**ÉDITION PROVISOIRE DU 14/01/2020**

CONCLUSIONS DE L'AVOCAT GÉNÉRAL
M. MANUEL CAMPOS SÁNCHEZ-BORDONA
présentées le 15 janvier 2020 [1]

**Affaire C-623/17**

**Privacy International**
**contre**
**Secretary of State for Foreign and Commonwealth Affairs,**
**Secretary of State for the Home Department,**
**Government Communications Headquarters,**
**Security Service,**
**Secret Intelligence Service**

[demande de décision préjudicielle formée par l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni)]

« Recours préjudiciel – Traitement de données à caractère personnel et protection de la vie privée dans le secteur des communications

1 Langue originale : l'espagnol.

électroniques – Directive 2002/58/CE – Champ d'application – Article 1er, paragraphe 3 – Article 15, paragraphe 3 – Charte des droits fondamentaux de l'Union européenne – Articles 7, 8 et 51 ainsi que article 52, paragraphe 1 – Article 4, paragraphe 2, TUE – Transmission généralisée et indifférenciée aux services de sécurité de données de connexion des utilisateurs d'un service de communications électroniques »

1. Ces dernières années, la Cour a maintenu une jurisprudence constante en matière de conservation et d'accès aux données à caractère personnel, dont les arrêts suivants constituent des jalons importants :

– L'arrêt du 8 avril 2014, Digital Rights Ireland e.a. [2], dans lequel elle a déclaré l'invalidité de la directive 2006/24/CE [3] au motif que celle-ci permettait une ingérence disproportionnée dans les droits reconnus par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne.

– L'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. [4], dans lequel elle a interprété l'article 15, paragraphe 1, de la directive 2002/58/CE [5].

2 C-293/12 et C-594/12, EU:C:2014:238.

3 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).

4 C-203/15 et C-698/15, ci-après l'« arrêt Tele2 Sverige et Watson e.a. », EU:C:2016:970.

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).

– L’arrêt du 2 octobre 2018, Ministerio Fiscal [6], dans lequel elle a confirmé l’interprétation de cette même disposition de la directive 2002/58.

2. Ces arrêts (en particulier le deuxième) préoccupent les autorités de certains États membres car elles estiment qu’ils ont pour conséquence de les priver d’un instrument qu’ils jugent indispensable à la sauvegarde de la sécurité nationale et à la lutte contre la criminalité et le terrorisme. C’est pourquoi quelques-uns de ces États membres plaident en faveur du renversement ou de l’atténuation de cette jurisprudence.

3. Certaines juridictions des États membres ont exprimé cette même préoccupation dans le cadre de quatre renvois préjudiciels [7], sur lesquels je présente mes conclusions ce jour.

4. Les quatre affaires soulèvent avant tout le problème de l’application de la directive 2002/58 à des activités liées à la sécurité nationale et à la lutte contre le terrorisme. Si ladite directive était applicable dans ce contexte, il conviendrait ensuite de déterminer dans quelle mesure les États membres peuvent restreindre les droits à la protection de la vie privée qu’elle garantit. Enfin, il conviendra

6 C-207/16, EU:C:2018:788.

7 Outre le présent renvoi, il s’agit des affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a., ainsi que de l’affaire C-520/18, Ordre des barreaux francophones et germanophone e.a.

d'analyser jusqu'à quel point les différentes réglementations nationales (britannique [8], belge [9] et française [10]) en la matière sont conformes au droit de l'Union tel qu'il a été interprété par la Cour.

## I. Le cadre juridique

### A. Le droit de l'Union

5. Je renvoie au point correspondant de mes conclusions dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a.

### B. Le droit du Royaume-Uni (applicable à la présente espèce)

#### *1. Telecommunications Act 1984* [11]

6. Conformément à l'article 94, le Secretary of State (secrétaire d'État, Royaume-Uni) peut, après avoir consulté un opérateur de réseau public de communications électroniques, donner à cet opérateur des instructions générales ou spécifiques qui lui semblent être nécessaires dans l'intérêt de la sécurité nationale ou des relations avec un gouvernement étranger.

8 Affaire Privacy International (C-623/17).

9 Affaire Ordre des barreaux francophones et germanophone e.a. (C-520/18).

10 Affaires jointes La Quadrature du Net e.a. (C-511/18 et C-512/18).

11 Loi sur les télécommunications de 1984 ; ci-après la « loi de 1984 ».

### *2. Data Retention and Investigatory Powers Act 2014* [12]

7. L'article 1er dispose ce qui suit :

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

(2) Un acte ordonnant la conservation peut :

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

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

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

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

[12] Loi de 2014 relative à la conservation des données et aux pouvoirs d'enquête ; ci-après « DRIPA ».

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

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

(3) Le secrétaire d'État peut, par voie de règlements, adopter davantage de dispositions concernant la conservation des données pertinentes relatives aux communications.

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

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

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

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

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

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

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

(g) le remboursement par le secrétaire d'État (sous certaines conditions ou non) des frais encourus par les opérateurs de télécommunications publiques pour se conformer aux exigences ou aux restrictions pertinentes ;

[...]

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

(6) Un opérateur de télécommunications publiques qui conserve des données pertinentes relatives aux communications en application du présent article ne peut les divulguer à moins que :

(a) il les divulgue conformément :

(i) au chapitre 2 de la partie 1 de la [RIPA] ou

(ii) à une décision judiciaire ou toute autre autorisation ou injonction du tribunal, ou que

(b) cela soit prévu par les règlements visés au paragraphe 3.

