue d'obtenir l'annulation de la décision contestée.

55. Constatant qu'il existait des arguments militant tant en faveur que contre le fait qu'une obligation de conservation d'une ampleur telle que celle prévue à l'article 16 a du chapitre 6 de la LEK soit compatible avec les dispositions de l'article 15, paragraphe 1, de la directive 2002/58 ainsi que de celles des articles 7, 8 et 52, paragraphe 1, de la Charte, le Kammarrätten i Stockholm (cour administrative d'appel de Stockholm, Suède) 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 ne soient opérées en fonction de l'objectif de lutte contre la criminalité [telle que décrite aux points 13 à 18 de la décision de renvoi], est-elle compatible avec l'article 15, paragraphe 1, de la directive 2002/58 compte tenu des articles 7, 8 et 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 l'est exposé au point 37 [de la décision de renvoi] ? »

B – *L'affaire C-698/15*

56. MM. Watson, Brice et Lewis ont introduit devant la High Court of Justice (England & Wales), Queen's Bench Division (Administrative Court) [Haute Cour de justice (Angleterre et pays de Galles), division du Banc de la Reine (chambre administrative)] des recours juridictionnels en contrôle de légalité (« judicial review ») du régime de conservation des données figurant dans la section 1 de la DRIPA, habilitant le Ministre à imposer aux opérateurs de télécommunications publiques la conservation de toutes les données relatives à des communications pour une durée maximale de douze mois, la conservation du contenu des communications en cause étant exclue.

57. Open Rights Group, Privacy International et la Law Society of England and Wales ont été autorisées à intervenir dans chacun de ces recours.

58. Par jugement du 17 juillet 2015, cette juridiction a constaté que ledit régime n'était pas compatible avec le droit de l'Union dans la mesure où il ne répond pas aux exigences posées par l'arrêt DRI, qu'elle a considérées comme étant applicables aux réglementations des États membres en matière de conservation des données relatives à des communications électroniques et d'accès à de telles données. Le Ministre a interjeté appel de ce jugement devant la juridiction de renvoi.

59. Dans un arrêt du 20 novembre 2015, la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile), Royaume-Uni] a estimé à titre provisoire que l'arrêt DRI n'a pas établi des exigences impératives en droit de l'Union auxquelles les législations nationales doivent se conformer, mais a simplement identifié et décrit des protections qui ne figuraient pas dans le régime harmonisé de l'Union.

60. Toutefois, estimant que les réponses à ces questions du droit de l'Union n'étaient pas claires et étaient nécessaires pour se prononcer dans ces procédures, la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile) (Royaume-Uni)] a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) L'arrêt [DRI] (y compris, notamment, ses points 60 et 62) établit-il des exigences impératives en droit de l'Union européenne, 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 [DRI] étend-il le champ d'application des articles 7 et/ou 8 de la charte au-delà de celui de l'article 8 de la Convention européenne des droits de l'homme (la "CEDH"), tel qu'établi par la jurisprudence de la Cour européenne des droits de l'homme (la Cour EDH) ? »

IV – La procédure devant la Cour

61. Les demandes de décision préjudicielle ont été enregistrées au greffe de la Cour le 4 mai 2015 dans l'affaire C-203/15 et le 28 décembre 2015 dans l'affaire C-698/15.

62. Par ordonnance du 1er février 2016, la Cour a décidé 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.

63. Dans l'affaire C-203/15, ont présenté des observations écrites Tele2 Sverige, les gouvernements belge, tchèque, danois, allemand, estonien, irlandais, espagnol, français, hongrois, néerlandais, suédois et du Royaume-Uni ainsi que la Commission européenne.

64. Dans l'affaire C-698/15, ont présenté des observations écrites MM. Watson, Brice et Lewis, Open Rights Group, Privacy International, la Law Society of England and Wales, les gouvernements tchèque, danois, allemand, estonien, irlandais, français, chypriote, polonais, finlandais et du Royaume-Uni ainsi que la Commission.

65. Par décision de la Cour du 10 mars 2016, ces deux affaires ont été jointes aux fins de la procédure orale et de l'arrêt.

66. Ont comparu à l'audience de plaidoiries du 12 avril 2016 pour y être entendus en leurs observations les représentants de Tele2 Sverige, MM. Watson, Brice et Lewis, Open Rights Group, Privacy International et la Law Society of England and Wales, les gouvernements tchèque, danois, allemand, estonien, irlandais, espagnol, français, finlandais, suédois et du Royaume-Uni ainsi que la Commission.

V – Analyse des questions préjudicielles

67. Par la première question posée dans l'affaire C-203/15, la juridiction de renvoi demande à la Cour si, à la lumière de l'arrêt DRI, l'article 15, paragraphe 1, de la directive 2002/58 ainsi que les articles 7, 8 et 52, paragraphe 1, de la Charte doivent être interprétés en ce sens qu'ils s'opposent à ce qu'un État membre impose aux fournisseurs une obligation générale de conservation de données, telle que celles en cause dans les litiges au principal, et ce indépendamment d'éventuelles garanties accompagnant cette obligation.

68. Dans l'hypothèse où cette question appelle une réponse négative, la seconde question posée dans l'affaire C-203/15 et la première question posée dans l'affaire C-698/15 visent à déterminer si ces dispositions doivent être interprétées en ce sens qu'elles s'opposent à ce qu'un État membre impose aux fournisseurs une obligation générale de conservation de données lorsque cette obligation n'est pas accompagnée de l'ensemble des garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI concernant l'accès aux données, la durée de conservation ainsi que la protection et la sécurité des données.

69. Dans la mesure où ces trois questions sont intimement liées, je les examinerai conjointement dans la suite de mon exposé.

70. En revanche, la seconde question posée dans l'affaire C-698/15 requiert un traitement séparé. Par cette question, la juridiction de renvoi demande à la Cour si l'arrêt DRI a étendu le champ d'application des articles 7 et/ou 8 de la Charte au-delà de celui de l'article 8 de la CEDH. J'exposerai dans la section suivante les raisons pour lesquelles je considère que cette question doit être rejetée comme irrecevable.

71. Avant d'entamer l'examen de ces questions, je crois utile de rappeler le type de données visées par les obligations de conservation en cause dans les litiges au principal. Selon les constatations effectuées par les juridictions de renvoi, l'étendue de ces obligations est, en substance, équivalente à celle de l'obligation qui était prévue à l'article 5 de la directive 2006/24[8]. De manière schématique, les données relatives aux communications qui font l'objet de ces obligations de conservation peuvent être rangées dans quatre catégories[9] :

— les données permettant d'identifier tant la source que la destination de la communication ;

— les données permettant de localiser tant la source que la destination de la communication ;

— les données relatives à la date, à l'heure et à la durée de la communication, et

— les données permettant de déterminer le type de communication et le type de matériel utilisé.

72. Le contenu des communications est exclu des obligations générales de conservation de données en cause dans les affaires au principal, à l'image de ce que prévoyait l'article 5, paragraphe 2, de la directive 2006/24.

A – *Sur la recevabilité de la seconde question posée dans l'affaire C-698/15*

73. La seconde question posée dans l'affaire C-698/15 invite la Cour à préciser si l'arrêt DRI étend le champ d'application des articles 7 et/ou 8 de la Charte au-delà de celui de l'article 8 de la CEDH tel qu'interprété par la Cour EDH.

74. Cette question reflète notamment un argument invoqué par le Ministre devant la juridiction de renvoi, selon lequel la jurisprudence de la Cour EDH n'exige pas, d'une part, que l'accès aux données soit subordonné à l'autorisation préalable d'un organe indépendant ni, d'autre part, que la conservation et l'accès à ces données soient limités à la lutte contre les infractions graves.

75. J'estime que cette question doit être rejetée comme étant irrecevable pour les motifs suivants. À l'évidence, les motifs et la solution adoptés par la Cour dans l'arrêt DRI revêtent une importance déterminante pour trancher les litiges au principal. Cependant, la circonstance que cet arrêt ait éventuellement étendu le champ d'application des articles 7 et/ou 8 de la Charte au-delà de celui de l'article 8 de la CEDH n'est pas, en soi, pertinente pour trancher ces litiges.

76. À cet égard, il importe de rappeler que, conformément à l'article 6, paragraphe 3, TUE, les droits fondamentaux, tels que garantis par la CEDH, font partie du droit de l'Union en tant que principes généraux. Toutefois, en l'absence d'adhésion de l'Union à cette convention, celle-ci ne constitue pas un instrument juridique formellement intégré à l'ordre juridique de l'Union[10].

77. Certes, la première phrase de l'article 52, paragraphe 3, de la Charte établit une règle d'interprétation selon laquelle, dans la mesure où la Charte contient des droits correspondant à des droits garantis par la CEDH, « leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ».

8 — Cette équivalence est compréhensible dès lors que ces régimes nationaux visaient à transposer cette directive aujourd'hui invalidée.

9 — Voir la description des régimes nationaux en cause dans les litiges au principal aux points 11 à 13 et 36 des présentes conclusions.

10 — Avis 2/13, du 18 décembre 2014 (EU:C:2014:2454, point 179), et arrêt du 15 février 2016, N. (C-601/15 PPU, EU:C:2016:84, point 45 et jurisprudence citée).

78. Toutefois, selon la seconde phrase de l'article 52, paragraphe 3, de la Charte, « cette disposition ne fait pas obstacle à ce que le droit de l'Union accorde une protection plus étendue ». À mes yeux, il résulte de cette phrase qu'il est loisible à la Cour, si elle le juge nécessaire dans le contexte du droit de l'Union, d'étendre le champ d'application des dispositions de la Charte au-delà de celui des dispositions correspondantes de la CEDH.

79. J'ajoute, à titre subsidiaire, que l'article 8 de la Charte, interprété par la Cour dans l'arrêt DRI, établit un droit qui ne correspond à aucun droit garanti par la CEDH, à savoir le droit à la protection des données à caractère personnel, ce que confirment par ailleurs les explications relatives à l'article 52 de la Charte [11]. Partant, la règle d'interprétation établie à l'article 52, paragraphe 3, première phrase, de la Charte n'est, en toute hypothèse, pas applicable à l'interprétation de l'article 8 de la Charte, comme l'ont relevé MM. Brice et Lewis, Open Rights Group et Privacy International, la Law Society of England and Wales ainsi que les gouvernements tchèque, irlandais et finlandais.

80. Il découle de ce qui précède que le droit de l'Union ne s'oppose pas à ce que les articles 7 et 8 de la Charte accordent une protection plus étendue que celle prévue par la CEDH. Dès lors, la circonstance que l'arrêt DRI ait éventuellement étendu le champ d'application de ces dispositions de la Charte au-delà de celui de l'article 8 de la CEDH n'est pas, en soi, pertinente pour trancher les litiges au principal. La solution à apporter à ces litiges dépend essentiellement des conditions auxquelles une obligation générale de conservation de données peut être considérée comme compatible avec l'article 15, paragraphe 1, de la directive 2002/58 ainsi qu'avec les articles 7, 8 et 52, paragraphe 1, de la Charte, interprétés à la lumière de l'arrêt DRI, ce qui fait précisément l'objet des trois autres questions posées dans les présentes affaires.

81. Selon une jurisprudence constante, le rejet d'une demande formée par une juridiction nationale n'est possible que s'il apparaît de manière manifeste que l'interprétation sollicitée du droit de l'Union n'a aucun rapport avec la réalité ou l'objet du litige au principal ou encore lorsque le problème est de nature hypothétique ou que la Cour ne dispose pas des éléments de fait et de droit nécessaires pour répondre de façon utile aux questions qui lui sont posées [12].

82. En l'occurrence, et pour les motifs exposés ci-avant, la seconde question posée dans l'affaire C-698/15 ne revêt, me semble-t-il, qu'un intérêt théorique étant donné qu'une éventuelle réponse à cette question ne permettrait pas de dégager des éléments d'interprétation de droit de l'Union que la juridiction de renvoi pourrait appliquer utilement pour résoudre, en fonction de ce droit, le litige pendant devant elle [13].

83. Dans ces conditions, je considère que ladite question doit être rejetée comme étant irrecevable, comme l'ont fait valoir à juste titre M. Watson, la Law Society of England and Wales et le gouvernement tchèque.

11 — Conformément à l'article 6, paragraphe 1, troisième alinéa, TUE et à l'article 52, paragraphe 7, de la Charte, les explications relatives à la Charte doivent être prises en considération en vue de son interprétation (voir arrêts du 26 février 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, point 20, et du 15 février 2016, N., C-601/15 PPU, EU:C:2016:84, point 47). Selon ces explications, l'article 7 de la Charte correspond à l'article 8 de la CEDH, tandis que l'article 8 de la Charte ne correspond à aucun droit de la CEDH.

12 — Voir notamment arrêts du 9 novembre 2010, Volker und Markus Schecke et Eifert (C-92/09 et C-93/09, EU:C:2010:662, point 40 et jurisprudence citée), ainsi que du 24 avril 2012, Kamberaj (C-571/10, EU:C:2012:233, point 42 et jurisprudence citée).

13 — Voir notamment arrêt du 16 septembre 1982, Vlaeminck (132/81, EU:C:1982:294, point 13) ; ordonnance du 24 mars 2011, Abt e.a. (C-194/10, EU:C:2011:182, points 36 et 37 ainsi que jurisprudence citée), et arrêt du 24 octobre 2013, Stoilov i Ko (C-180/12, EU:C:2013:693, point 46 et jurisprudence citée).

B – *Sur la compatibilité d'une obligation générale de conservation de données avec le régime établi par la directive 2002/58*

84. La présente section porte sur la possibilité, pour les États membres, de faire usage de la faculté offerte par l'article 15, paragraphe 1, de la directive 2002/58 en vue d'imposer une obligation générale de conservation de données. Elle n'examine pas, en revanche, les exigences particulières devant être respectées par les États membres souhaitant faire usage de cette faculté, lesquelles seront amplement analysées dans une section ultérieure [14].

85. En effet, Open Rights Group et Privacy International ont fait valoir qu'une telle obligation serait incompatible avec le régime harmonisé établi par la directive 2002/58, et ce indépendamment du respect des exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58, au motif qu'elle réduirait à néant l'essentiel des droits et du régime établis par cette directive.

