COMMISSION EUROPÉENNE

Bruxelles, le 9 février 2018
sj.f(2018)865066

TRAD: FR - OR: EN

Document de procédure juridictionnelle

À MONSIEUR LE PRÉSIDENT ET AUX MEMBRES DE LA COUR DE JUSTICE

OBSERVATIONS ÉCRITES

déposées, conformément à l'article 23 du statut de la Cour de justice,

par la Commission européenne, représentée par M. Martin WASMEIER, Mme Piedade COSTA DE OLIVEIRA, M. Herke KRANENBORG et M. Daniele NARDI, en qualité d'agents, ayant élu domicile à Bruxelles, auprès du Service juridique, Greffe Contentieux, BERL 1/169, 1049 Bruxelles, et consentant à la signification de tout acte de procédure via par e-Curia,

dans l'affaire C-623/17

ayant pour objet le renvoi à la Cour, conformément à l'article 267 TFUE, par l'Investigatory Powers Tribunal of the United Kingdom, d'une demande de décision préjudicielle dans le cadre du litige pendant devant cette juridiction entre

Privacy International

(partie requérante au principal)

et

1) Secretary of State for Foreign and Commonwealth Affairs
2) Secretary of State for the Home Department
3) Government Communications Headquarters
4) Security Service
5) Secret Intelligence Service

(parties défenderesses au principal),

sur l'interprétation de l'article 4, paragraphe 2, du TUE et des articles 1er, paragraphe 3 et 15, paragraphe 1, de la directive 2002/58/CE.

Table des matières

LA COMMISSION A L'HONNEUR DE PRESENTER LES OBSERVATIONS SUIVANTES.

1. CADRE JURIDIQUE

1.1. Droit de l'Union européenne

1. La demande de décision préjudicielle porte sur l'interprétation de l'article 4, paragraphe 2, TUE ainsi que de l'article 1er, paragraphe 3, et de l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO L 201 du 31.7.2002, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 (JO L 337 du 18.12.2009, p. 11) (ci-après la «directive 2002/58/CE»).

2. L'article 4, paragraphe 2, TUE est libellé comme suit:

> «[…]
>
> 2. L'Union respecte l'égalité des États membres devant les traités ainsi que leur identité nationale, inhérente à leurs structures fondamentales politiques et constitutionnelles, y compris en ce qui concerne l'autonomie locale et régionale. Elle respecte les fonctions essentielles de l'État, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre public et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque État membre.
>
> […]»

3. L'article 1er de la directive 2002/58/CE, intitulé «Champ d'application et objectif », dispose ce qui suit:

> «1. La présente directive prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et services de communications électroniques dans la Communauté.
>
> 2. Les dispositions de la présente directive précisent et complètent la directive 95/46/CE aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.
>
> 3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris

la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal.»

4. L'article 5 de la directive 2002/58/CE, intitulé «Confidentialité des communications», est libellé comme suit:

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

[…]

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

5. L'article 6 de la directive 2002/58/CE, intitulé «Données relatives au trafic», dispose ce qui suit:

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

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

3. Afin de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d'un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1 dans la mesure et pour la durée nécessaires à la fourniture ou à la

commercialisation de ces services, pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.

[…]

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

6. L'article 15 de la même directive, intitulé «Application de certaines dispositions de la directive 95/46/CE», prévoit que:

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

[…]

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

[…]»

1.2. Législation nationale

7. L'article 94 du Telecommunications Act 1984, la loi britannique de 1984 sur les télécommunications (ci-après le «1984 Act») dispose :

«Instructions dans l'intérêt de la sécurité nationale, etc.

1) Le Secretary of State peut, après la consultation d'une personne à laquelle s'applique le présent article, donner à cette personne des instructions de caractère général, dans la mesure de ce qui, aux yeux du ministre, est [nécessaire] dans l'intérêt de la sécurité nationale ou des relations entretenues avec le gouvernement d'un pays ou territoire situé en dehors du Royaume-Uni.

2) S'il apparaît [nécessaire] au Secretary of State de procéder ainsi dans l'intérêt de la sécurité nationale ou des relations entretenues avec le gouvernement d'un pays ou territoire situé en dehors du Royaume-Uni, il peut, après la consultation d'une personne à laquelle s'applique le présent article, donner à cette personne des instructions lui demandant (selon les circonstances de l'espèce) d'exécuter ou de ne pas exécuter une action particulière spécifiée dans les instructions.

[2 *bis*) Le Secretary of State ne peut donner d'instructions au titre du paragraphe 1) ou 2) que s'il estime que le comportement requis par les instructions est proportionné à l'objectif à atteindre au moyen de ce comportement.]

3) La personne à laquelle s'applique le présent article doit mettre en œuvre toutes les instructions qui lui sont données par le Secretary of State au titre du présent article, nonobstant toute autre obligation qui lui incombe en vertu de [la partie 1 ou de la partie 2, chapitre 1, du Communications Act 2003 (loi de 2003 sur les communications) et, dans le cas d'instructions données au fournisseur d'un réseau public de communications électroniques, même si lesdites instructions s'appliquent à lui au titre d'une qualité autre que celle de fournisseur d'accès à un tel réseau].

4) Le Secretary of State dépose auprès de chacune des chambres du Parlement une copie de toutes instructions données en vertu du présent article, sauf s'il estime que la divulgation desdites instructions serait contraire aux intérêts de la sécurité nationale ou des relations entretenues avec le gouvernement d'un pays ou territoire situé en dehors du Royaume-Uni, ou aux intérêts commerciaux d'une personne.

5) Une personne ne doit pas divulguer, ou ne saurait être tenue de divulguer, en vertu d'une loi ou autre, de quelconques informations concernant des mesures prises conformément au présent article si le Secretary of State lui a notifié qu'il était d'avis que la divulgation de ces informations serait contraire aux intérêts de la sécurité nationale ou des relations entretenues avec le gouvernement d'un pays ou territoire situé en dehors du Royaume-Uni, ou aux intérêts commerciaux d'une autre personne.

6) Le Secretary of State peut, avec l'accord du Treasury, verser des indemnités [aux fournisseurs de réseaux publics de communications électroniques] afin de rembourser ou de prendre en charge les pertes éventuelles subies par lesdits fournisseurs d'accès du fait qu'ils se conforment aux instructions données en vertu du présent article.

7) Toute somme requise par le Secretary of State en vue de verser des indemnités en vertu du présent article devrat être payée au moyen de fonds mis à disposition par le Parlement.

8) Le présent article s'applique à [l'OFCOM et à des fournisseurs de réseaux publics de communications électroniques.]»

Le texte intégral de l'article 94, y compris les notes de bas de page relatives aux parties entre crochets, peuvent être consultés à **l'annexe A.3**.

2. FAITS DU LITIGE AU PRINCIPAL ET QUESTIONS PRÉJUDICIELLES

8. Les faits du litige au principal peuvent être résumés comme suit. Pour une description plus détaillée des faits, nous renvoyons à l'ordonnance de renvoi (notamment aux points 6 à 22) ainsi qu'aux deux arrêts rendus par l'Investigatory Powers Tribunal (ci-après la «juridiction de renvoi»), respectivement le 17 octobre 2016 et le 8 septembre 2017 (voir **les annexes A.1** et **A.2**).

9. En vertu de l'article 94 du 1984 Act, le Secretary of State du Royaume-Uni peut, après avoir consulté un opérateur de réseau public de communications électroniques (RPCE), donner à cet opérateur des instructions générales ou spécifiques qui lui semblent nécessaires dans l'intérêt de la sécurité nationale ou des relations entretenues avec un gouvernement étranger.

10. Sur la base des instructions formulées par le Secretary of State (voir les exemples à **l'annexe A.4**), les services de sécurité et de renseignement du Royaume-Uni acquièrent des données de communication en masse (DCM) des opérateurs de RPCE. Ces services de sécurité et de renseignement (ci-après les «SSR») sont le Government Communications Headquarters (GCHQ), le Security Service (MI5) et le Secret Intelligence Service (MI6). Le GCHQ acquiert des DCM depuis 2001 et le MI5 depuis 2005. Le MI6 ne collecte ni ne détient de telles données (voir l'ordonnance de la juridiction de renvoi du 17 octobre 2016, **annexe A.1**, point 19, p. 10).

11. Les DCM sont des données à caractère personnel non ciblées détenues par les opérateurs de RPCE et comprennent les données relatives au trafic et les informations sur les services utilisés (le «qui, où, quand, comment» d'une communication), mais pas le contenu des communications[1]. Les opérateurs de RPCE ne sont pas tenus de conserver les DCM après leur transmission aux SSR.

12. Une fois qu'ils ont reçu les DCM, les SSR conservent les données et les exploitent au moyen de techniques qui sont majoritairement non ciblées, c'est-à-dire qu'elles ne ciblent pas un objet spécifique et connu (voir le point 20 de l'ordonnance de renvoi). Cette absence de caractère ciblé constitue un élément fondamental des

---

[1] Les notions de «données relatives au trafic» et d'«informations sur les services utilisés» sont définies à l'article 21, paragraphe 4, du Regulation of Investigatory Powers Act 2000 (règlement relatif aux pouvoirs d'enquête de 2000), voir le point 3.5.1, p. 44 de l'arrêt de la juridiction de renvoi du 17 octobre 2016, à **l'annexe A.1**.

techniques employées par les SSR pour exploiter les DCM. Selon la juridiction de renvoi, qui se fonde sur un rapport publié en 2016 par le conseiller de la reine David Anderson (ci-après le «rapport Anderson»), seule une «quantité minuscule» des données recueillies est examinée (voir le point 20 de l'ordonnance de renvoi).

13. La requérante dans la procédure devant la juridiction de renvoi soutient que l'acquisition de DCM (ainsi que l'accès à celles-ci et leur utilisation) est illégale en vertu du droit de l'Union, en particulier à la lumière de l'arrêt *Tele2/Watson* de la Cour de justice du 21 décembre 2016 (affaires C-203/15 et C-698/15, *Tele2 Sverige AB/ Post- och telestyrelsen* et *Secretary of State for the Home Department / Watson e. a.*, ECLI:EU:C:2016:970).

14. Dans l'arrêt *Tele2/Watson*, la Cour de justice a conclu que la législation nationale imposant aux opérateurs de télécommunications de conserver les données relatives au trafic et les données de localisation et définissant les conditions d'accès à ces données par les autorités compétentes dans le but de lutter contre la criminalité relevait du champ d'application de la directive 2002/58/CE. La Cour a défini les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données conservées (voir les points 118 et suivants de l'arrêt *Tele2/Watson*).

15. Les parties défenderesses dans la procédure nationale font essentiellement valoir que la jurisprudence *Tele2/Watson* concerne la législation nationale visant à lutter contre la criminalité, qui est différente de la mesure nationale en cause prise à des fins de sécurité nationale. Selon les défenderesses, la présente affaire requiert une analyse différente et doit, eu égard à l'article 4, paragraphe 2, TUE, être considérée comme ne relevant pas du champ d'application de la directive 2002/58/CE.