86. Avant d'examiner cet argument, il y a lieu de vérifier qu'une obligation générale de conservation de données relève du champ d'application de cette directive.

1. Sur l'inclusion d'une obligation générale de conservation de données dans le champ d'application de la directive 2002/58

87. Aucune des parties ayant soumis des observations à la Cour n'a contesté le fait qu'une obligation générale de conservation de données, telle que celles en cause dans les litiges au principal, relève de la notion de « 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] » au sens de l'article 3 de la directive 2002/58.

88. Cependant, les gouvernements tchèque, français, polonais et du Royaume-Uni ont soutenu qu'une obligation générale de conservation de données relève de l'exclusion établie à l'article 1er, paragraphe 3, de la directive 2002/58. D'une part, les dispositions nationales régissant l'accès aux données et l'exploitation de celles-ci par les autorités policières ou judiciaires des États membres concerneraient la sécurité publique, la défense ou la sûreté de l'État ou relèveraient à tout le moins du droit pénal. D'autre part, le seul objectif de la conservation des données serait de permettre à ces autorités policières ou judiciaires d'y accéder et de les exploiter. Partant, une obligation de conservation des données serait exclue du champ d'application de cette directive en application de la disposition précitée.

89. Ce raisonnement n'emporte pas ma conviction pour les motifs suivants.

90. En premier lieu, le libellé de l'article 15, paragraphe 1, de la directive 2002/58 confirme que les obligations de conservation imposées par les États membres relèvent du champ d'application de cette directive. Aux termes de cette disposition, en effet, « 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 ». Il me semble pour le moins difficile de soutenir que les obligations de conservation sont exclues du champ d'application de cette directive alors même que l'article 15, paragraphe 1, de ladite directe régit la faculté d'adopter de telles obligations.

91. En réalité, et comme l'ont fait valoir M. Watson, MM. Brice et Lewis, les gouvernements belge, danois, allemand, finlandais ainsi que la Commission, une obligation générale de conservation de données, telle que celles en cause dans les litiges au principal, constitue une mise en œuvre de l'article 15, paragraphe 1, de la directive 2002/58.

14 — Voir points 126 à 262 des présentes conclusions.

92. En deuxième lieu, le fait que les dispositions régissant l'accès puissent relever de l'exclusion établie à l'article 1er, paragraphe 3, de la directive 2002/58 [15] n'implique pas que l'obligation de conservation en relève également et, partant, se situe en dehors du champ d'application de cette directive.

93. À cet égard, la Cour a déjà eu l'opportunité de préciser que les activités mentionnées à l'article 3, paragraphe 2, premier tiret, de la directive 95/46/CE [16], dont le libellé a une portée équivalente à celui de l'article 1er, paragraphe 3, de la directive 2002/58, étaient des activités propres aux États ou aux autorités étatiques et étrangères aux domaines d'activité des particuliers [17].

94. Or, les obligations de conservation en cause dans les litiges au principal sont imposées à des opérateurs privés dans le cadre d'activités privées de fourniture de services de communications électroniques, comme l'a relevé la Commission. En outre, ces obligations s'imposent indépendamment de toute demande d'accès de la part des autorités policières ou judiciaires ainsi que, plus généralement, de tout acte des autorités étatiques relevant de la sécurité publique, de la défense, de la sûreté de l'État ou du droit pénal.

95. En troisième lieu, la solution adoptée par la Cour dans l'arrêt Irlande/Parlement et Conseil confirme qu'une obligation générale de conservation de données ne relève pas du domaine pénal [18]. La Cour a en effet jugé que la directive 2006/24, qui établissait une telle obligation, relevait non pas du domaine pénal mais bien du fonctionnement du marché intérieur, de sorte que l'article 95 CE (devenu article 114 TFUE) constituait la base juridique appropriée pour l'adoption de cette directive.

96. Pour arriver à cette conclusion, la Cour a notamment constaté que les dispositions de cette directive étaient essentiellement limitées aux activités des fournisseurs et ne réglementaient pas l'accès aux données ni l'exploitation de celles-ci par les autorités policières ou judiciaires des États membres [19]. J'en déduis que des dispositions de droit national établissant une obligation de conservation similaire à celle prévue par la directive 2006/24 ne relèvent pas non plus du domaine pénal.

97. Eu égard à ce qui précède, je suis d'avis qu'une obligation générale de conservation de données ne relève pas de l'exclusion établie à l'article 1er, paragraphe 3, de la directive 2002/58 et, partant, tombe dans le champ d'application de cette directive.

2. Sur la possibilité de déroger au régime établi par la directive 2002/58 en établissant une obligation générale de conservation de données

98. Il y a lieu à présent de déterminer si une obligation générale de conservation de données est compatible avec le régime établi par la directive 2002/58.

99. La question qui se pose à cet égard est celle de savoir s'il est possible, pour un État membre, de faire usage de la faculté offerte par l'article 15, paragraphe 1, de la directive 2002/58 en vue d'imposer une telle obligation.

100. Quatre arguments ont été avancés à l'encontre d'une telle possibilité, notamment par Open Rights Group et Privacy International.

15 — Voir points 123 à 125 des présentes conclusions.

16 — Directive 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).

17 — Arrêt du 6 novembre 2003, Lindqvist (C-101/01, EU:C:2003:596, points 43 et 44).

18 — Arrêt du 10 février 2009 (C-301/06, EU:C:2009:68).

19 — Arrêt du 10 février 2009, Irlande/Parlement et Conseil (C-301/06, EU:C:2009:68, point 80).

101. Selon un premier argument, octroyer aux États membres le pouvoir d'adopter une obligation générale de conservation de données remettrait en cause l'objectif d'harmonisation qui constitue la raison d'être de la directive 2002/58. Selon son article 1er, paragraphe 1, en effet, cette 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 l'Union.

102. Ainsi, l'article 15, paragraphe 1, de la directive 2002/58 ne pourrait pas être interprété en ce sens qu'il offrirait aux États membres le pouvoir d'adopter une dérogation au régime établi par cette directive d'une ampleur telle que cet effort d'harmonisation serait privé de tout effet utile.

103. Selon un deuxième argument, le libellé de l'article 15, paragraphe 1, de la directive 2002/58 s'opposerait également à une interprétation aussi large du pouvoir des États membres de déroger au régime établi par cette directive. Aux termes de cette disposition, en effet, « 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 [cette] directive » (italique ajouté par mes soins).

104. Or, une obligation générale de conservation de données ne se contenterait pas de « limiter la portée » des droits et des obligations mentionnés par cette disposition, mais réduirait ces droits et obligations à néant. Il en irait ainsi :

— de l'obligation de garantir la confidentialité des données relatives au trafic et de l'obligation de subordonner le stockage d'informations à l'accord de l'utilisateur, respectivement prévues à l'article 5, paragraphes 1 et 3 de la directive 2002/58 ;

— de l'obligation d'effacer ou de rendre anonymes les données relatives au trafic, inscrite à l'article 6, paragraphe 1, de cette directive, et

— de l'obligation de rendre anonymes les données de localisation ou d'obtenir le consentement de l'utilisateur pour traiter ces données, imposée par l'article 9, paragraphe 1, de ladite directive.

105. Ces deux premiers arguments me semblent devoir être rejetés pour les motifs suivants.

106. D'une part, le libellé de l'article 15, paragraphe 1, de la directive 2002/58 évoque la possibilité, pour les États membres, d'adopter « des mesures législatives prévoyant la conservation de données pendant une durée limitée ». Cette référence explicite aux obligations de conservation de données confirme que de telles obligations ne sont pas, en soi, incompatibles avec le régime établi par la directive 2002/58. Si cette formulation ne prévoit pas expressément la possibilité d'adopter une obligation *générale* de conservation de données, force est de constater qu'elle ne s'y oppose pas non plus.

107. D'autre part, le considérant 11 de la directive 2002/58 précise que celle-ci ne modifie 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 [cette] 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, « [ladite] 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 [CEDH] ».

108. Il résulte, à mon avis, de ce considérant 11 que l'intention du législateur de l'Union était non pas de porter atteinte à la faculté des États membres d'adopter les mesures visées à l'article 15, paragraphe 1, de la directive 2002/58, mais bien de soumettre cette faculté à certaines exigences ayant trait, notamment, aux buts poursuivis et à la proportionnalité de ces mesures. En d'autres termes, une obligation générale de conservation de données n'est pas, à mon avis, incompatible avec le régime établi par cette directive, à condition qu'elle satisfasse à certaines conditions.

109. Selon un troisième argument, l'article 15, paragraphe 1, de la directive 2002/58 devrait, en tant que dérogation au régime établi par cette directive, faire l'objet d'une interprétation stricte, et ce en vertu d'une règle d'interprétation résultant d'une jurisprudence constante de la Cour. Cette règle d'interprétation stricte interdirait d'interpréter cette disposition en ce sens qu'elle offrirait la faculté d'imposer une obligation générale de conservation de données.

110. À cet égard, j'ai le sentiment que la faculté prévue à l'article 15, paragraphe 1, de la directive 2002/58 ne peut être qualifiée de dérogation et ne saurait en conséquence être interprétée strictement, comme l'a fait valoir à juste titre la Commission. Il me semble, en effet, difficile de qualifier cette faculté de dérogation au regard du considérant 11 évoqué ci-avant, selon lequel cette directive ne porte pas atteinte à la faculté des États membres d'adopter les mesures visées à cette disposition. Je relève, par ailleurs, que l'article 15 de ladite directive est intitulé « Applications de certaines dispositions de la directive 95/46 », alors que l'article 10 de cette même directive est explicitement intitulé « Dérogations ». Ces intitulés me confortent dans l'idée que la faculté prévue audit article 15 ne peut être qualifiée de « dérogation ».

111. Selon un quatrième et dernier argument, l'incompatibilité d'une obligation générale de conservation de données avec le régime établi par la directive 2002/58 serait corroborée par l'ajout de l'article 15, paragraphe 1 bis, de cette directive lors de l'adoption de la directive 2006/24, invalidée par l'arrêt DRI. En vertu de cet argument, c'est cette incompatibilité qui aurait conduit le législateur de l'Union à déclarer l'article 15, paragraphe 1, de la directive 2002/58 inapplicable au régime de conservation générale prévu par la directive 2006/24.

112. Cet argument me paraît procéder d'une compréhension erronée de la portée de l'article 15, paragraphe 1 bis, de la directive 2002/58. Aux termes de cette disposition, « [l'article 15, paragraphe 1, de la directive 2002/58] 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 [cette] directive ».

113. Ma lecture de cette disposition est la suivante. En ce qui concerne les données dont la conservation était exigée par la directive 2006/24 et aux fins établies par celle-ci, les États membres perdaient la faculté, prévue à l'article 15, paragraphe 1, de la directive 2002/58, de limiter plus avant la portée des droits et des obligations visés par cette disposition, notamment par le biais d'obligations complémentaires de conservation de données. En d'autres termes, l'article 15, paragraphe 1 bis, prévoyait une harmonisation exhaustive en ce qui concerne les données dont la conservation était exigée par la directive 2006/24 et aux fins établies par celle-ci.

114. Je trouve confirmation de cette interprétation au considérant 12 de la directive 2006/24, selon lequel « l'article 15, paragraphe 1, de la directive [2002/58] *continue à s'appliquer* aux données, y compris à celles relatives aux appels téléphoniques infructueux, dont la conservation n'est pas expressément requise par la présente directive et *qui ne relèvent donc pas de son champ d'application*, ainsi qu'à la conservation de données *à d'autres fins que celles prévues par la présente directive*, notamment à des fins judiciaires » (italique ajouté par mes soins).

115. Ainsi, l'insertion de l'article 15, paragraphe 1 bis, de la directive 2002/58 atteste non pas de l'incompatibilité d'une obligation générale de conservation de données avec le régime établi par cette directive, mais bien de la volonté du législateur de l'Union de procéder à une harmonisation exhaustive lors de l'adoption de la directive 2006/24.

116. Eu égard à ce qui précède, j'estime qu'une obligation générale de conservation de données est compatible avec le régime établi par la directive 2002/58 et, partant, qu'il possible pour un État membre de faire usage de la faculté offerte par l'article 15, paragraphe 1, de cette directive en vue d'imposer une telle obligation [20]. Le recours à cette faculté est cependant subordonné au respect d'exigences strictes, découlant non seulement de cette disposition mais également des dispositions pertinentes de la Charte lues à la lumière de l'arrêt DRI, qui seront examinées dans une section ultérieure [21].

C – *Sur l'applicabilité de la Charte à une obligation générale de conservation de données*

117. Avant d'examiner la teneur des exigences qui sont imposées par la Charte, conjointement à l'article 15, paragraphe 1, de la directive 2002/58, lorsqu'un État choisit d'instaurer une obligation générale de conservation de données, il y a lieu de vérifier que la Charte est bien applicable à une telle obligation.

118. L'applicabilité de la Charte à une obligation générale de conservation de données dépend essentiellement de l'applicabilité de la directive 2002/58 à une telle obligation.

119. En effet, selon son article 51, paragraphe 1, première phrase, « les dispositions de la [Charte] s'adressent aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union ». Les explications relatives à l'article 51 de la Charte renvoient, à cet égard, à la jurisprudence de la Cour selon laquelle l'obligation de respecter les droits fondamentaux définis dans le cadre de l'Union ne s'impose aux États membres que lorsqu'ils agissent dans le champ d'application du droit de l'Union [22].

120. Les gouvernements tchèque, français, polonais et du Royaume-Uni, qui ont contesté l'applicabilité de la directive 2002/58 à une obligation générale de conservation de données [23], ont également soutenu que la Charte n'était pas applicable à une telle obligation.

121. J'ai déjà exposé les raisons pour lesquelles je considère qu'une obligation générale de conservation de données constitue une mise en œuvre de la faculté prévue à l'article 15, paragraphe 1, de la directive 2002/58 [24].

122. Par conséquent, je considère que les dispositions de la Charte sont applicables aux mesures nationales instaurant une telle obligation, en application de l'article 51, paragraphe 1, de la Charte, comme l'ont fait valoir M. Watson, MM. Brice et Lewis, Open Rights Group et Privacy International, les gouvernements danois, allemand, finlandais ainsi que la Commission [25].