16. Comme l'affaire concerne l'interprétation du droit de l'Union, la juridiction de renvoi a décidé de soumettre deux questions à la Cour de justice. Toutefois, avant de formuler ces questions, la juridiction de renvoi énumère les circonstances à l'aune desquelles, selon elle, la question devrait être examinée par la Cour de justice:

> «*a. les capacités des SSR pour utiliser les DCM qui leur sont fournies sont essentielles pour la protection de la sécurité nationale du Royaume-Uni, notamment dans les domaines du contreterrorisme, du contre-espionnage et de la lutte contre la prolifération nucléaire ;*

b. une caractéristique fondamentale de l'utilisation des DCM par les SSR est la découverte de menaces pour la sécurité nationale inconnues jusque-là par le biais de techniques de masse non-ciblées qui exigent le regroupement des DCM en un endroit unique. Son utilité principale repose dans l'identification et l'établissement rapide des cibles ainsi que la fourniture d'une base d'action au vu d'une menace imminente;

c. le fournisseur d'un réseau de communications électroniques n'est pas tenu de conserver par la suite les DCM (au-delà de la période requise par l'activité commerciale ordinaire) qui sont conservées par l'État seul (les SSR);

d. la juridiction nationale a jugé (sous réserve de certaines questions réservées) que les garanties entourant l'utilisation des DCM par les SSR sont conformes aux exigences de la CEDH; et

e. la juridiction nationale a jugé que l'imposition des exigences spécifiées aux points 119 à 125 de l'arrêt [Tele2/Watson de la Cour de Justice*], si ces dernières étaient applicables, ferait échec aux mesures prises par les SSR pour protéger la sécurité nationale et mettrait par là même en péril la sécurité nationale du Royaume-Uni.*»

17. Les «questions réservées» visées au point d concernent la proportionnalité de la mesure et les accords relatifs au transfert de données à des tiers (voir le paragraphe 3 de l'arrêt de la juridiction de renvoi du 8 septembre 2017, à **l'annexe A.2**).

18. Les deux questions déférées à la Cour de justice sont les suivantes:

«1. *Vus l'article 4 TUE et l'article 1er, paragraphe 3, de la directive 2002/58/CE (directive vie privée et communications électroniques), une exigence dans des instructions données par le Secretary of State à un fournisseur d'un réseau de communications électroniques qu'il doit fournir les données de communications en masse aux services de sécurité et de renseignement («SSR») d'un État membre, relève-t-elle du champ d'application du droit de l'Union et de la directive vie privée et communications électroniques?*

2. *En cas de réponse affirmative à la première question, les exigences Watson ou toute autre exigence en plus de celles imposées par la CEDH s'imposent-elles à de telles instructions du Secretary of State? Si tel est le cas, comment et dans quelle mesure ces exigences s'appliquent-elles, eu égard à la nécessité essentielle pour les*

SSR d'utiliser l'acquisition de masse et les techniques de traitement automatisé pour protéger la sécurité nationale et eu égard à la mesure dans laquelle de telles capacités, si elles sont conformes à la CEDH, pourraient être fondamentalement frustrées par l'imposition de telles exigences?»

3. EN DROIT

3.1. Sur la première question

19. Au moyen de sa première question, la juridiction de renvoi souhaite savoir si une exigence figurant dans des instructions données par le Secretary of State du Royaume-Uni à un opérateur de télécommunications et en vertu de laquelle ce dernier est tenu de fournir des DCM aux SSR relève du champ d'application de la directive 2002/58/CE, compte tenu de l'article 4, paragraphe 2, TUE et de l'article 1er, paragraphe 3, de la directive 2002/58/CE.

20. Selon la Commission, il découle du raisonnement de la Cour de justice dans l'arrêt *Tele2/Watson* qu'il convient de répondre par l'affirmative à la première question.

3.1.1. L'arrêt Tele2/Watson

21. Dans l'arrêt *Tele2/Watson*, la Cour de justice a précisé le sens de l'article 1er, paragraphe 3, de la directive 2002/58/CE, lequel exclut du champ d'application de celle-ci les «activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et, en tout état de cause, [les] 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 [les] activités de l'État dans des domaines relevant du droit pénal».

22. La législation nationale en cause dans l'arrêt *Tele2/Watson* prévoyait l'exigence, pour les opérateurs de télécommunications, de conserver les données relatives au trafic et les données de localisation ainsi que des conditions d'accès à ces données par les autorités compétentes dans le but de lutter contre la criminalité. En vertu de l'article 1er, paragraphe 3, de telles activités pourraient être considérées comme ne relevant pas du champ d'application de la directive: premièrement, au moment où la directive 2002/58/CE a été adoptée, le traité instituant la Communauté européenne ne couvrait pas la coopération en matière pénale et, deuxièmement, les activités de

l'État dans les domaines du droit pénal ont été expressément exclues du champ d'application de la directive[2].

23. Toutefois, malgré le libellé de l'article 1er, paragraphe 3, la Cour de justice a conclu, dans l'affaire *Tele2/Watson,* que la législation nationale en cause relevait du champ d'application de la directive 2002/58/CE. La Cour est parvenue à cette conclusion en examinant la structure générale de la directive. Le raisonnement de la Cour de justice figure aux points 67 à 81 de l'arrêt.

24. La Cour de justice s'est notamment référée à l'article 15, paragraphe 1, de la directive 2002/58/CE, qui autorise les États membres à adopter des mesures législatives visant à limiter la portée de certains droits et obligations prévus par la directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder, entre autres, la sécurité nationale (c'est-à-dire la sûreté de l'État), la défense et la sécurité publique et assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales.

25. Sur la base de l'article 15, paragraphe 1, les obligations de garantie de la confidentialité des communications (voir l'article 5, paragraphe 1) et d'effacement ou d'anonymisation des données lorsqu'elles ne sont plus nécessaires aux objectifs commerciaux de l'opérateur de télécommunications (voir l'article 6), par exemple, peuvent être limitées.

26. La Cour a reconnu que les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58/CE se rapportent aux activités propres aux États et aux autorités étatiques, qu'elles sont étrangères aux domaines d'activités des particuliers (paragraphe 72) et qu'il existe un chevauchement important entre les objectifs que doivent poursuivre les mesures visées à l'article 15, paragraphe 1 et les objectifs poursuivis par les activités visées à l'article 1er, paragraphe 3, de la directive 2002/58/CE (voir le point 21 ci-dessus).

27. Toutefois, la Cour a considéré que les mesures législatives visées à l'article 15, paragraphe 1, régissent, aux fins mentionnées dans cette disposition, l'activité des fournisseurs de services de communications électroniques (point 74). Il ressort de

---

[2] La coopération en matière pénale n'était pas couverte par le traité instituant la Communauté européenne, mais n'était pas exclue du *droit de l'Union* en tant que tel, étant donné que la compétence de l'UE dans ce domaine a été consacrée dans le traité sur l'Union européenne antérieur.

l'article 3 de la directive 2002/58/CE que les activités de ces fournisseurs sont précisément l'objet de la directive 2002/58/CE (point 74).

28. Selon la Cour, les mesures nationales en cause dans l'arrêt *Tele2/Watson* ne doivent pas être exclues du champ d'application de la directive 2002/58/CE, sauf à priver l'article 15, paragraphe 1 de tout effet utile (voir le point 73).

29. La Cour a déclaré que relève, en particulier, du champ d'application de la directive 2002/58/CE une mesure législative qui impose aux fournisseurs de services de communications électroniques de conserver les données relatives au trafic et les données de localisation, mais aussi une mesure législative telle que celle en cause dans l'arrêt *Tele2/Watson*, portant sur l'accès des autorités nationales aux données conservées (points 75 et 76).

30. À cet égard, la Cour a souligné que la protection de la confidentialité des communications électroniques et des données relatives au trafic y afférentes, garantie à l'article 5, paragraphe 1, de la directive 2002/58/CE, s'applique aux mesures prises par l'ensemble des personnes autres que les utilisateurs, qu'il s'agisse de personnes ou d'entités privées, ou d'entités étatiques (point 77). En outre, la Cour a estimé que dès lors que la conservation des données dans l'affaire *Watson/Tele2* n'était intervenue qu'aux seules fins de les rendre accessibles aux autorités nationales compétentes, la législation nationale imposant la conservation de données impliquait, en principe, nécessairement l'existence de dispositions relatives à l'accès par les autorités à ces données (point 79).

3.1.2. Applicabilité du raisonnement Tele2/Watson à la présente affaire

31. Dans la présente affaire, l'objectif poursuivi par la mesure nationale en cause (les instructions du Secretary of State du Royaume-Uni sur la base de l'article 94 du 1984 Act) est, en principe, différent de l'objectif poursuivi par la mesure en cause dans l'affaire *Tele2/Watson*, étant donné qu'il concerne la sauvegarde de la sécurité nationale.

32. Cependant, tout comme l'objectif de la lutte contre la criminalité, la sécurité nationale est visée à la fois à l'article 1er, paragraphe 3, et à l'article 15, paragraphe 1, de la directive 2002/58/CE[3]. Par conséquent, la Commission est

---

[3] L'article 1er, paragraphe 3, de la directive 2002/58/CE fait référence à la «sûreté de l'État», qui, dans les présentes observations, est traitée comme un synonyme de «sécurité nationale».

d'avis que le raisonnement de la Cour de justice dans l'affaire *Tele2/Watson*, fondé sur la structure générale de la directive 2002/58/CE, devrait, en principe, être appliqué en l'espèce. Le fait que l'article 4, paragraphe 2, TUE dispose que la sécurité nationale reste de la seule responsabilité de chaque État membre, n'a pas, en principe, selon la Commission, d'incidence sur le raisonnement de la Cour de justice dans l'affaire *Tele2/Watson* pour ce qui est de l'applicabilité de la directive.

33. Comme la Cour l'a relevé dans l'arrêt *Tele2/Watson*, la directive 2002/58/CE régit les activités des fournisseurs de services de communications électroniques. Il s'ensuit que l'activité des opérateurs de RPCE consistant dans la transmission de DCM aux SSR tombe sous le coup de la directive. Étant donné qu'une telle transmission est à tout le moins contraire à l'obligation, prévue à l'article 5 de ladite directive, de garantir la confidentialité des communications et, éventuellement, à l'obligation, prévue à l'article 6 de la directive, d'effacer les données, les opérateurs de RPCE ne peuvent fournir ces informations que sur la base d'une mesure législative nationale au sens de l'article 15, paragraphe 1, de la directive 2002/58/CE.

34. La Commission estime, cependant, que s'il est confirmé que la conservation et l'utilisation ultérieure des données par les SSR, après leur réception, sont considérées comme des activités de l'État aux fins de la sécurité nationale ne requérant aucune autre intervention des opérateurs de RPCE, les activités des SSR ne devraient normalement pas relever du champ d'application de la directive 2002/58/CE. À cet égard, contrairement à la situation de l'affaire *Tele2/Watson* (voir le point 79), les dispositions relatives à l'accès et à l'utilisation ultérieure ne constituent pas, en l'espèce, un élément essentiel de l'obligation de conservation des données imposée aux opérateurs de télécommunications. Dans la présente affaire, l'obligation imposée aux opérateurs de RPCE consiste à transférer les DCM aux SSR. Par la suite, les opérateurs n'interviennent plus dans le traitement des données par les SSR.

35. Considérer que la transmission obligatoire de DCM aux SSR par les opérateurs de RPCE relève du champ d'application de la directive 2002/58/CE emporte certaines conséquences, qui seront abordées de manière plus approfondie au moment de répondre à la seconde question de la juridiction de renvoi.

36. La juridiction de renvoi considère que la transmission de DCM par les opérateurs de RPCE devrait être perçue comme le support d'une fonction essentielle de l'État, en l'espèce la protection de la sécurité nationale à travers un cadre établi par les autorités publiques ayant trait à la sécurité publique (voir le point 36 de la décision de renvoi). Selon la juridiction de renvoi, il découle du raisonnement de la Cour de justice, dans ses arrêts de 2006 relatifs au transfert, aux États-Unis, de données des dossiers passagers (données PNR) par les compagnies aériennes (C-317/04 et C-318/04, *Parlement européen/Conseil* et *Parlement européen/Commission*, ECLI:EU:C: 2006:346, ci-après les «arrêts relatifs au transfert de PNR aux États-Unis»), que l'activité doit être considérée comme ne relevant pas du champ d'application de la directive 2002/58/CE, en vertu de l'article 1er, paragraphe 3 de celle-ci[4].