20 — Étant donné que la directive 2002/58 peut être qualifiée de « lex specialis » par rapport à la directive 95/46 (voir, à cet égard, l'article 1er, paragraphe 2, de la directive 2002/58), je ne crois pas nécessaire de vérifier la compatibilité d'une obligation générale de conservation de données avec le régime établi par la directive 95/46, qui ne fait d'ailleurs pas l'objet des questions posées à la Cour. Par souci d'exhaustivité, je tiens néanmoins à préciser que le libellé de l'article 13, paragraphe 1, de la directive 95/46 offre une plus grande latitude aux États membres que celle offerte par l'article 15, paragraphe 1, de la directive 2002/58, qui en précise la portée dans le cadre de la fourniture de services de communications électroniques accessibles au public. Dès lors que la faculté prévue à l'article 15, paragraphe 1, de la directive 2002/58 permet l'adoption par un État membre d'une obligation générale de conservation de données, j'en déduis que l'article 13, paragraphe 1, de la directive 95/46 le permet également.

21 — Voir points 126 à 262 des présentes conclusions.

22 — Il résulte, en effet, d'une jurisprudence constante de la Cour que les droits fondamentaux garantis dans l'ordre juridique de l'Union ont vocation à être appliqués dans toutes les situations régies par le droit de l'Union, mais pas en dehors de telles situations. C'est dans cette mesure que la Cour a déjà rappelé qu'elle ne peut apprécier, au regard de la Charte, une réglementation nationale qui ne se situe pas dans le cadre du droit de l'Union. En revanche, dès lors qu'une telle réglementation entre dans le champ d'application de ce droit, la Cour, saisie à titre préjudiciel, doit fournir tous les éléments d'interprétation nécessaires à l'appréciation, par la juridiction nationale, de la conformité de cette réglementation avec les droits fondamentaux dont elle assure le respect (voir arrêt du 26 février 2013, Åkerberg Fransson, C-617/10, EU:C:2013:105, point 19 et jurisprudence citée).

23 — Voir point 88 des présentes conclusions.

24 — Voir points 90 à 97 des présentes conclusions.

25 — De manière plus précise, l'article 51, paragraphe 1, seconde phrase, de la Charte dispose que les États membres sont tenus de respecter les droits garantis par celle-ci lorsqu'ils mettent en œuvre le droit de l'Union.

123. Cette conclusion n'est pas remise en cause par le fait que les dispositions nationales régissant l'accès aux données conservées ne tombent pas, en tant que telles, dans le domaine d'application de la Charte.

124. Certes, dans la mesure où elles concernent des « activités de l'État dans des domaines relevant du droit pénal », les dispositions nationales régissant l'accès aux données conservées par les autorités policières ou judiciaires en vue de lutter contre des infractions graves relèvent, à mon avis, de l'exclusion prévue à l'article 1er, paragraphe 3, de la directive 2002/58 [26]. Par conséquent, de telles dispositions nationales ne mettent pas en œuvre le droit de l'Union, de sorte que la Charte ne leur est pas applicable.

125. Néanmoins, la raison d'être d'une obligation de conservation de données est de permettre aux autorités répressives d'accéder aux données conservées, de sorte que les problématiques de la conservation et de l'accès ne sauraient être complètement dissociées. Comme l'a souligné à juste titre la Commission, les dispositions régissant l'accès revêtent une importance déterminante pour juger de la compatibilité avec la Charte des dispositions instaurant une obligation générale de conservation de données, lesquelles mettent en œuvre l'article 15, paragraphe 1, de la directive 2002/58. Plus précisément, les dispositions régissant l'accès doivent être prises en compte pour apprécier la nécessité et la proportionnalité d'une telle obligation [27].

D – *Sur la compatibilité d'une obligation générale de conservation de données avec les exigences établies par l'article 15, paragraphe 1, de la directive 2002/58 ainsi que par les articles 7, 8 et 52, paragraphe 1, de la Charte*

126. Il me reste à présent à aborder la difficile question de la compatibilité d'une obligation générale de conservation de données avec les exigences établies par l'article 15, paragraphe 1, de la directive 2002/58 ainsi que par les articles 7, 8 et 52, paragraphe 1, de la Charte lus à la lumière de l'arrêt DRI. Cette question concerne, de manière plus générale, la nécessaire adaptation du cadre légal encadrant les capacités de surveillance des États, lesquelles ont été démultipliées par les récents progrès technologiques [28].

127. La première étape de toute analyse, dans ce contexte, réside dans le constat d'ingérence dans les droits consacrés par la directive 2002/58 et dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte.

128. En effet, une telle obligation constitue une ingérence grave dans le droit au respect de la vie privée, consacré à l'article 7 de la Charte, et dans le droit à la protection des données à caractère personnel, garanti par l'article 8 de la Charte. Je ne crois pas utile de m'appesantir sur ce constat d'ingérence, qui a été clairement posé par la Cour aux points 32 à 37 de l'arrêt DRI [29]. De la même façon, une obligation générale de conservation de données constitue une ingérence dans plusieurs droits consacrés par la directive 2002/58 [30].

26 — Sur la portée de cette exclusion, voir points 90 à 97 des présentes conclusions.

27 — Voir points 185 à 262 des présentes conclusions.

28 — Voir notamment Conseil des droits de l'homme des Nations unies, rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, 17 avril 2013, A/HRC/23/40, n° 33 : « Les progrès technologiques permettent à l'État de se livrer à des activités de surveillance qui ne sont plus limitées par des critères d'échelle ou de durée. […] En conséquence, l'État dispose à présent plus que jamais de moyens accrus pour mener des activités de surveillance simultanées, attentatoires à la vie privée, ciblées et à grande échelle. […] ». Voir également n° 50 : « De manière générale, la législation n'a pas suivi le rythme des changements technologiques. Dans la plupart des États, les normes juridiques sont soit inexistantes, soit inadéquates pour faire face aux conditions modernes de surveillance des communications. […] ».

29 — Je reviendrai néanmoins sur les risques spécifiques posés par la constitution de bases de données d'une telle ampleur dans le cadre de l'exigence de proportionnalité, dans une société démocratique, d'une obligation générale de conservation de données telle que celles en cause dans les litiges au principal : voir points 252 à 261 des présentes conclusions.

30 — Voir, à cet égard, l'argument invoqué par Open Rights Group et Privacy International, résumé au point 104 des présentes conclusions.

129. La seconde étape de l'analyse consiste à déterminer si, et à quelles conditions, cette ingérence grave dans les droits consacrés par la directive 2002/58 ainsi que dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte peut être justifiée.

130. Deux dispositions établissent les conditions devant être satisfaites pour que cette double ingérence soit justifiée : l'article 15, paragraphe 1, de la directive 2002/58, qui encadre la faculté pour les États membres de limiter la portée de certains droits établis par cette directive, et l'article 52, paragraphe 1, de la Charte, lu à la lumière de l'arrêt DRI, qui encadre toute limitation de l'exercice des droits consacrés par la Charte.

131. Je tiens à souligner que ces exigences sont *cumulatives*. En effet, le respect des exigences établies à l'article 15, paragraphe 1, de la directive 2002/58 n'implique pas, en soi, que les exigences prévues à l'article 52, paragraphe 1, de la Charte sont satisfaites, et inversement [31]. Par conséquent, une obligation générale de conservation de données ne pourra être considérée comme compatible avec le droit de l'Union que si elle respecte à la fois les exigences établies à l'article 15, paragraphe 1, de la directive 2002/58 et celles prévues à l'article 52, paragraphe 1, de la Charte, comme l'a souligné la Law Society of England and Wales [32].

132. Ensemble, ces deux dispositions établissent six exigences devant être satisfaites pour que soit justifiée l'ingérence engendrée par une obligation générale de conservation de données :

— l'obligation de conservation doit avoir une base légale ;

— elle doit respecter le contenu essentiel des droits consacrés par la Charte ;

— elle doit poursuivre un objectif d'intérêt général ;

— elle doit être appropriée à la poursuite de cet objectif ;

— elle doit être nécessaire à la poursuite dudit objectif, et

— elle doit être proportionnée, au sein d'une société démocratique, à la poursuite de ce même objectif.

133. Plusieurs de ces conditions ont déjà été évoquées par la Cour dans l'arrêt DRI. Par souci de clarté et compte tenu des particularités des présentes affaires par rapport à l'affaire DRI, je souhaite néanmoins revenir sur chacune d'entre elles, en examinant de manière plus détaillée les exigences ayant trait à la base légale, au caractère nécessaire ainsi qu'au caractère proportionné au sein d'une société démocratique d'une obligation générale de conservation de données.

1. Sur l'exigence d'une base légale en droit national

134. Tant l'article 52, paragraphe 1, de la Charte que l'article 15, paragraphe 1, de la directive 2002/58 établissent des exigences quant à la base légale devant être utilisée par un État membre en vue d'imposer une obligation générale de conservation de données.

31 — Je trouve confirmation de cette nature cumulative dans la dernière phrase de l'article 15, paragraphe 1, de la directive 2002/58, selon laquelle « toutes les mesures visées par [ce] paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, TUE ». En vertu de l'article 6, paragraphe 1, TUE, « l'Union reconnaît les droits, les libertés et les principes énoncés dans la [Charte], laquelle a la même valeur juridique que les traités ».

32 — Il résulte logiquement de cette nature cumulative que, dans la mesure où les exigences établies par ces deux dispositions se chevauchent, il y a lieu de faire application de l'exigence la plus stricte ou, en d'autres termes, de l'exigence la plus protectrice des droits en cause.

135. En premier lieu, toute limitation de l'exercice des droits reconnus par la Charte doit être « prévue par la loi » en vertu de son article 52, paragraphe 1. Je précise que cette exigence n'a pas été formellement examinée par la Cour dans l'arrêt DRI, qui concernait une ingérence prévue par une directive.

136. Jusqu'au récent arrêt WebMindLicenses [33], la Cour ne s'était jamais prononcée sur la portée exacte de cette exigence, et ce même lorsqu'elle avait expressément constaté que cette exigence était [34] ou n'était pas [35] satisfaite. Au point 81 de cet arrêt, la troisième chambre de la Cour s'est prononcée dans les termes suivants :

« À cet égard, il convient de souligner que l'exigence que toute limitation de l'exercice de ce droit doit être prévue par la loi implique que la base légale qui permet l'utilisation des preuves mentionnées au point précédent par l'administration fiscale doit être suffisamment claire et précise et que, en définissant elle-même la portée de la limitation de l'exercice du droit garanti par l'article 7 de la Charte, elle offre une certaine protection contre d'éventuelles atteintes arbitraires de cette administration (voir, notamment, Cour EDH, Malone c. Royaume-Uni, 2 août 1984, série A nº 82, § 67, ainsi que Gillan et Quinton c. Royaume-Uni, 12 janvier 2010, nº 4158/05, § 77, CEDH 2010) ».

137. J'invite la grande chambre de la Cour à confirmer cette interprétation dans les présentes affaires pour les motifs suivants.

138. Comme l'a justement relevé M. l'avocat général Cruz Villalón dans ses conclusions dans l'affaire Scarlet Extended [36], la Cour EDH a élaboré un abondant corps de jurisprudence relatif à cette exigence dans le contexte de la CEDH, laquelle se caractérise par une acception matérielle et non formelle du terme « loi» [37].

139. Selon cette jurisprudence, l'expression « prévue par la loi » implique que la base légale soit suffisamment accessible et prévisible, c'est-à-dire énoncée avec assez de précision pour permettre à l'individu, en s'entourant au besoin de conseils éclairés, de régler sa conduite. Cette base légale doit également fournir une protection adéquate contre l'arbitraire et, en conséquence, définir avec une netteté suffisante l'étendue et les modalités d'exercice du pouvoir conféré aux autorités compétentes (principe de la prééminence du droit) [38].

140. Or, il est selon moi nécessaire que l'expression « prévue par la loi » utilisée à l'article 52, paragraphe 1, de la Charte se voie attribuer une portée similaire à celle que revêt cette expression dans le contexte de la CEDH, pour les raisons suivantes.

33 — Arrêt du 17 décembre 2015 (C-419/14, EU:C:2015:832).

34 — Voir, notamment, arrêts du 17 octobre 2013, Schwarz (C-291/12, EU:C:2013:670, point 35) (ingérence prévue par un règlement européen) ; du 27 mai 2014, Spasic (C-129/14 PPU, EU:C:2014:586, point 57) (ingérence prévue par la Convention d'application de l'accord de Schengen du 14 juin 1985 entre les gouvernements des États de l'Union économique Benelux, de la République fédérale d'Allemagne et de la République française relatif à la suppression graduelle des contrôles aux frontières communes, signée à Schengen le 19 juin 1990 et entrée en vigueur le 26 mars 1995) ; du 6 octobre 2015, Delvigne (C-650/13, EU:C:2015:648, point 47) (ingérence prévue par le code électoral et le code pénal français) ; et du 17 décembre 2015, Neptune Distribution (C-157/14, EU:C:2015:823, point 69) (ingérence prévue par un règlement et une directive européens).

35 — Arrêt du 1er juillet 2010, Knauf Gips/Commission (C-407/08 P, EU:C:2010:389, points 87 à 92) (ingérence dépourvue de base légale).

36 — C-70/10, EU:C:2011:255 (points 94 à 100).

37 — Voir notamment Cour EDH, 14 septembre 2010, Sanoma Uitgevers B.V. c. Pays-Bas, CE:ECHR:2010:0914JUD003822403, § 83.

38 — Voir notamment Cour EDH, 26 mars 1987, Leander c. Suède, CE:ECHR:1987:0326JUD000924881, § 50-51 ; Cour EDH, 26 octobre 2000, Hassan et Tchaouch c. Bulgarie, CE:ECHR:2000:1026JUD003098596, § 84 ; Cour EDH, 4 décembre 2008, S. et Marper c. Royaume-Uni, CE:ECHR:2008:1204JUD003056204, § 95 ; Cour EDH, 14 septembre 2010, Sanoma Uitgevers B.V. c. Pays-Bas, CE:ECHR:2010:0914JUD003822403, § 81-83 ; Cour EDH, 31 mars 2016, Stoyanov et Autres c. Bulgarie, CE:ECHR:2016:0331JUD005538810, § 124-126.