37. La Commission est d'avis que le raisonnement de la Cour de justice dans les arrêts relatifs au transfert de PNR aux États-Unis ne saurait s'appliquer dans le cadre de la présente affaire, en particulier à la lumière de l'arrêt dans l'affaire *Tele2/Watson*.

38. À cet égard, la Commission renvoie aux conclusions de l'avocat général Mengozzi relatif au projet d'accord entre l'Union européenne et le Canada sur le transfert de données PNR (A-1/15, ECLI:EU:C:2016:656). Dans ses conclusions, l'avocat général a souligné le contexte spécifique des arrêts relatifs au transfert des PNR aux États-Unis. Ces arrêts, qui ont été rendus bien avant l'adoption du traité de Lisbonne, concernaient une décision d'adéquation relative au traitement des données dans le cadre d'un accord avec les États-Unis relatif au transfert de données PNR qui n'ont pas pu être rattachées à des prestations de services, mais relevaient du cadre établi par les autorités publiques visant la sécurité publique (voir le point 85 des conclusions de l'avocat général). Selon l'avocat général, la Cour a conclu, en toute logique, que l'objet *de la décision d'adéquation* ne relevait pas du champ d'application de la directive 95/46/CE. Toutefois, l'avocat général a mis en garde contre le fait de tirer des conclusions définitives en dehors du contexte spécifique de l'affaire.

---

[4] Ces arrêts portaient, entre autres, sur l'interprétation de l'article 3, paragraphe 2, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31) (ci-après la «directive 95/46»). L'article 3, paragraphe 2, de la directive 95/46 correspond à l'article 1er, paragraphe 3, de la directive 2002/58/CE.

39. La Commission adhère à cette conclusion, en particulier à la lumière de l'arrêt *Tele2/Watson*.

40. Dans *Tele2/Watson*, la Cour ne s'appuie pas sur le raisonnement des arrêts relatifs au transfert de PNR aux États-Unis lorsqu'il s'agit de déterminer si les mesures nationales en cause relèvent du champ d'application de la directive 2002/58/CE. Au contraire, les points 69 et 70 de l'arrêt de la Cour ont clairement fait la distinction entre les activités de l'État et les activités des fournisseurs de services de télécommunications. L'article 1er, paragraphe 3, de la directive 2002/58/CE exclut les «activités de l'État» du champ d'application de la directive (voir le point 69), tandis que les activités des fournisseurs de services de télécommunications sont régies par la directive, et relèvent donc de son champ d'application (voir le point 70). La Cour a conclu que les mesures législatives nationales en cause dans l'affaire *Tele2/Watson* relevaient du champ d'application de la directive 2002/58/CE parce qu'elles portaient sur l'activité des fournisseurs de services de télécommunications. Le fait que la conservation des données (et de l'accès ultérieur des autorités compétentes à celles-ci) avait pour objectif de lutter contre la criminalité n'a pas eu d'incidence sur cette conclusion[5].

41. Enfin, le point 29 de l'ordonnance de renvoi préjudiciel fait référence au point 5 de la section C de la décision des chefs d'État et de gouvernement, réunis au sein du Conseil européen du 19 février 2016 concernant un nouvel arrangement pour le Royaume-Uni dans l'Union européenne. La Commission tient à souligner que cette décision n'a jamais pris effet (voir le point 2 de la section E de la décision)[6] et ne devrait donc pas être prise en considération par la Cour.

42. Sur la base de l'ensemble des considérations qui précèdent, la Commission propose à la Cour de répondre à la première question comme suit:

«Une exigence figurant dans des instructions données par le Secretary of State à un fournisseur de services de communications électroniques et en vertu de laquelle ce dernier est tenu de fournir des données de communications en masse aux services de

---

5 Concernant l'article 3, paragraphe 2, de la directive 95/46, qui correspond à l'article 1er, paragraphe 3, de la directive 2002/58/CE, la Cour de justice a, de façon plus générale, jugé que cette clause devait être interprétée strictement. Voir l'affaire C-73/16, *Puškar*, ECLI:EU:C:2017:725, point 38.

6 Voir également le point 4 des conclusions du Conseil européen des 18 et 19 février 2016, en vertu desquelles l'ensemble des dispositions visées au point 2 de ces conclusions, parmi lesquelles figurait la décision, a cessé d'exister après le référendum qui s'est tenu au Royaume-Uni et dont le résultat a été l'annonce du retrait du Royaume-Uni de l'Union européenne.

sécurité et de renseignement d'un État membre pour des raisons de sécurité nationale, comme en l'espèce, relève du champ d'application de la directive 2002/58/CE dans la mesure où elle concerne la transmission par le fournisseur.»

3.1.3. Considérations subsidiaires

43. Dans le cas où la Cour de justice ne partagerait pas la conclusion ci-dessus, mais considérerait plutôt qu'une mesure nationale exigeant d'un opérateur de télécommunications qu'il fournisse des données à des services de sécurité nationaux, pour des raisons de sécurité nationale, ne relève en principe pas du champ d'application de la directive 2002/58/CE, la Commission propose que les considérations suivantes soient prises en compte afin de permettre à la juridiction nationale de déterminer si la situation dont elle est saisie est couverte par une telle exclusion.

44. Tout d'abord, la Commission tient à souligner que l'affirmation selon laquelle la sécurité nationale reste de la compétence exclusive des États membres, dans la troisième phrase de l'article 4, paragraphe 2, TUE, doit être interprétée à la lumière du principe du respect de l'identité nationale des États membres, dont la sécurité nationale est un élément (voir l'article 4, paragraphe 2, TUE, première et deuxième phrases)[7].

45. L'article 4, paragraphe 2, TUE ne devrait, en tout état de cause, pas être interprété de manière à permettre aux États membres de s'écarter de leurs obligations au titre du droit de l'UE du simple fait qu'une décision concerne la sûreté de l'État (voir l'affaire C-300/11, *ZZ*, EU:C:2013:363, point 38, comportant une référence à l'affaire C-387/05, *Commission/Italie*, ECLI:EU:C:2009:781, point 45; l'affaire C-273/97, *Sirdar*, EU:C:1999:523, point 16; les conclusions de l'avocat général Kokott dans l'affaire C-187/16, *Commission/Autriche*, EU:C:2017:578, point 46). Dans son arrêt dans l'affaire 461/05, *Commission/Danemark* (EU:C:2009:783, point 51), la Cour a expliqué:

> «Il ne saurait en être déduit qu'il existerait une réserve générale, inhérente au traité, excluant du champ d'application du droit communautaire toute mesure prise au titre de la sécurité publique. Reconnaître l'existence d'une telle réserve,

---

[7] Ce principe a déjà été consacré à l'ancien article 6, paragraphe 3, TUE, c'est-à-dire avant l'adoption du traité de Lisbonne (respectivement à l'article F, paragraphe 1, du traité de Maastricht).

en dehors des conditions spécifiques des dispositions du traité, risquerait de porter atteinte au caractère contraignant et à l'application uniforme du droit communautaire (voir, en ce sens, l'arrêt du 11 mars 2003, *Dory*, C-186/01, Rec. p. I-2479, point 31 et jurisprudence citée).»[8]

46. Afin de déterminer si un État membre peut se prévaloir de la compétence exclusive pour une certaine question, il est nécessaire d'évaluer si la mesure en cause répond *véritablement* à l'objectif consistant à sauvegarder la sécurité nationale. Selon la Commission, cela nécessite tout d'abord de clarifier la notion de «sécurité nationale», telle qu'elle figure à l'article 4, paragraphe 2, TUE, et telle qu'elle ressort de l'article 1er, paragraphe 3, de la directive 2002/58/CE. En second lieu, cela requiert d'apprécier si la mesure est, dans les faits, *capable* d'atteindre l'objectif recherché.

47. La Commission est d'avis que la notion de «sécurité nationale» constitue une notion du droit de l'Union, qui requiert une interprétation autonome. Le caractère contraignant du droit de l'Union se verrait gravement compromis si un État membre pouvait éviter l'application de celui-ci en indiquant simplement qu'une mesure sert l'objectif de la sécurité nationale. Cela dit, la Commission reconnaît que les États membres devraient bénéficier d'un large pouvoir d'appréciation en ce qui concerne la définition de ce qu'ils considèrent être des mesures de sauvegarde de la sécurité nationale (voir, en ce sens, les conclusions de l'avocat général Kokott dans l'affaire C-187/16, *Commission/Autriche*, EU:C:2017:578, point 47).

48. Le TUE et le TFUE ne définissent pas la notion de «sécurité nationale». L'article 4, paragraphe 2, TUE, dans le cadre du principe général du respect de l'identité nationale des États membres, indique que la sécurité nationale est un exemple de «fonctions essentielles de l'État».

49. La Commission estime qu'il existe des similitudes entre la notion de «sécurité nationale» et les «intérêts essentiels de [la] sécurité» d'un État membre, à l'article 346, paragraphe 1, TFUE. En ce qui concerne l'article 346, paragraphe 1, TFUE, il est de jurisprudence constante que la notion de «sécurité» dans cette disposition constitue un concept autonome du droit de l'Union (voir l'affaire C-273/97, *Sirdar*, EU:C:1999:523, point 16; les conclusions de l'avocat général

---

[8] Voir également le raisonnement presque identique dans l'arrêt rendu dans l'affaire C-387/05, *Commission/Italie*, EU:C:2009:781, point 45.

Kokott dans l'affaire C-187/16, *Commission/Autriche*, EU:C:2017:578, points 46 et suivants).

50. Il peut en être déduit que la notion de «sécurité nationale» se rapporte à la nécessité de préserver et de défendre un ensemble de base d'intérêts essentiels de l'État, qui sont nécessaires pour garantir son existence et son ordre constitutionnel (voir, par exemple, l'affaire C-601/15 PPU, *J.N.*, EU:C:2016:84, points 64 à 67). La sécurité nationale peut être considérée comme se référant à des menaces réelles, actuelles et suffisamment graves touchant à l'un des intérêts fondamentaux de l'État (voir à cet effet, *ibidem*, point 65)[9].

51. Il appartient au contraire aux États membres d'expliquer, dans tous les cas, de façon circonstanciée, quels intérêts de la sécurité nationale sont précisément affectés et dans quelle mesure le respect de certaines obligations découlant du droit de l'Union serait concrètement contraire à ces intérêts (voir l'affaire C-474/12, *Schiebel Aircraft*, EU:C:2014:2139, point 34, et les conclusions de l'avocat général Kokott dans l'affaire C-187/16, *Commission/Autriche*, point 48, et la jurisprudence y citée).

52. Selon la Commission, il pourrait y avoir un certain chevauchement entre les objectifs poursuivis dans l'intérêt de la sécurité nationale et les objectifs «ordinaires» liés à la répression (*law enforcement)* . En particulier, la prévention des actes de terrorisme pourrait relever à la fois de la prévention des infractions pénales et de la prévention des menaces pour la sécurité nationale.

53. Afin de déterminer si une mesure nationale constitue une activité relevant de la sécurité nationale ou, plutôt, une activité liée à la répression *(law enforcement)*, il convient de tenir compte de l'objectif en vue duquel les données sont collectées et de déterminer si un objectif de cette nature correspond à la protection des intérêts essentiels de l'État. À cet égard, certains actes, et donc aussi les infractions pénales, pourraient être d'une gravité et d'une nature telles qu'ils menacent les intérêts fondamentaux de l'État. La prévention de tels actes peut alors être considérée comme servant l'intérêt de la sécurité nationale de l'État.