141. D'une part, en vertu de l'article 53 de la Charte et des explications relatives à cet article, le niveau de protection offert par la Charte ne peut jamais être inférieur à celui qui est garanti par la CEDH. Cette interdiction de franchir le « seuil CEDH » implique que l'interprétation par la Cour de l'expression « prévue par la loi » utilisée à l'article 52, paragraphe 1, de la Charte doive être au moins aussi stricte que celle de la Cour EDH dans le contexte de la CEDH [39].

142. D'autre part, eu égard à la nature horizontale de cette exigence, qui est susceptible de s'appliquer à de nombreux types d'ingérences tant dans le contexte de la Charte que dans celui de la CEDH [40], il serait inopportun de soumettre les États membres à des critères différents selon que l'ingérence est examinée au regard de l'un ou de l'autre de ces instruments [41].

143. Partant, j'estime, comme l'ont fait valoir le gouvernement estonien et la Commission, que l'expression « prévue par la loi » inscrite à l'article 52, paragraphe 1, de la Charte doit être interprétée, à la lumière de la jurisprudence de la Cour EDH résumée au point 139 des présentes conclusions, en ce sens qu'une obligation générale de conservation de données, telle que celles en cause dans les litiges au principal, doit être prévue par une base légale suffisamment accessible et prévisible, d'une part, et offrant une protection adéquate contre l'arbitraire, d'autre part.

144. En second lieu, il y a lieu de déterminer la teneur des exigences imposées par l'article 15, paragraphe 1, de la directive 2002/58 en ce qui concerne la base légale devant être utilisée par un État membre souhaitant faire usage de la faculté offerte par cette disposition.

145. Il me faut relever, à cet égard, l'existence d'une divergence entre les versions linguistiques de la première phrase de cette disposition.

146. Dans les versions anglaise (« *legislative measures* »), française (« mesures législatives »), italienne (« *disposizioni legislative* »), portugaise (« *medidas legislativas* »), roumaine (« *măsuri legislative* ») et suédoise (« *genom lagstiftning vidta åtgärder* »), l'article 15, paragraphe 1, première phrase, de la directive 2002/58 impose, à mon avis, l'adoption de mesures émanant du pouvoir législatif.

147. En revanche, les versions danoise (« *retsforskrifter* »), allemande (« *Rechtsvorschriften* »), néerlandaise (« *wettelijke maatregele* ») et espagnole (« *medidas legales* ») de cette phrase peuvent être interprétées comme exigeant l'adoption soit de mesures émanant du pouvoir législatif, soit de mesures réglementaires émanant du pouvoir exécutif.

148. Conformément à une jurisprudence constante, la nécessité d'une application et, dès lors, d'une interprétation uniformes d'un acte de l'Union exclut que celui-ci soit considéré isolément dans l'une de ses versions, mais exige qu'il soit interprété en fonction tant de la volonté réelle de son auteur que du but poursuivi par ce dernier, à la lumière, notamment, des versions établies dans toutes les autres langues officielles. En cas de divergence entre celles-ci, la disposition en cause doit être interprétée en fonction de l'économie générale et de la finalité de la réglementation dont elle constitue un élément [42].

39 — Pour être plus précis, la Cour ne peut, selon moi, adopter une interprétation de cette exigence qui serait plus permissive que celle de la Cour EDH, ce qui aurait pour conséquence de permettre un nombre d'ingérences plus élevé que celui qui résulterait de l'interprétation de cette exigence par la Cour EDH.

40 — Cette expression « prévue par la loi » est utilisée à l'article 8, paragraphe 2 (droit au respect de la vie privée et familiale), à l'article 9, paragraphe 2 (liberté de pensée, de conscience et de religion), à l'article 10, paragraphe 2 (liberté d'expression), et à l'article 11, paragraphe 2 (liberté de réunion et d'association), de la CEDH. Dans le contexte de la Charte, l'article 52, paragraphe 1, s'applique à toute limitation de l'exercice des droits consacrés par celle-ci, à supposer qu'une telle limitation soit permise.

41 — Voir en ce sens Peers, S., « Article 52 – Scope of guaranteed rights », in Peers, S., et al, *The EU Charter of Fundamental Rights : a Commentary,* Oxford, OUP, 2014, n° 52.39.

42 — Voir, notamment, arrêt du 30 mai 2013, Asbeek Brusse et de Man Garabito (C-488/11, EU:C:2013:341, point 26) ; du 24 juin 2015, Hotel Sava Rogaška (C-207/14, EU:C:2015:414, point 26), et du 26 février 2015, Christie's France (C-41/14, EU:C:2015:119, point 26).

149. En l'occurrence, l'article 15, paragraphe 1, de la directive 2002/58 régit la faculté pour les États membres de déroger aux droits fondamentaux consacrés aux articles 7 et 8 de la Charte, dont la protection est mise en œuvre par cette directive. J'estime dès lors opportun d'interpréter l'exigence d'une base légale imposée par l'article 15, paragraphe 1, de la directive 2002/58 à la lumière de la Charte, et en particulier de l'article 52, paragraphe 1, de celle-ci.

150. Ainsi, les « mesures » exigées par l'article 15, paragraphe 1, de la directive 2002/58 doivent impérativement posséder les qualités d'accessibilité, de prévisibilité et de protection adéquate contre l'arbitraire, évoquées au point 143 des présentes conclusions. Il découle notamment de ces qualités, et en particulier de l'exigence de protection adéquate contre l'arbitraire, que ces mesures doivent être *contraignantes* pour les autorités nationales se voyant octroyer le pouvoir d'accéder aux données conservées. Il ne serait notamment pas suffisant que les garanties entourant l'accès à ces données soient prévues dans des codes ou des lignes directrices internes ne possédant pas un tel caractère contraignant, comme l'a souligné à juste titre la Law Society of England and Wales.

151. En outre, l'expression « les États membres peuvent adopter des mesures », commune à toutes les versions linguistiques de l'article 15, paragraphe 1, première phrase, de la directive 2002/58, me paraît exclure la possibilité qu'une jurisprudence nationale, même constante, puisse constituer une base légale suffisante en vue de mettre en œuvre cette disposition. Je souligne que, dans cette mesure, ladite disposition va au-delà des exigences résultant de la jurisprudence de la Cour EDH [43].

152. J'ajoute qu'il me paraît souhaitable, eu égard à la gravité des ingérences qu'implique une obligation générale de conservation de données dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, que le contenu essentiel du régime en cause, et notamment celui des garanties entourant cette obligation, soient établis dans une mesure adoptée par le pouvoir législatif, à charge pour le pouvoir exécutif d'en préciser les modalités d'application.

153. Eu égard à ce qui précède, je considère que l'article 15, paragraphe 1, de la directive 2002/58 et l'article 52, paragraphe 1, de la Charte doivent être interprétés en ce sens que le régime établissant une obligation générale de conservation de données, telle que celles en cause dans les litiges au principal, doit être établi par des mesures législatives ou réglementaires possédant les qualités d'accessibilité, de prévisibilité et de protection adéquate contre l'arbitraire.

154. Il appartient aux juridictions de renvoi de vérifier le respect de cette exigence, eu égard à leur position privilégiée aux fins de l'évaluation de leurs régimes nationaux respectifs.

2. Sur le respect du contenu essentiel des droits reconnus par les articles 7 et 8 de la Charte

155. Aux termes de son article 52, paragraphe 1, toute limitation de l'exercice des droits reconnus par la Charte doit « respecter le contenu essentiel desdits droits» [44]. Cet aspect, qui a été examiné par la Cour aux points 39 et 40 de l'arrêt DRI dans le contexte de la directive 2006/24, ne me semble pas soulever de problème particulier dans le cadre des présentes affaires, comme l'ont relevé les gouvernements espagnol et irlandais ainsi que la Commission.

43 — Voir notamment Cour EDH, 14 septembre 2010, Sanoma Uitgevers B.V. c. Pays-Bas, CE:ECHR:2010:0914JUD003822403, § 83 : « [le terme "loi" figurant aux articles 8 à 11 de la CEDH inclut] à la fois le "droit écrit", comprenant aussi bien des textes de rang infralégislatif que des actes réglementaires pris par un ordre professionnel, par délégation du législateur, dans le cadre de son pouvoir normatif autonome, et le "droit non écrit". La "loi" doit se comprendre comme englobant le texte écrit et le "droit élaboré" par les juges ».

44 — Une telle exigence ne ressort pas du libellé de de l'article 15, paragraphe 1, de la directive 2002/58 ni de l'économie de cette directive pour les raisons exposées aux points 99 à 116 des présentes conclusions.

156. Au point 39 de l'arrêt DRI, la Cour a jugé que cette directive ne portait pas atteinte au contenu essentiel du droit au respect de la vie privée et des autres droits consacrés à l'article 7 de la Charte dès lors qu'elle ne permettait pas de prendre connaissance du contenu des communications électroniques en tant que tel.

157. Cette appréciation est, d'après moi, transposable aux régimes nationaux en cause dans les affaires au principal, étant donné que ceux-ci ne permettent pas non plus de prendre connaissance du contenu des communications électroniques en tant que tel [45].

158. Au point 40 de l'arrêt DRI, la Cour a considéré que la directive 2006/24 ne portait pas atteinte au contenu essentiel du droit fondamental à la protection des données à caractère personnel, consacré à l'article 8 de la Charte, eu égard aux principes de protection et de sécurité des données devant être respectés par les fournisseurs en vertu de l' article 7 de cette directive, à charge pour les États membres de veiller à l'adoption de mesures techniques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données.

159. À nouveau, je considère que cette appréciation est transposable aux régimes nationaux en cause dans les affaires au principal, étant donné que ceux-ci prévoient, me semble-t-il, des garanties comparables quant à la protection et la sécurité des données conservées par les fournisseurs, ces garanties devant permettre de protéger efficacement les données à caractère personnel contre les risques d'abus ainsi que contre tout accès et toute utilisation illicites de ces données [46].

160. Il appartient néanmoins aux juridictions de renvoi de vérifier que les régimes nationaux en cause dans les litiges au principal respectent effectivement le contenu essentiel des droits reconnus par les articles 7 et 8 de la Charte, à la lumière des considérations qui précèdent.

3. Sur l'existence d'un objectif d'intérêt général reconnu par l'Union susceptible de justifier une obligation générale de conservation de données

161. Tant l'article 15, paragraphe 1, de la directive 2002/58 que l'article 52, paragraphe 1, de la Charte exigent que toute ingérence dans les droits consacrés par ces instruments poursuive un objectif d'intérêt général.

162. Aux points 41 à 44 de l'arrêt DRI, la Cour a jugé, d'une part, que l'obligation générale de conservation de données imposée par la directive 2006/24 contribuait à « la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique » et, d'autre part, que cette lutte constituait un objectif d'intérêt général l'Union.

163. Il ressort en effet 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. Il en va de même de la lutte contre la criminalité grave afin de garantir la sécurité publique. 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 [47].

164. Cette appréciation est transposable aux obligations générales de conservation de données en cause dans les litiges au principal, qui sont susceptibles d'être justifiées par l'objectif de lutte contre les infractions graves.

45 — Voir la description des régimes nationaux en cause dans les litiges au principal, notamment aux points 13 et 36 des présentes conclusions.

46 — Arrêt DRI, point 54. Voir la description des régimes nationaux en cause dans les litiges au principal aux points 29 à 33 ainsi que 45 et 46 des présentes conclusions.

47 — Arrêt DRI, point 42 et jurisprudence citée.

165. Néanmoins, eu égard à certains arguments soumis à la Cour, il y a lieu de déterminer si une telle obligation peut être justifiée par un autre objectif d'intérêt général que celui de la lutte contre les infractions graves.

166. À cet égard, le libellé de l'article 52, paragraphe 1, de la Charte évoque, de manière générale, « les objectifs d'intérêt général reconnus par l'Union » et « le besoin de protection des droits et libertés d'autrui ».

167. Le libellé de l'article 15, paragraphe 1, de la directive 2002/58 est plus précis quant aux objectifs susceptibles de justifier une ingérence dans les droits établis par cette directive. En effet, selon cette disposition, les mesures en question doivent contribuer à « 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 ».

168. En outre, dans l'arrêt Promusicae [48], la Cour a jugé que cette disposition devait être interprétée à la lumière de l'article 13, paragraphe 1, de la directive 95/46, lequel autorise les dérogations aux droits prévus par cette directive lorsqu'elles sont justifiées par « la protection des droits et libertés d'autrui ». En conséquence, la Cour a jugé que l'article 15, paragraphe 1, de la directive 2002/58 offrait aux États membres la faculté de prévoir l'obligation, pour un fournisseur, de divulguer des données à caractère personnel en vue de déterminer, dans le cadre d'une procédure civile, l'existence d'une atteinte aux droits d'auteur portant sur des enregistrements musicaux et audiovisuels.

169. Le gouvernement du Royaume-Uni a tiré argument de cet arrêt pour faire valoir qu'une obligation générale de conservation de données peut être justifiée par tout objectif mentionné soit à l'article 15, paragraphe 1, de la directive 2002/58, soit à l'article 13, paragraphe 1, de la directive 95/46. Selon ce gouvernement, une telle obligation pourrait être justifiée par l'utilité que présentent les données conservées dans la lutte contre des infractions « simples » (par opposition à « graves ») ou même dans le contexte de procédures non pénales en rapport avec les objectifs mentionnés par ces dispositions.

170. Cet argument n'emporte pas ma conviction pour les raisons suivantes.

171. En premier lieu, et comme l'ont souligné à juste titre M. Watson ainsi que Open Rights Group et Privacy International, l'approche adoptée par la Cour dans l'arrêt Promusicae [49] n'est pas transposable aux présentes affaires, dès lors que cet arrêt concernait une demande d'accès, par une association de titulaires de droits d'auteur, à des données conservées spontanément par un fournisseur, à savoir Telefónica de España. En d'autres termes, cet arrêt ne concernait pas les objectifs susceptibles de justifier les graves ingérences dans les droits fondamentaux qu'implique une obligation générale de conservation de données, telle que celles en cause dans les litiges au principal.

172. En second lieu, j'estime que l'exigence de proportionnalité dans une société démocratique exclut que la lutte contre des infractions simples ou le bon déroulement de procédures non pénales puisse justifier une obligation générale de conservation de données. En effet, les risques considérables qu'engendre une telle obligation sont démesurés par rapport aux avantages qu'elle procurerait dans la lutte contre des infractions simples ou dans le contexte de procédures non pénales [50].

48 — Arrêt du 29 janvier 2008 (C-275/06, EU:C:2008:54, points 50 à 54).

49 — Arrêt du 29 janvier 2008 (C-275/06, EU:C:2008:54).

50 — Voir points 252 à 261 des présentes conclusions.

173. Eu égard à ce qui précède, je considère que l'article 15, paragraphe 1, de la directive 2002/58 et l'article 52, paragraphe 1, de la Charte doivent être interprétés en ce sens que la lutte contre les infractions graves constitue un objectif d'intérêt général susceptible de justifier une obligation générale de conservation de données, à la différence de la lutte contre les infractions simples ou le bon déroulement de procédures non pénales.

174. Par conséquent, il y a lieu d'examiner les caractère approprié, nécessaire et proportionné d'une telle obligation à la lumière de l'objectif de lutte contre les infractions graves.

4. Sur le caractère approprié d'une obligation générale de conservation de données au regard de la lutte contre les infractions graves

175. Les exigences relatives au caractère approprié, nécessaire [51] et proportionné [52] découlent tant de l'article 15, paragraphe 1, de la directive 2002/58 que de l'article 52, paragraphe 1, de la Charte.

176. En vertu de la première de ces exigences, une obligation générale de conservation de données telle que celles en cause dans les litiges au principal doit être apte à contribuer à l'objectif d'intérêt général identifié ci-avant, à savoir la lutte contre les infractions graves.

177. Cette exigence ne pose pas de difficulté particulière dans le contexte des présentes affaires. Comme la Cour l'a relevé en substance au point 49 de l'arrêt DRI, les données conservées permettent aux autorités nationales compétentes en matière pénale de disposer d'un moyen d'investigation supplémentaire pour prévenir ou élucider des infractions graves. Par conséquent, une telle obligation contribue à la lutte contre les infractions graves.

178. Je tiens néanmoins à préciser l'utilité que peut revêtir une obligation générale de conservation de données aux fins de la lutte contre les infractions graves. Comme l'a fait valoir à juste titre le gouvernement français, une telle obligation permet, dans une certaine mesure, aux autorités répressives de « lire le passé » en consultant les données conservées, et ce à la différence des mesures de surveillance ciblées.

179. Une mesure de surveillance ciblée vise des personnes qui ont été préalablement identifiées comme pouvant avoir un lien, même indirect ou lointain, avec une infraction grave. De telles mesures ciblées permettent aux autorités compétentes d'avoir accès aux données relatives aux communications réalisées par ces personnes, voire au contenu de ces communications. Cependant, cet accès ne pourra viser que les communications réalisées par de telles personnes *postérieurement* à leur identification.

180. En revanche, une obligation générale de conservation de données vise l'ensemble des communications réalisées par l'ensemble des utilisateurs, sans que ne soit exigé un quelconque lien avec une infraction grave. Une telle obligation permet aux autorités compétentes d'avoir accès à l'historique des communications réalisées par une personne avant d'avoir été identifiée comme ayant un tel lien. C'est en ce sens qu'une telle obligation octroie aux autorités répressives une capacité limitée de lire le passé, en leur offrant un accès aux communications réalisées par de telles personnes *antérieurement* à leur identification [53].

51 — Sur le caractère nécessaire, voir points 185 à 245 des présentes conclusions.

52 — Sur le caractère proportionné stricto sensu, voir points 246 à 262 des présentes conclusions.

53 — La Commission a également souligné que la valeur ajoutée d'une obligation générale de conservation de données, par rapport à une conservation ciblée de données, réside dans cette capacité limitée de lire le passé : voir Commission Staff Working Document présenté en annexe à la proposition de directive ayant conduit à l'adoption de la directive 2006/24, SEC(2005) 1131, 21 septembre 2005, nº 3.6, « Data Preservation versus Data Retention » : « [W]ith only data preservation as a tool, it is impossible for investigators to go back in time. Data preservation is only useful as of the moment when suspects have been identified – data retention is indispensable in many cases to actually identify those suspects ».

181. En d'autres termes, l'utilité que revêt une obligation générale de conservation de données aux fins de la lutte contre les infractions graves réside dans cette capacité limitée de lire le passé au travers de données retraçant l'historique des communications réalisées par une personne avant même d'être suspectée d'avoir un lien avec une infraction grave [54].

182. Lors de la présentation de la proposition de directive ayant conduit à l'adoption de la directive 2006/24, la Commission a illustré cette utilité à l'aide de plusieurs exemples concrets d'enquêtes portant notamment sur des actes de terrorisme, de meurtre, d'enlèvement et de pédopornographie [55].

183. Plusieurs exemples similaires ont été exposés à la Cour dans le cadre des présentes affaires, notamment par le gouvernement français, lequel a souligné l'obligation positive qui incombe aux États membres d'assurer la sécurité des personnes se trouvant sur leur territoire. Selon ce gouvernement, dans le cadre des enquêtes relatives au démantèlement des filières organisant le départ de résidents français vers des zones de conflit en Irak ou en Syrie, l'accès aux données conservées joue un rôle déterminant pour identifier les personnes qui ont facilité un tel départ. Ledit gouvernement ajoute que l'accès aux données relatives aux communications des personnes impliquées dans les récents attentats terroristes de janvier et de novembre 2015 en France a été extrêmement utile aux enquêteurs pour découvrir les complices des auteurs de ces attentats. De même, dans le cadre de la recherche d'une personne disparue, les données afférentes à la localisation de cette personne lors des communications effectuées avant sa disparition pourraient jouer un rôle déterminant aux fins de l'enquête.

184. Eu égard aux considérations qui précèdent, je considère qu'une obligation générale de conservation de données est apte à contribuer à la lutte contre les infractions graves. Il reste toutefois à vérifier si une telle obligation est à la fois nécessaire et proportionnée à cet objectif.

5. Sur le caractère nécessaire d'une obligation générale de conservation de données au regard de la lutte contre les infractions graves

185. Selon une jurisprudence constante, une mesure ne peut être considérée comme nécessaire qu'en l'absence de toute autre mesure qui serait aussi appropriée tout en étant moins contraignante [56].

54 — Le gouvernement français a fait référence, à cet égard, au rapport du Conseil d'État, *Le numérique et les droits fondamentaux*, 2014, p. 209 et 210. Le Conseil d'État (France) souligne qu'un mécanisme de mesures de surveillance ciblées « serait nettement moins efficace que la conservation systématique du point de vue de la sécurité nationale et de la recherche des auteurs d'infraction. En effet, il ne permettrait aucun accès rétrospectif aux échanges ayant eu lieu avant que l'autorité n'identifie une menace ou une infraction : son caractère opérationnel dépendrait donc de la capacité des autorités à anticiper sur l'identité des personnes dont les données de connexion pourraient être utiles, ce qui est impossible dans le cadre de la police judiciaire. S'agissant par exemple d'un crime, l'autorité judiciaire ne pourrait avoir accès aux communications antérieures à celui-ci, donnée pourtant précieuse et parfois même indispensable pour l'identification de son auteur et de ses complices, comme l'ont montré quelques récentes affaires d'attentats terroristes. Dans le domaine de la prévention des atteintes à la sécurité nationale, les nouveaux programmes techniques reposent sur une capacité de détection des signaux faibles, incompatible avec l'idée du pré-ciblage des personnes dangereuses ».

55 — Commission Staff Working Document présenté en annexe à la proposition de directive ayant conduit à l'adoption de la directive 2006/24, SEC(2005) 1131, 21 septembre 2005, n° 1.2, « The importance of traffic data for law enforcement ».

56 — Voir notamment arrêts du 22 janvier 2013, Sky Österreich (C-283/11, EU:C:2013:28, points 54 à 57) ; du 13 novembre 2014, Reindl (C-443/13, EU:C:2014:2370, point 39), et du 16 juillet 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, points 120 à 122). Au sein de la doctrine, voir notamment Pirker, B., *Proportionality Analysis and Models of Judicial Review*, Europa Law Publishing, Groningen, 2013, p. 29 : « Under a necessity test, the adjudicator examines whether there exists an alternative measure which achieves the same degree of satisfaction for the first value while entailing a lower degree of non-satisfaction of the second value ».

186. L'exigence relative au caractère approprié revient à évaluer l'efficacité « absolue » – indépendamment de toute autre mesure envisageable – d'une obligation générale de conservation de données au regard de la lutte contre les infractions graves. L'exigence de nécessité conduit, quant à elle, à apprécier l'efficience – ou efficacité « relative », c'est-à-dire en comparaison avec toute autre mesure envisageable – d'une telle obligation [57].

187. Dans le contexte des présentes affaires, le test de nécessité impose de vérifier, d'une part, si d'autres mesures pourraient être aussi efficaces qu'une obligation générale de conservation de données dans la lutte contre les infractions graves et, d'autre part, si ces éventuelles mesures sont moins attentatoires aux droits consacrés par la directive 2002/58 et par les articles 7 et 8 de la Charte [58].

188. Je rappelle en outre la jurisprudence constante, rappelée au point 52 de l'arrêt DRI, selon laquelle la protection du droit fondamental à la vie privée exige que les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du « strict nécessaire» [59].

189. Deux problématiques ayant trait à l'exigence de stricte nécessité dans le contexte des présentes affaires ont été amplement débattues par les parties ayant soumis des observations à la Cour, lesquelles correspondent en substance aux deux questions posées par la juridiction de renvoi dans l'affaire C-203/15 :

— d'une part, à la lumière des points 56 à 59 de l'arrêt DRI, une obligation générale de conservation de données doit-elle être considérée comme excédant, en soi, les limites du strictement nécessaire aux fins de la lutte contre les infractions graves, et ce indépendamment d'éventuelles garanties accompagnant cette obligation ?

— d'autre part, à supposer qu'une telle obligation puisse être considérée comme n'excédant pas, en soi, les limites du strictement nécessaire, doit-elle être accompagnée de l'ensemble des garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI en vue de limiter au strict nécessaire l'atteinte aux droits consacrés par la directive 2002/58 et par les articles 7 et 8 de la Charte ?

190. Avant d'aborder ces questions, je crois opportun de rejeter un argument avancé par le gouvernement du Royaume-Uni, selon lequel les critères établis dans l'arrêt DRI seraient dénués de pertinence dans le contexte des présentes affaires, au motif que cet arrêt concernait non pas un régime national mais un régime établi par le législateur de l'Union.

191. À cet égard, je souligne que l'arrêt DRI a interprété les articles 7, 8 et 52, paragraphe 1, de la Charte et que ces dispositions font également l'objet des questions posées dans les litiges au principal. Or, il est, à mon avis, impossible d'interpréter les dispositions de la Charte différemment selon que le régime en cause a été établi au niveau de l'Union ou au niveau national, comme l'ont souligné à juste titre MM. Brice et Lewis ainsi que la Law Society of England and Wales. Lorsqu'il a été constaté que la Charte est applicable, comme c'est le cas dans les présentes affaires [60], celle-ci doit être appliquée de la même façon indépendamment du régime en cause. Partant, les critères dégagés par la Cour dans l'arrêt DRI sont pertinents aux fins d'apprécier les régimes nationaux en cause dans les présentes affaires, comme l'ont notamment fait valoir les gouvernements danois et irlandais ainsi que la Commission.

57 — Voir Rivers, J., « Proportionality and variable intensity of review », 65(1) *Cambridge Law Journal* (2006) 174, p. 198 : « The test of necessity thus expresses the idea of efficiency or Pareto-optimality. A distribution is efficient or Pareto-optimal if no other distribution could make at least one person better off without making any one else worse off. Likewise an act is necessary if no alternative act could make the victim better off in terms of rights-enjoyment without reducing the level of realisation of some other constitutional interest ».

58 — Sur l'existence de ces deux composantes au sein du test de nécessité, voir Barak, A., *Proportionality : Constitutional Rights and their Limitations,* Cambridge University Press, Cambridge, 2012, p. 323 à 331.

59 — Voir notamment arrêts du 9 novembre 2010, Volker und Markus Schecke et Eifert (C-92/09 et C-93/09, EU:C:2010:662, points 77 et 86), et du 7 novembre 2013, IPI (C-473/12, EU:C:2013:715, point 39).

60 — Voir points 117 à 125 des présentes conclusions.

a) Sur le caractère strictement nécessaire d'une obligation générale de conservation de données

192. Selon une première approche, défendue par Tele2 Sverige ainsi que par Open Rights Group et Privacy International, une obligation générale de conservation de données doit, à la suite de l'arrêt DRI, être considérée comme excédant, en soi, les limites de ce qui est strictement nécessaire aux fins de la lutte contre les infractions graves, et ce indépendamment d'éventuelles garanties accompagnant cette obligation.

193. Selon une seconde approche, soutenue par la majorité des autres parties ayant soumis des observations à la Cour, une telle obligation n'excède pas les limites du strictement nécessaire à condition d'être accompagnée de certaines garanties concernant l'accès aux données, la durée de conservation ainsi que la protection et la sécurité des données.

194. Les raisons suivantes me conduisent à adopter cette seconde approche.

195. En premier lieu, selon la lecture que je fais de l'arrêt DRI, la Cour a jugé qu'une obligation générale de conservation de données excède les limites de ce qui est strictement nécessaire lorsqu'elle n'est *pas accompagnée* de garanties strictes concernant l'accès aux données, la durée de conservation ainsi que la protection et la sécurité des données. En revanche, la Cour ne s'est pas prononcée sur la compatibilité avec le droit de l'Union d'une obligation générale de conservation de données qui serait *accompagnée* de telles garanties, dès lors qu'un tel régime ne faisait pas l'objet des questions posées à la Cour dans cette affaire.