---

[9] Voir l'arrêt rendu dans l'affaire C-601/15 PPU *J.N., EU:C:2016:84, points 64 et 67, relatif à l'article 8, paragraphe 3, de la directive 2013/33, établissant des normes pour l'accueil des demandeurs de protection internationale, qui, sous e), se réfère à la protection de la sécurité nationale ou de l'ordre public.*

54. Parmi les autres indicateurs qui pourraient être importants, il convient de mentionner les caractéristiques spécifiques des autorités qui mènent ces activités, à savoir les autorités de sécurité et de renseignement et, éventuellement, l'utilisation par ces autorités de méthodes de travail spécifiques qui pourraient inclure le suivi des activités visant la prévention des menaces pesant sur les intérêts essentiels de l'État. Il y a toutefois lieu de souligner que ces deux éléments, pris ensemble ou isolément, ne devraient pas, en tant que tels, être considérés comme concluants en ce qui concerne l'identification d'une véritable activité de sécurité nationale. Par exemple, dans l'hypothèse où certaines tâches auraient été confiées aux autorités de renseignement plutôt qu'à la police, n'exclurait pas, en soi, la possibilité que les activités des autorités de renseignement puissent, en réalité, être considérées comme étant menées essentiellement dans le but de lutter contre les formes graves de criminalité ou dans le cadre d'autres activités répressives (*law enforcement)*. Ce point est illustré par la notion générale d'«autorités compétentes» à l'article 87, paragraphe 1, TFUE.

55. Une fois qu'il est établi qu'une mesure poursuit un véritable intérêt de sécurité nationale, les États membres doivent démontrer que la mesure est effectivement capable d'atteindre l'objectif visé.

56. Il incombe à la juridiction nationale de déterminer si la mesure nationale en cause sert réellement les intérêts de la sécurité nationale, en tenant compte des considérations qui précèdent.

3.2. Sur la seconde question

57. À travers sa seconde question, la juridiction de renvoi souhaite savoir, dans le cas où la réponse à la première question serait affirmative, si, et le cas échéant comment et dans quelle mesure, les exigences matérielles et procédurales fixées par la Cour de justice dans l'arrêt *Tele2/Watson* concernant l'accès aux données conservées par les autorités compétentes s'appliquent également aux instructions du Secretary of State, comme en l'espèce.

3.2.1. Les exigences énoncées dans l'arrêt Tele2/Watson

58. Aux points 113 à 125 de l'arrêt *Tele2/Watson*, la Cour s'est prononcée sur les implications de l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7 et 8 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux, sur la législation nationale relative à l'accès par les autorités

nationales aux données que les opérateurs de télécommunications sont tenus de conserver aux fins de la lutte contre la criminalité.

59. Selon la Cour, une mesure de conservation des données doit prévoir des règles claires et précises indiquant en quelles circonstances et sous quelles conditions les fournisseurs de services de communications électroniques sont tenus d'accorder aux autorités nationales compétentes l'accès aux données (voir le point 117). Une mesure de cette nature doit être légalement contraignante en droit interne (*ibidem*).

60. Afin de garantir que l'accès aux données conservées est limité à ce qui est strictement nécessaire, la législation nationale ne saurait se limiter à exiger que l'accès réponde à l'un des objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58/CE. Selon la Cour, la législation nationale doit également prévoir les conditions matérielles et procédurales régissant l'accès des autorités nationales compétentes aux données conservées (voir le point 118).

61. À cet égard, la Cour de justice a énoncé les conditions matérielles et procédurales suivantes aux points 119 et 125 de l'arrêt:

    a) l'accès ne saurait être accordé qu'aux données conservées de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction (point 119). Dans des situations particulières, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités. À titre d'exemple, la Cour mentionne les «intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique» (*ibidem*);

    b) l'accès des autorités nationales compétentes aux données conservées doit être subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, à la suite d'une demande motivée de ces autorités, sauf cas d'urgence dûment justifiés (point 120);

    c) les autorités nationales compétentes auxquelles l'accès a été accordé en informent les personnes concernées dès le moment où cette

communication n'est plus susceptible de compromettre les enquêtes menées par ces autorités (point 121);

d) un niveau particulièrement élevé de protection et de sécurité des données conservées par les fournisseurs de télécommunications devrait être garanti au moyen de mesures d'ordre technique ou organisationnel appropriées. Cela signifie, selon la Cour, que les données doivent être conservées au sein de l'Union (voir le point 122);

e) les États membres devraient garantir le contrôle, par une autorité indépendante, du respect du niveau de protection garanti par le droit de l'Union (point 123). Cette exigence découle de l'article 8, paragraphe 3, de la charte des droits fondamentaux.

3.2.2. Applicabilité des conditions Tele2/Watson à la présente affaire

62. La situation en l'espèce diffère de celle de l'affaire *Tele2/Watson*, non seulement au regard de l'objectif poursuivi par la mesure nationale concernée, mais aussi par la manière dont la mesure est organisée.

63. Dans la présente affaire, la mesure nationale oblige les opérateurs de RPCE à transmettre les DCM aux SSR, à la suite de quoi les données sont conservées par les SSR puis exploitées (voir le point 12 ci-dessus). Dans l'affaire *Tele2/Watson*, en revanche, les mesures nationales exigeaient des opérateurs de télécommunications qu'ils conservent les données, auxquelles les autorités nationales compétentes pouvaient avoir accès.

64. Il s'ensuit que, si la réponse à la première question de la demande de décision préjudicielle est que seule la transmission de DCM aux SSR par l'opérateur de RPCE, et non pas la conservation et l'utilisation ultérieure des données par les SSR, est couverte par la directive 2002/58/CE, la condition énoncée au point 61 d) ci-dessus (conservation dans l'Union) n'est pas pertinente, étant donné que les données sont conservées par les SSR, qui ne sont pas, à cet égard, soumis aux exigences de sécurité de la directive 2002/58/CE.

65. En ce qui concerne les autres conditions énoncées au point 61 ci-dessus, dans la mesure nécessaire aux activités des opérateurs de RPCE, la Commission estime que ces conditions ne s'appliquent pas nécessairement en tant que telles à la présente situation. Cela est dû non seulement aux situations factuelles différentes, mais aussi

aux spécificités de l'objectif de sauvegarde de la sécurité nationale ainsi qu'au fait que, conformément à l'article 4, paragraphe 2, TUE, la sécurité nationale reste de la seule responsabilité des États membres. Les conditions formulées par la Cour dans l'arrêt *Tele2/Watson*, rappelées au point 61 ci-dessus, mériteraient peut-être d'être abordées différemment.

66. Cela dit, comme indiqué au point 33, les opérateurs de RPCE peuvent uniquement transmettre les DCM aux SSR si les conditions énoncées à l'article 15, paragraphe 1, de la directive 2002/58/CE sont remplies. L'article 15, paragraphe 1, lu à la lumière des articles 7 et 8 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux, exige que les trois conditions principales suivantes soient remplies pour que l'obligation des opérateurs de RPCE de transmettre les DCM aux SSR soit licite:

    a) la mesure devrait être prévue par une mesure législative qui satisfait aux exigences de qualité de la loi;

    b) la mesure devrait réellement atteindre l'objectif de sauvegarde de la sécurité nationale;

    c) la mesure devrait être nécessaire, appropriée et proportionnée pour atteindre l'objectif de sauvegarde de la sécurité nationale.

67. Afin de satisfaire à la première condition, l'obligation pour les opérateurs de RPCE de transmettre les DCM aux SSR devrait être prévue dans une mesure législative qui satisfasse aux exigences de qualité de la loi, établisse des règles claires et précises régissant la portée et l'application de la mesure et impose des garanties minimales (voir *Tele2/Watson*, points 109 et 117, voir également l'avis de la Cour de justice sur le projet d'accord entre l'Union européenne et le Canada sur le transfert de données PNR, A-1/15, ECLI:EU:C:2017:592, point 141).

68. Dans la présente affaire, l'obligation pour les opérateurs de RPCE de transmettre des données aux SSR est définie dans des instructions du Secretary of State du Royaume-Uni sur la base de l'article 94 du 1984 Act. Il appartient à la juridiction nationale de déterminer si cette mesure peut être considérée comme juridiquement contraignante en vertu de la législation nationale. Ensuite, il devrait être établi s'il existe des règles claires et précises régissant la portée et l'application de la mesure.

69. La deuxième condition requiert que la mesure poursuive réellement l'objectif de sauvegarde de la sécurité nationale. La question de savoir si cette condition est remplie ressemble, dans une large mesure, à l'évaluation décrite à la section 3.1.3 ci-dessus. La Commission renvoie la Cour à son analyse présentée dans ladite section.

70. Quant à la troisième condition (la mesure doit être appropriée, nécessaire et proportionnée pour atteindre l'objectif de sauvegarde de la sécurité nationale), la Commission estime que, lorsque la mesure nationale poursuit véritablement l'objectif de sauvegarde de la sécurité nationale et est capable de l'atteindre, l'appréciation ultérieure de la proportionnalité devrait se limiter à établir s'il y a eu une erreur manifeste d'appréciation ou un détournement de pouvoir (voir, par analogie, l'affaire C-266/05 P, *José María Sisón*, ECLI:EU:C:2007:75, point 64).

71. Dans la présente affaire, la question est de savoir si l'exigence imposée à un opérateur de RPCE de transmettre des DCM aux SSR constituerait, en tant que telle, une erreur manifeste d'appréciation au regard du principe de proportionnalité ou un détournement de pouvoir. À cet égard, le degré d'intrusion que représente la transmission de DCM en tant que telle, la nature des données, le nombre de personnes concernées, le but de la transmission et les méthodes de travail nécessaires des SSR devraient tous être pris en compte.

72. Il incombe à la juridiction de renvoi de déterminer si et dans quelle mesure la législation nationale en cause satisfait aux exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58/CE, comme indiqué plus haut (voir également *Tele2/Watson*, point 124).

73. Pour ces motifs, la Commission propose à la Cour de répondre à la seconde question, comme suit:

«L'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7 et 8 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété comme exigeant que les instructions données par le Secretary of State à un fournisseur de services de communications électroniques de fournir les données de communications en masse aux services de sécurité et de renseignement d'un État membre pour des raisons de sécurité nationale se fondent sur une mesure législative qui satisfasse aux exigences de qualité de la loi, réponde effectivement à l'objectif de

sauvegarde de la sécurité nationale et soit nécessaire, appropriée et proportionnée pour atteindre l'objectif de sauvegarde de la sécurité nationale.»

4. CONCLUSION

74. Eu égard aux considérations qui précèdent, la Commission propose à la Cour d'apporter les réponses suivantes aux questions qui lui ont été posées par la juridiction de renvoi:

«1. Une exigence dans des instructions données par le Secretary of State à un fournisseur de services de communications électroniques de fournir les données de communications en masse aux services de sécurité et de renseignement d'un État membre pour des raisons de sécurité nationale, comme en l'espèce, relève du champ d'application directive 2002/58/CE dans la mesure où elle concerne la transmission par le fournisseur.

2. L'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7 et 8 et de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété comme exigeant que les instructions données par le Secretary of State à un fournisseur de services de communications électroniques de fournir les données de communications en masse aux services de sécurité et de renseignement d'un État membre pour des raisons de sécurité nationale se fonde sur une mesure législative qui satisfasse aux exigences de qualité de la loi, réponde effectivement à l'objectif de sauvegarde de la sécurité nationale et soit nécessaire, appropriée et proportionnée pour atteindre l'objectif de sauvegarde de la sécurité nationale.»

Martin WASMEIER, Piedade COSTA DE OLIVEIRA, Herke KRANENBORG et Daniele NARDI

Agents de la Commission