196. À cet égard, je souligne que les points 56 à 59 de l'arrêt DRI ne comportent aucune déclaration de la Cour en ce sens qu'une obligation générale de conservation de données excéderait, en soi, les limites du strictement nécessaire.

197. Aux points 56 et 57 de cet arrêt, la Cour constate que l'obligation de conservation prévue par la directive 2006/24 vise l'ensemble des moyens de communication électronique, l'ensemble des utilisateurs 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.

198. Aux points 58 et 59 dudit arrêt, la Cour expose de manière plus détaillée les implications pratiques de cette absence de différenciation. D'une part, cette obligation de conservation concerne même 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. D'autre part, cette 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 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.

199. Ce faisant, la Cour constate qu'une obligation générale de conservation de données se caractérise par son absence de différenciation en fonction de l'objectif de lutte contre les infractions graves. Elle n'a toutefois pas jugé que cette absence de différenciation signifiait qu'une telle obligation excédait, en soi, les limites du strictement nécessaire.

200. En réalité, ce n'est qu'au terme de l'examen du régime prévu par la directive 2006/24, et après avoir constaté l'absence de certaines garanties que j'examinerai ci-après [61], que la Cour juge, au point 69 de l'arrêt DRI :

« *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 » (italique ajouté par mes soins).

201. Comme l'ont fait valoir les gouvernements allemand et néerlandais, si la seule conservation généralisée des données avait suffi à entraîner l'invalidité de la directive 2006/24, la Cour n'aurait pas eu besoin d'examiner, et ce de manière détaillée, l'absence des garanties énoncées aux points 60 à 68 de cet arrêt.

202. Partant, l'obligation générale de conservation de données prévue par la directive 2006/24 n'excédait pas, en soi, les limites du strictement nécessaire. Cette directive excédait les limites du strictement nécessaire en raison de l'*effet combiné* de la conservation généralisée des données et de l'absence de garanties visant à limiter au strict nécessaire l'atteinte aux droits consacrés par les articles 7 et 8 de la Charte. En raison de cet effet combiné, la directive devait être déclarée invalide dans son intégralité [62].

203. En deuxième lieu, je trouve confirmation de cette interprétation au point 93 de l'arrêt Schrems [63], que je reproduis ci-après :

« Ainsi, n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis *sans qu'*aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi *et sans que* soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données [voir en ce sens, en ce qui concerne la directive 2006/24, arrêt DRI, points 57 à 61] » (italique ajouté par mes soins).

204. À nouveau, la Cour n'a pas jugé que le régime en cause dans cette affaire excédait les limites du strict nécessaire au seul motif qu'il autorisait une conservation généralisée de données à caractère personnel. En l'occurrence, les limites du strict nécessaire étaient dépassées en raison de l'effet combiné de la possibilité d'une telle conservation généralisée et de l'absence de garantie concernant l'accès en vue de réduire l'ingérence au strict nécessaire.

205. Je déduis de ce qui précède qu'une obligation générale de conservation de données ne doit pas toujours être considérée comme excédant, en soi, les limites de ce qui est strictement nécessaire aux fins de la lutte contre les infractions graves. En revanche, une telle obligation excède toujours les limites de ce qui est strictement nécessaire lorsqu'elle n'est pas accompagnée de garanties concernant l'accès aux données, la durée de conservation ainsi que la protection et la sécurité des données.

206. En troisième lieu, mon sentiment à cet égard est corroboré par la nécessité de vérifier de manière concrète le respect de l'exigence de stricte nécessité dans le contexte des régimes nationaux en cause dans les litiges au principal.

61 — Voir points 216 à 245 des présentes conclusions.

62 — Voir arrêt DRI, point 65 : « 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 » (italique ajouté par mes soins).

63 — Arrêt du 6 octobre 2015, Schrems (C-362/14, EU:C:2015:650).

207. Comme je l'ai exposé au point 187 des présentes conclusions, l'exigence de stricte nécessité requiert d'examiner si d'autres mesures pourraient être aussi efficaces qu'une obligation générale de conservation de données dans la lutte contre les infractions graves, tout en étant moins attentatoires aux droits consacrés par la directive 2002/58 et par les articles 7 et 8 de la Charte.

208. Or, une telle appréciation doit être réalisée dans le contexte spécifique de chaque régime national prévoyant une obligation générale de conservation de données. D'une part, cette appréciation requiert de comparer l'efficacité de cette obligation avec celle de toute autre mesure envisageable dans le contexte national, en tenant compte du fait que ladite obligation offre aux autorités compétentes une capacité limitée de lire le passé au travers des données conservées [64].

209. Eu égard à l'exigence de stricte nécessité, il est impératif que ces juridictions ne se contentent pas de vérifier la simple utilité d'une obligation générale de conservation de données, mais vérifie strictement qu'aucune autre mesure ou combinaison de mesures, et notamment une obligation ciblée de conservation de données accompagnée d'autres outils d'investigation, ne peut offrir la même efficacité dans la lutte contre les infractions graves. Je souligne à cet égard que plusieurs études portées à l'attention de la Cour remettent en cause la nécessité de ce type d'obligation aux fins de la lutte contre les infractions graves [65].

210. D'autre part, à supposer que d'autres mesures puissent être aussi efficaces dans la lutte contre les infractions graves, il appartiendra encore aux juridictions de renvoi de déterminer si celles-ci sont moins attentatoires aux droits fondamentaux en cause qu'une obligation générale de conservation de données, en application de la jurisprudence constante rappelée au point 185 des présentes conclusions.

211. À la lumière du point 59 de l'arrêt DRI, il incombera aux juridictions nationales de s'interroger, notamment, sur la possibilité de limiter l'étendue matérielle de l'obligation de conservation tout en préservant l'efficacité de cette mesure dans la lutte contre les infractions graves [66]. De telles obligations peuvent en effet avoir une étendue matérielle plus ou moins grande, en fonction des utilisateurs, des zones géographiques et des moyens de communication visés [67].

212. À mes yeux, il serait notamment souhaitable, si la technologie le permet, d'exclure de l'obligation de conservation les données particulièrement sensibles au regard des droits fondamentaux en cause dans les présentes affaires, telles que les données couvertes par le secret professionnel ou encore les données permettant d'identifier les sources des journalistes.

213. Il faut toutefois garder à l'esprit qu'une limitation substantielle de l'étendue d'une obligation générale de conservation de données risque de réduire considérablement l'utilité que présente un tel régime dans la lutte contre les infractions graves. D'une part, plusieurs gouvernements ont souligné la difficulté, voire l'impossibilité de déterminer à l'avance les données qui pourraient présenter un lien avec une infraction grave. Partant, une telle limitation est susceptible d'exclure la conservation de données qui pourraient s'avérer pertinentes pour lutter contre les infractions graves.

64 — Voir points 178 à 183 des présentes conclusions.

65 — Voir commissaire aux droits de l'homme du Conseil de l'Europe, « Issue paper on the rule of law on the Internet and in the wider digital world », décembre 2014, CommDH/IssuePaper(2014)1, p. 115 ; Conseil des droits de l'homme des Nations unies, Rapport du Haut-Commissariat des Nations unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique, 30 juin 2014, A/HRC/27/37, n° 26 ; Assemblée générale des Nations Unies, rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, 23 septembre 2014, A/69/397, n° 18 et 19.

66 — Cette remarque vise uniquement les obligations générales de conservation de données (qui sont susceptibles de viser toute personne indépendamment d'un quelconque lien avec une infraction grave) et non les mesures de surveillance ciblées (lesquelles visent des personnes ayant été préalablement identifiées comme présentant un lien avec une infraction grave) : sur cette distinction, voir points 178 à 183 des présentes conclusions.

67 — Le gouvernement allemand a notamment précisé, lors de l'audience de plaidoiries, que le Parlement allemand a exclu les courriels de l'obligation de conservation imposée par la législation allemande, mais que ce régime couvre l'ensemble des utilisateurs et l'ensemble du territoire national.

214. D'autre part, comme l'a fait valoir le gouvernement estonien, la criminalité grave est un phénomène dynamique, capable de s'adapter aux outils d'investigation dont disposent les autorités de répression. Ainsi, une limitation à une zone géographique ou à un moyen de communication déterminés risquerait de provoquer un déplacement des activités liées aux infractions graves vers une zone géographique et/ou un moyen de communication non couverts par ce régime.

215. Dès lors qu'elle requiert une évaluation complexe des régimes nationaux en cause dans les litiges au principal, j'estime que cette appréciation doit être effectuée par les juridictions nationales, comme l'ont souligné les gouvernements tchèque, estonien, irlandais, français, néerlandais ainsi que la Commission.

b) Sur le caractère impératif des garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI au regard de l'exigence de stricte nécessité

216. À supposer qu'une obligation générale de conservation de données puisse être considérée comme strictement nécessaire dans le contexte du régime national en cause, ce qu'il appartient au juge national d'apprécier, il faut encore déterminer si une telle obligation doit être accompagnée de l'ensemble des garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI en vue de limiter au strict nécessaire l'atteinte aux droits consacrés par la directive 2002/58 et par les articles 7 et 8 de la Charte.

217. Ces garanties concernent les règles régissant l'accès et l'utilisation des données conservées par les autorités compétentes (points 60 à 62 de l'arrêt DRI), la durée de conservation des données (points 63 et 64 de cet arrêt) ainsi que la sécurité et la protection des données conservées par les fournisseurs (points 66 à 68 de cet arrêt).

218. Au sein des observations soumises à la Cour, deux thèses se sont opposées quant à la nature de ces garanties.

219. Selon une première thèse défendue par M. Watson, MM. Brice et Lewis ainsi que par Open Rights Group et Privacy International, les garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI sont impératives. Selon cette thèse, la Cour a établi des garanties minimales devant *toutes* être satisfaites par le régime national en cause afin de limiter l'atteinte aux droits fondamentaux au strict nécessaire.

220. Selon une seconde thèse soutenue par les gouvernements allemand, estonien, irlandais, français et du Royaume-Uni, les garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI sont seulement indicatives. La Cour aurait procédé à une « appréciation d'ensemble » des garanties absentes du régime prévu par la directive 2006/24, sans que l'une de ces garanties puisse, de manière isolée, être considérée comme étant impérative au regard de l'exigence de stricte nécessité. Pour illustrer cette thèse, le gouvernement allemand a évoqué l'image de « vases communicants » en vertu de laquelle une approche plus souple sur l'un des trois aspects identifiés par la Cour (par exemple, l'accès aux données conservées) pourrait être compensée par une approche plus stricte en ce qui concerne les deux autres aspects (la durée de conservation ainsi que la sécurité et la protection des données).

221. J'ai la conviction que cette thèse des « vases communicants » doit être rejetée et que *toutes* les garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI doivent être considérées comme étant impératives, pour les raisons suivantes.

222. En premier lieu, le langage utilisé par la Cour dans son examen de la stricte nécessité du régime établi par la directive 2006/24 ne se prête pas à une telle interprétation. En particulier, la Cour ne fait nulle part allusion, aux points 60 à 68 dudit arrêt, à une quelconque possibilité de « compenser » une approche plus souple sur l'un des trois aspects identifiés par la Cour par une approche plus stricte en ce qui concerne les deux autres aspects.

223. En réalité, la thèse des « vases communicants » me semble procéder d'une confusion entre l'exigence de nécessité et celle de proportionnalité stricto sensu, laquelle n'a pas été examinée par la Cour dans l'arrêt DRI. En effet, comme je l'ai indiqué au point 186 des présentes conclusions, l'exigence de nécessité consiste à rejeter toute mesure inefficiente. Il ne saurait être question, dans ce contexte, d'« appréciation d'ensemble », de « compensation » ou de « mise en balance », procédés qui n'interviennent qu'au stade de la proportionnalité stricto sensu [68].

224. En deuxième lieu, cette thèse des « vases communicants » réduirait à néant l'effet utile des garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI, de sorte que les personnes dont les données ont été conservées ne disposeraient plus 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, comme l'exige le point 54 de cet arrêt.

225. L'effet destructeur de cette thèse peut être aisément illustré à l'aide des exemples suivants. Un régime national restreignant strictement l'accès aux seules fins de la lutte contre le terrorisme et limitant la durée de conservation à trois mois (approche stricte quant à l'accès et à la durée de conservation), mais qui n'obligerait pas les fournisseurs à conserver les données sur son territoire national et sous un format encrypté (approche souple quant à la sécurité), exposerait l'ensemble de sa population à un risque élevé d'accès illégal aux données conservées. De la même façon, un régime national prévoyant une durée de conservation de trois mois ainsi qu'une conservation des données sur son territoire national et sous un format encrypté (approches strictes quant à la durée et la sécurité), mais qui permettrait à tous les employés de toutes les autorités publiques d'accéder aux données conservées (approche souple quant à l'accès), exposerait l'ensemble de sa population à un risque élevé d'abus de la part des autorités nationales.

226. À mes yeux, il découle de ces exemples que la préservation de l'effet utile des garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI exige de considérer *chacune* de celles-ci comme étant impérative. La Cour EDH a également souligné l'importance fondamentale de ces garanties dans le récent arrêt Szabó et Vissy c. Hongrie, en se référant expressément à l'arrêt DRI [69].

227. En troisième lieu, la mise en œuvre de ces garanties, par les États membres souhaitant imposer une obligation générale de conservation de données, ne me semble pas poser de difficultés pratiques majeures. En réalité, ces garanties me semblent à bien des égards « minimales » comme l'a fait valoir M. Watson.

228. Plusieurs de ces garanties ont été débattues devant la Cour en raison de leur possible absence au sein des régimes nationaux en cause dans les affaires au principal.

68 — Voir Barak, A., *Proportionality : Constitutional Rights and their Limitations*, Cambridge University Press, Cambridge, 2012, p. 344 : « The first three components of proportionality deal mainly with the relation between the limiting law's purpose and the means to fulfil that purpose. […] Accordingly, those tests are referred to as means-end analysis. *They are not based on balancing*. The test of proportionality stricto sensu is different. […] It focuses on the relation between the benefit in fulfilling the law's purpose and the harm caused by limiting the constitutional right. *It is based on balancing* » (italique ajouté par mes soins).

69 — Cour EDH, 12 janvier 2016, Szabó et Vissy c. Hongrie, CE:ECHR:2016:0112JUD003713814, §68 : « Indeed, it would defy the purpose of government efforts to keep terrorism at bay, thus restoring citizens' trust in their abilities to maintain public security, if the terrorist threat were paradoxically substituted for by a perceived threat of unfettered executive power intruding into citizens' private spheres by virtue of uncontrolled yet far-reaching surveillance techniques and prerogatives. In this context the Court also refers to the observations made by the Court of Justice of the European Union and, especially, the United Nations Special Rapporteur, emphasising the importance of adequate legislation of sufficient safeguards in the face of the authorities' enhanced technical possibilities to intercept private information ».

229. Premièrement, il ressort des points 61 et 62 de l'arrêt DRI que l'accès et l'utilisation ultérieure des données conservées 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.

230. Selon Tele2 Sverige et la Commission, cette exigence ne serait pas respectée par le régime suédois en cause dans l'affaire C-203/15, lequel permettrait l'accès aux données conservées en vue de la lutte contre des infractions simples. Une critique similaire est émise par MM. Brice et Lewis ainsi que par M. Watson à l'encontre du régime du Royaume-Uni en cause dans l'affaire C-698/15, lequel autoriserait l'accès en vue de la lutte contre des infractions simples et même en l'absence d'infraction.

231. S'il n'appartient pas à la Cour de se prononcer sur la teneur de ces régimes nationaux, il lui revient d'identifier les objectifs d'intérêt général susceptibles de justifier une ingérence grave dans les droits consacrés par la directive et par les articles 7 et 8 de la Charte. En l'occurrence, j'ai déjà exposé les raisons pour lesquelles je considère que *seule* la lutte contre les infractions graves est susceptible de justifier une telle ingérence [70].

232. Deuxièmement, selon le point 62 de l'arrêt DRI, l'accès aux données conservées doit être 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. Ce contrôle préalable doit en outre intervenir à la suite d'une demande motivée de ces autorités présentée dans le cadre de procédures de prévention, de détection ou de poursuites pénales.

233. Selon les observations de Tele2 Sverige et la Commission, cette garantie de contrôle indépendant et préalable à l'accès serait partiellement absente du régime suédois en cause dans l'affaire C-203/15. Le même constat, dont la véracité n'est pas contestée pas le gouvernement du Royaume-Uni, est posé par MM. Brice et Lewis, M. Watson ainsi que par Open Rights Group et Privacy International à l'égard du régime du Royaume-Uni en cause dans l'affaire C-698/15.

234. Je n'aperçois aucun motif d'assouplir cette exigence de contrôle préalable par une entité indépendante, qui résulte incontestablement du langage utilisé par la Cour au point 62 de l'arrêt DRI [71]. Tout d'abord, cette exigence est dictée par la gravité de l'ingérence et des risques engendrés par la constitution de bases de données couvrant la quasi-totalité de la population concernée [72]. Je relève que plusieurs experts en matière de protection des droits de l'homme dans la lutte antiterroriste ont critiqué la tendance actuelle consistant à remplacer les traditionnelles procédures d'autorisation indépendante et de suivi effectif par des systèmes d'« auto-autorisation » d'accès aux données par les services de renseignement et de police [73].

70 — Voir points 170 à 173 des présentes conclusions.

71 — Je précise néanmoins que cette exigence de contrôle préalable et indépendant ne saurait, à mon avis, trouver sa source dans l'article 8, paragraphe 3, de la Charte, dès lors que la Charte n'est pas applicable, en tant que telle, aux dispositions nationales régissant l'accès aux données conservées : voir points 123 à 125 des présentes conclusions.

72 — Voir points 252 à 261 des présentes conclusions.

73 — Conseil des droits de l'homme des Nations unies, rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, 28 décembre 2009, A/HRC/13/37, nº 62 : « [Il] ne doit y avoir aucun système secret de surveillance qui ne soit placé sous la supervision d'une instance de contrôle efficace, ni aucune ingérence qui ne soit autorisée par l'intermédiaire d'un organisme indépendant » (voir également nº 51). Voir également Assemblée générale des Nations unies, rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, 23 septembre 2014, A/69/397, nº 61.

235. Ensuite, un contrôle indépendant et préalable à l'accès aux données est nécessaire en vue de permettre un traitement au cas par cas des données particulièrement sensibles au regard des droits fondamentaux en cause dans les présentes affaires, telles que les données couvertes par le secret professionnel ou encore les données permettant d'identifier les sources des journalistes, comme l'ont souligné la Law Society of England and Wales ainsi que les gouvernements français et allemand. Ce contrôle préalable à l'accès est d'autant plus nécessaire dans l'hypothèse où il est techniquement difficile d'exclure l'ensemble de ces données au stade de la conservation [74].

236. Enfin, j'ajoute que, d'un point de vue pratique, aucune des trois parties concernées par une demande d'accès n'est en mesure d'exercer un contrôle effectif quant à l'accès aux données conservées. Les autorités compétentes en matière répressive ont tout intérêt à demander un accès le plus large possible à ces données. Les fournisseurs, qui n'ont pas connaissance du dossier d'investigation, ne peuvent pas vérifier que la demande d'accès est limitée au strict nécessaire. Quant aux personnes dont les données sont consultées, ils n'ont aucun moyen de savoir qu'ils font l'objet d'une telle mesure d'investigation, et ce même en cas d'utilisation abusive ou illicite comme l'ont souligné M. Watson ainsi que MM. Brice et Lewis. Cette configuration des intérêts en jeu commande, à mes yeux, l'intervention d'une entité indépendante préalablement à la consultation des données conservées, en vue de protéger les personnes dont les données sont conservées de tout accès abusif de la part des autorités compétentes.

237. Cela étant dit, il me semble raisonnable de considérer que des situations ponctuelles d'extrême urgence, évoquées par le gouvernement du Royaume-Uni, peuvent justifier un accès immédiat aux données conservées par les autorités répressives, sans contrôle préalable, en vue de prévenir la commission d'infractions graves ou de poursuivre les auteurs de telles infractions [75]. Dans toute la mesure du possible, il est impératif de maintenir l'exigence d'une autorisation préalable en instaurant une procédure d'urgence au sein de l'entité indépendante en vue du traitement de ce type de demande d'accès. Néanmoins, si le simple fait de saisir cette entité d'une demande d'accès paraît incompatible avec l'extrême urgence de la situation, l'accès et l'utilisation des données devront faire l'objet d'un contrôle a posteriori par cette entité, et ce dans les délais les plus brefs.

238. Troisièmement, le point 68 de l'arrêt DRI établit une obligation, à la charge des fournisseurs, de conserver les données sur le territoire de l'Union, afin de garantir le contrôle par une autorité indépendante, exigé par l'article 8, paragraphe 3, de la Charte, du respect des exigences de protection et de sécurité énoncées aux points 66 et 67 de cet arrêt.

239. Tele2 Sverige et la Commission ont fait valoir que la conservation des données sur le territoire national ne serait pas garantie dans le cadre du régime suédois en cause dans l'affaire C-203/15. La même critique est avancée par MM. Brice et Lewis ainsi que par M. Watson à l'encontre du régime du Royaume-Uni en cause dans l'affaire C-698/15.

240. À cet égard, d'une part, je ne vois aucune raison d'affaiblir cette exigence établie au point 68 de l'arrêt DRI, dès lors qu'une conservation des données en dehors du territoire de l'Union ne permettrait pas de garantir aux personnes dont les données sont conservées le niveau de protection offert par la directive 2002/58 et par les articles 7, 8 et 52, paragraphe 1, de la Charte [76].

74 — Voir point 212 des présentes conclusions. En ce qui concerne les sources des journalistes, la Cour EDH a souligné la nécessité d'une autorisation préalable par une entité indépendante, dans la mesure où un contrôle a posteriori ne permet pas de restaurer la confidentialité de telles sources : voir Cour EDH, 22 novembre 2012, Telegraaf Media Nederland Landelijke Media B.V. et Autres c. Pays-Bas, CE:ECHR:2012:1122JUD003931506, § 101, et Cour EDH, 12 janvier 2016, Szabó et Vissy c. Hongrie, CE:ECHR:2016:0112JUD003713814, §77. Dans l'arrêt Kopp c. Suisse, qui concernait la surveillance des lignes téléphoniques d'un avocat, la Cour EDH a critiqué le fait qu'un fonctionnaire appartenant à l'administration soit chargé, sans contrôle par un magistrat indépendant, de filtrer les informations couvertes par le secret professionnel : voir Cour EDH, 25 mars 1998, Kopp c. Suisse, CE:ECHR:1998:0325JUD002322494, § 74.

75 — Voir, à cet égard, le mécanisme décrit au point 22 des présentes conclusions. Je souligne que cette problématique n'a pas été abordée par la Cour dans l'arrêt DRI.

76 — Voir, à cet égard, arrêt du 6 octobre 2015, Schrems (C-362/14, EU:C:2015:650).

241. Il me semble raisonnable, d'autre part, d'adapter cette exigence, exprimée par la Cour dans le contexte de la directive 2006/24, au contexte de régimes nationaux en prévoyant la conservation des données sur le territoire national, comme l'ont fait valoir les gouvernements allemand et français ainsi que la Commission. En effet, en vertu de l'article 8, paragraphe 3, de la Charte, il incombe à chaque État membre de garantir le contrôle, par une autorité indépendante, du respect des exigences de protection et de sécurité par les fournisseurs visés par son régime national. Or, en l'absence de coordination au niveau de l'Union, une telle autorité nationale pourrait se trouver dans l'impossibilité de mener à bien ses missions de contrôle sur le territoire d'un autre État membre.

242. Quatrièmement, en ce qui concerne la durée de conservation, les juridictions de renvoi devront faire application des critères définis par la Cour aux points 63 et 64 de l'arrêt DRI. D'une part, ces juridictions doivent déterminer si les données conservées peuvent être distinguées en fonction de leur utilité et, le cas échéant, si la durée de conservation a été adaptée en fonction de ce critère. D'autre part, lesdites juridictions doivent vérifier que la durée de conservation est fondée sur des critères objectifs permettant de garantir que celle-ci est limitée au strict nécessaire.

243. Je souligne que la Cour EDH, dans le récent arrêt Roman Zakharov c. Russie, a jugé raisonnable une durée maximale de conservation de six mois, tout en déplorant l'absence d'obligation de détruire sur le champ les données qui n'ont pas de rapport avec le but pour lequel elles ont été recueillies [77]. J'ajoute, à cet égard, que les régimes nationaux en cause dans les litiges au principal doivent prévoir une obligation de détruire irrémédiablement toute donnée conservée dès qu'elle n'est plus strictement nécessaire à la lutte contre des infractions graves. Cette obligation doit être respectée non seulement par les fournisseurs qui procèdent à la conservation des données, mais également par les autorités ayant eu accès à des données conservées.

244. Eu égard aux considérations qui précèdent, j'estime que toutes les garanties énoncées par la Cour aux points 60 à 68 de l'arrêt DRI présentent un caractère impératif et doivent, par conséquent, accompagner une obligation générale de conservation de données en vue de limiter au strict nécessaire l'atteinte aux droits consacrés par la directive 2002/58 et par les articles 7 et 8 de la Charte.

245. Il appartient aux juridictions de renvoi de vérifier que les régimes nationaux en cause dans les litiges au principal comportent chacune de ces garanties.

6. Sur le caractère proportionné, dans une société démocratique, d'une obligation générale de conservation de données au regard de l'objectif de lutte contre les infractions graves

246. Après avoir vérifié le caractère nécessaire des régimes nationaux en cause dans les affaires au principal, il incombera encore aux juridictions de renvoi d'en vérifier le caractère proportionné, dans une société démocratique, au regard de l'objectif de lutte contre les infractions graves. Cet aspect n'a pas été examiné par la Cour dans l'arrêt DRI étant donné que le régime établi par la directive 2006/24 excédait les limites de ce qui est strictement nécessaire aux fins de la lutte contre les infractions graves.

77 — Voir, à cet égard, Cour EDH, 4 décembre 2015, Roman Zakharov c. Russie, CE:ECHR:2015:1204JUD004714306, § 254 et 255. Selon le droit russe, la destruction des éléments interceptés devait intervenir au terme d'un délai de six mois de conservation si la personne concernée n'avait pas été inculpée d'une infraction pénale. La Cour EDH a jugé raisonnable la durée maximale de conservation, à savoir six mois, fixée par le droit russe pour de telles données. Elle a toutefois déploré l'absence d'obligation de détruire sur le champ les données qui n'ont pas de rapport avec le but pour lequel elles ont été recueillies, précisant que la conservation automatique, six mois durant, de données manifestement dénuées d'intérêt ne saurait passer pour justifiée au regard de l'article 8 de la CEDH.

247. Cette exigence de proportionnalité dans une société démocratique – ou proportionnalité « stricto sensu » – découle à la fois de l'article 15, paragraphe 1, de la directive 2002/58, de l'article 52, paragraphe 1, de la Charte et d'une jurisprudence constante. Selon cette jurisprudence constante, une mesure portant atteinte à des droits fondamentaux ne peut être considérée comme proportionnée que si les inconvénients causés ne sont pas démesurés par rapport aux buts visés [78].

248. À la différence des exigences relatives au caractère approprié et nécessaire de la mesure en cause, lesquelles évaluent son efficacité au regard de l'objectif poursuivi, l'exigence de proportionnalité stricto sensu consiste à mettre en balance, d'une part, les avantages résultant de cette mesure au regard de l'objectif légitime poursuivi avec, d'autre part, les inconvénients en découlant au regard des droits fondamentaux consacrés dans une société démocratique [79]. Cette exigence ouvre ainsi un débat sur les valeurs devant prévaloir dans une société démocratique et, en définitive, sur le type de société dans lequel nous souhaitons vivre [80].

249. Par conséquent, et comme je l'ai indiqué au point 223 des présentes conclusions, c'est au stade de l'examen de la proportionnalité au sens strict qu'il convient de procéder à une appréciation d'ensemble du régime en cause, et non au stade de l'examen de nécessité comme l'ont fait valoir les partisans de la thèse des « vases communicants» [81].

250. En application de la jurisprudence rappelée au point 247 des présentes conclusions, il y a lieu de mettre en balance les avantages et les inconvénients, dans une société démocratique, d'une obligation générale de conservation de données. Ces avantages et ces inconvénients sont intimement liés à la caractéristique essentielle d'une telle obligation, dont ils représentent en quelque sorte la face claire et la face sombre, à savoir le fait qu'elle vise l'ensemble des communications réalisées par l'ensemble des utilisateurs sans que ne soit exigé un quelconque lien avec une infraction grave.

251. D'une part, j'ai déjà exposé aux points 178 à 183 des présentes conclusions les avantages que procure, dans la lutte contre les infractions graves, la conservation des données relatives à l'ensemble des communications réalisées sur le territoire national.

252. D'autre part, les inconvénients d'une obligation générale de conservation de données découlent du fait que l'immense majorité des données conservées concernent des personnes qui ne présenteront jamais aucun lien avec une infraction grave. Il est important, à cet égard, de préciser la nature des inconvénients qui affecteront ces personnes. Or, ces inconvénients sont de natures différentes en fonction du niveau d'ingérence dans leurs droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel.

78 — Voir, notamment, arrêts du 15 février 2016, N. (C-601/15 PPU, EU:C:2016:84, point 54 ; le caractère nécessaire est examiné aux points 56 à 67, le caractère proportionné aux points 68 et 69) ; du 16 juillet 2015, CHEZ Razpredelenie Bulgaria (C-83/14, EU:C:2015:480, point 123 ; le caractère nécessaire est examiné aux points 120 à 122, le caractère proportionné aux points 123 à 127), et du 22 janvier 2013, Sky Österreich (C-283/11, EU:C:2013:28, point 50 ; le caractère nécessaire est examiné aux points 54 à 57, le caractère proportionné aux points 58 à 67).

79 — Voir Rivers J., « Proportionality and variable intensity of review », 65(1) *Cambridge Law Journal* (2006) 174, p. 198 : « It is vital to realise that the test of balance has a totally different function from the test of necessity. The test of necessity rules out inefficient human rights limitations. It filters out cases in which the same level of realisation of a legitimate aim could be achieved at less cost to rights. By contrast, the test of balance is strongly evaluative. It asks whether the combination of certain levels of rights-enjoyment combined with the achievement of other interests is good or acceptable ».

80 — Voir Pirker B., *Proportionality Analysis and Models of Judicial Review,* Europa Law Publishing, Groningen, 2013, p. 30 : « In its simple form, one could state that proportionality *stricto sensu* leads to a weighing between competing values to assess which value should prevail ».

81 — La spécificité de l'exigence de proportionnalité stricto sensu, par rapport aux exigences de caractère approprié et nécessaire, peut être illustrée par l'exemple suivant. Imaginons qu'un État membre impose l'injection d'une puce électronique de géolocalisation à toute personne résidant sur son territoire, cette puce permettant aux autorités de retracer les allées et venues de son porteur au cours de l'année écoulée. Une telle mesure pourrait être considérée comme étant « nécessaire » si aucune autre mesure ne permet d'atteindre le même degré d'efficacité dans la lutte contre les infractions graves. Cependant, à mes yeux, une telle mesure serait disproportionnée dans une société démocratique, étant donné que les inconvénients résultant de l'atteinte aux droits à l'intégrité physique, au respect de la vie privé et à la protection des données à caractère personnel seraient démesurés par rapport aux avantages en découlant dans la lutte contre les infractions graves.

253. Dans le cadre d'une ingérence « individuelle », affectant un individu déterminé, les inconvénients résultant d'une obligation générale de conservation de données ont été décrits avec une grande acuité par M. l'avocat général Cruz Villalón aux points 72 à 74 de ses conclusions dans l'affaire DRI [82]. Pour reprendre les termes utilisés par celui-ci, l'exploitation de ces données rend possible « l'établissement d'une cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voire d'un portrait complet et précis de son identité privée ».

254. En d'autres termes, dans un contexte individuel, une obligation générale de conservation de données permet des ingérences aussi graves que des mesures de surveillance ciblées, en ce compris celles interceptant le contenu des communications effectuées.

255. Si la gravité de telles ingérences individuelles ne peut être sous-estimée, il me semble néanmoins que les risques spécifiques engendrés par une obligation générale de conservation de données se révèlent dans le contexte d'ingérences « de masse ».

256. En effet, à la différence de mesures de surveillance ciblées, une telle obligation est susceptible de faciliter considérablement les ingérences de masse, c'est-à-dire les ingérences affectant une partie substantielle ou même l'ensemble de la population pertinente, ce qui peut être illustré à l'aide des exemples suivants.

257. Supposons, en premier lieu, qu'une personne ayant accès aux données conservées ait l'intention d'identifier, au sein de la population de l'État membre, tous les individus atteints de troubles d'ordre psychologique. L'analyse, à cette fin, du contenu de l'ensemble des communications réalisées sur le territoire national exigerait des ressources considérables. En revanche, l'exploitation des bases de données relatives aux communications permettrait d'identifier instantanément tous les individus ayant contacté un psychologue au cours de la période de conservation des données [83]. J'ajoute que cette technique pourrait être étendue à chacune des spécialités médicales enregistrées dans un État membre [84].

258. Supposons, en second lieu, que cette même personne souhaite identifier les individus opposés à la politique du gouvernement en place. À nouveau, l'analyse, à cette fin, du contenu des communications exigerait des ressources considérables. En revanche, l'exploitation des données relatives aux communications permettrait d'identifier tous les individus inscrits à des listes de distribution de courriels critiquant la politique du gouvernement. En outre, ces données permettraient également d'identifier les individus participant à toute manifestation publique d'opposition au gouvernement [85].

82 — C-293/12 et C-594/12, EU:C:2013:845. Voir également arrêt DRI (points 27 et 37).

83 — Les données conservées incluent en effet l'identité de la source et du destinataire d'une communication, données qu'il suffirait de croiser avec la liste des numéros de téléphones des psychologues opérant sur le territoire national.

84 — Voir, à cet égard, Conseil des droits de l'homme des Nations unies, rapport du rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, 28 décembre 2009, A/HRC/13/37, nº 42 : « [E]n Allemagne, des études ont signalé une conséquence inquiétante des politiques de conservation des données : 52 % des personnes interrogées ont indiqué qu'il était peu probable qu'elles utiliseraient les télécommunications pour se mettre en relation avec un toxicologue, un psychothérapeute ou un conseiller conjugal en raison des lois sur la conservation des données ».

85 — Dès lors que les données conservées incluent la localisation de la source et du destinataire d'une communication, toute personne initiant ou recevant une communication lors d'une manifestation pourra être aisément identifiée grâce aux données conservées. À cet égard, Marc Goodman, expert auprès du FBI et d'Interpol dans le domaine des risques liés aux nouvelles technologies, relate que, dans un passé récent, le gouvernement ukrainien a procédé, lors d'une manifestation de l'opposition, à l'identification de tous les téléphones portables localisés à proximité d'affrontements de rue entre les forces de l'ordre et les opposants au gouvernement. L'ensemble de ces téléphones reçut alors un message que l'auteur décrit comme étant possiblement le message le plus « orwellien » jamais envoyé par un gouvernement : « Cher abonné, vous êtes enregistré en tant que participant à un trouble grave de l'ordre public » (Goodman, M., *Future Crimes,* Anchor Books, New York, 2016, p. 153, traduction libre). Voir également Conseil des droits de l'homme des Nations unies, rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, 17 avril 2013, A/HRC/23/40, nº 75, et Conseil des droits de l'homme des Nations unies, rapport du Haut-Commissariat des Nations unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique, 30 juin 2014, A/HRC/27/37, nº 3.

259. Je tiens à souligner que les risques liés à l'accès aux données relatives aux communications (ou « métadonnées ») peuvent être équivalents, voire supérieurs à ceux résultant de l'accès au contenu de ces communications, comme l'ont souligné Open Rights Group et Privacy International, la Law Society of England and Wales ainsi qu'un récent rapport du Haut-Commissariat des Nations unies aux droits de l'homme [86]. En particulier, et comme le montrent les exemples précités, les « métadonnées » permettent un catalogage presque instantané d'une population dans son entièreté, ce que ne permet pas le contenu des communications.

260. J'ajoute que les risques d'accès abusif ou illégal aux données conservées n'ont rien de théorique. D'une part, le risque d'accès abusif par les autorités compétentes doit être mis en rapport avec les nombres extrêmement élevés de demandes d'accès évoqués dans les observations soumises à la Cour. Dans le contexte du régime suédois, Tele2 Sverige a indiqué qu'elle recevait environ 10 000 demandes d'accès par mois, nombre qui n'inclut pas les demandes reçues par d'autres fournisseurs actifs sur le territoire suédois. En ce qui concerne le régime du Royaume-Uni, M. Watson a reproduit des nombres extraits d'un rapport officiel faisant état de 517 236 autorisations et de 55 346 autorisations orales urgentes pour la seule année 2014. D'autre part, le risque d'accès illégal, par toute personne, est consubstantiel à l'existence même de bases de données conservées sur des supports informatiques [87].

261. Il appartient, selon moi, aux juridictions de renvoi d'apprécier si les inconvénients causés par les obligations générales de conservation de données en cause dans les litiges au principal ne sont pas démesurés, dans une société démocratique, par rapport aux buts visés, en application de la jurisprudence rappelée au point 247 des présentes conclusions. Dans le cadre de cette appréciation, ces juridictions devront mettre en balance les risques et avantages liés à une telle obligation, à savoir :

— d'une part, les avantages liés à l'octroi d'une capacité limitée de lire le passé aux autorités chargées de lutter contre les infractions graves [88] et,

— d'autre part, les graves risques résultant, dans une société démocratique, du pouvoir de cartographie de la vie privée d'un individu et du pouvoir de catalogage d'une population dans son entièreté.

262. Cette appréciation doit se faire au regard de toutes les caractéristiques pertinentes des régimes nationaux en cause dans les litiges au principal. Je souligne, à cet égard, que les garanties impératives énoncées par la Cour aux points 60 à 68 de l'arrêt DRI ne constituent que des garanties minimales en vue de limiter au strict nécessaire l'atteinte aux droits consacrés par la directive 2002/58 et par les articles 7 et 8 de la Charte. Il n'est, par conséquent, pas exclu qu'un régime national comportant l'ensemble de ces garanties doive néanmoins être considéré comme disproportionné au sein d'une société démocratique, en raison de la disproportion entre les graves risques engendrés par cette obligation dans une société démocratique et les avantages en découlant dans la lutte contre les infractions graves.

86 — Voir, à cet égard, Conseil des droits de l'homme des Nations Unies, Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme sur le droit à la vie privée à l'ère du numérique, 30 juin 2014, A/HRC/27/37, n° 19 : « Dans le même ordre d'idées, d'aucuns soutiennent que l'interception - ou la collecte - de données sur une communication, et non plus sur le contenu de la communication, ne constitue pas à elle seule une immixtion dans la vie privée. Or du point de vue du droit à la vie privée, cette distinction n'est pas convaincante. Les agrégations d'informations communément appelées 'métadonnées' peuvent donner des indications sur la conduite d'un individu, ses relations sociales, ses préférences privées et son identité *qui vont bien au-delà de ce que l'on obtient en accédant au contenu* d'une communication privée » (italique ajouté par mes soins). Voir également Assemblée générale des Nations Unies, Rapport du Rapporteur spécial sur la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte antiterroriste, 23 septembre 2014, A/69/397, n° 53.

87 — Voir, notamment, Conseil des droits de l'homme des Nations unies, rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, 17 avril 2013, A/HRC/23/40, n° 67 : « Les bases des données de communications deviennent vulnérables au vol, à la fraude et à la divulgation accidentelle ».

88 — Voir points 178 à 183 des présentes conclusions.

VI – Conclusion

263. Eu égard à ce qui précède, je propose à la Cour de répondre comme suit aux questions préjudicielles du Kammarrätten i Stockholm (cour administrative d'appel de Stockholm, Suède) et de la Court of Appeal (England & Wales) (Civil Division) [Cour d'appel (Angleterre et pays de Galles) (division civile), Royaume-Uni] :

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, ainsi que les articles 7, 8 et 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne doivent être interprétés en ce sens qu'ils ne s'opposent pas à ce qu'un État membre impose aux fournisseurs de services de communications électroniques une obligation de conserver l'ensemble des données relatives aux communications réalisées par les utilisateurs de leurs services lorsque toutes les conditions suivantes sont satisfaites, ce qu'il appartient aux juridictions de renvoi de vérifier à la lumière de toutes les caractéristiques pertinentes des régimes nationaux en cause dans les litiges au principal :

— cette obligation et les garanties accompagnant celle-ci doivent être prévues par des mesures législatives ou réglementaires possédant les qualités d'accessibilité, de prévisibilité et de protection adéquate contre l'arbitraire ;

— cette obligation et les garanties accompagnant celle-ci doivent respecter le contenu essentiel des droits reconnus par les articles 7 et 8 de la charte des droits fondamentaux ;

— cette obligation doit être strictement nécessaire à la lutte contre les infractions graves, ce qui implique qu'aucune autre mesure ou combinaison de mesures ne pourrait être aussi efficace dans la lutte contre les infractions graves tout en étant moins attentatoire aux droits consacrés par la directive 2002/58 et par les articles 7 et 8 de la charte des droits fondamentaux ;

— cette obligation doit être accompagnée de toutes les garanties énoncées par la Cour aux points 60 à 68 de l'arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, EU:C:2014:238) concernant l'accès aux données, la durée de conservation ainsi que la protection et la sécurité des données, en vue de limiter au strict nécessaire l'atteinte aux droits consacrés par la directive 2002/58 et par les articles 7 et 8 de la charte des droits fondamentaux, et

— cette obligation doit être proportionnée, dans une société démocratique, à l'objectif de lutte contre les infractions graves, ce qui implique que les graves risques engendrés par cette obligation dans une société démocratique ne doivent pas être démesurés par rapport aux avantages en découlant dans la lutte contre les infractions graves.