(7) Le secrétaire d'État peut, par voie de règlements, adopter des dispositions relatives aux différentes dispositions adoptées (ou

susceptibles d'être adoptées) en application du paragraphe 4, points d) à g), ou du paragraphe 6, concernant les données relatives aux communications conservées par les fournisseurs de services de télécommunications conformément à un code des bonnes pratiques, en vertu de l'article 102 de l'Anti-Terrorism, Crime and Security Act 2001 [loi sur la sécurité et la répression de la criminalité et du terrorisme de 2001] ».

### *3. La RIPA*

8. L'article 21 est rédigé comme suit :

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

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

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

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

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

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

[...]

(6) Dans cette section, la notion de “donnée relative au trafic”, concernant toute communication, fait référence à :

(a) toute donnée identifiant ou permettant d’identifier une personne, un appareil ou un lieu vers lequel ou à partir duquel une communication est ou peut être transmise ;

(b) toute donnée identifiant ou sélectionnant, ou permettant d’identifier ou de sélectionner l’équipement par lequel la communication est ou peut être transmise ;

(c) toute donnée comprenant des signaux pour le fonctionnement de l’appareil utilisé dans un système de communication afin de transmettre toute communication ; et

(d) toute donnée identifiant les données comprises dans, ou annexées à, une communication particulière ou d’autres données dans la mesure où elles sont comprises dans, ou annexées à, une communication particulière.

[...] »

9. L’article 22 est libellé comme suit :

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

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

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

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

(c) dans l'intérêt du bien-être économique du Royaume-Uni, à condition que ces intérêts soient également pertinents pour les intérêts de la sûreté nationale ;

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

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

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

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

blessure ou préjudice pour la santé physique ou mentale d'une personne physique ;

(h) à toute autre fin [ne relevant pas des points a) à g)] précisée dans une injonction délivrée par le secrétaire d'État en vertu de l'article 22, paragraphe 2, point h), de la loi de 2014 relative à la conservation des données et aux pouvoirs d'enquête.

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

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

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

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

10. Conformément à l'article 65, des plaintes peuvent être déposées auprès de l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs

d’enquête, Royaume-Uni) s’il existe une raison de penser que des données ont été obtenues de manière inappropriée.

## II. Les faits et les questions préjudicielles

11. D’après la juridiction de renvoi, le litige au principal porte sur l’acquisition et l’utilisation par les United Kingdom Security and Intelligence Agencies (services de sécurité et de renseignement, Royaume-Uni, ci-après les « SSR ») des données de communications en masse.

12. Ces données concernent « celui qui » utilise le téléphone et internet et « quand, où, comment et avec qui » il les utilise. Elles comprennent la localisation des téléphones mobiles et fixes depuis lesquels des appels sont passés et reçus, ainsi que celle des ordinateurs à partir desquels on accède à internet. Elles n’incluent pas le contenu des communications, qui ne peut être obtenu que par voie d’ordonnance.

13. La requérante au principal (Privacy International, une organisation non gouvernementale de protection des droits de l’homme) a introduit un recours devant la juridiction de renvoi, car elle considère que l’acquisition et l’utilisation des données précitées par les SSR violent le droit au respect de la vie privée consacré à l’article 8 de la convention de sauvegarde des droits de l’homme et des libertés fondamentales et qu’elles sont contraires au droit de l’Union.

14. Les autorités défenderesses [13] font valoir que l'exercice de leur compétence dans ce cadre est légitime et essentiel, en particulier pour protéger la sécurité nationale.

15. Selon les informations figurant dans la décision de renvoi, conformément aux instructions émises par le secrétaire d'État en vertu de l'article 94 de loi sur les télécommunications de 1984, les SSR obtiennent les données de communication en masse par l'intermédiaire des opérateurs de réseau public de communications électroniques.

16. Ces données incluent des informations sur le trafic et la localisation ainsi que sur les activités sociales, commerciales et financières, les communications et les voyages des utilisateurs. Une fois en leur possession, les données sont conservées par les SSR de manière sécurisée grâce à des techniques (telles que le filtrage et l'agrégation) généralisées, c'est-à-dire qu'elles ne sont pas dirigées vers des cibles spécifiques et connues.

17. La juridiction de renvoi considère qu'il ne fait aucun doute que ces techniques sont essentielles pour le travail des SSR dans la lutte

[13] Le Secretary of State for Foreign and Commonwealth Affairs (ministre des Affaires étrangères et du Commonwealth, Royaume-Uni), le Secretary of State for the Home Department (ministre de l'Intérieur, Royaume-Uni), et trois SSR du Royaume-Uni à savoir le Government Communications Headquarters (quartier général des communications du Royaume-Uni) (GCHQ), le Security Service (Service de sécurité, Royaume-Uni) (MI5), et le Secret Intelligence Service (Service secret de renseignement, Royaume-Uni) (MI6).

contre les menaces graves pour la sécurité nationale, en particulier le terrorisme, l'espionnage et la prolifération nucléaire. La capacité d'acquérir et d'utiliser les données, de la part des SSR, serait essentielle pour protéger la sécurité nationale du Royaume-Uni.

18. Pour la juridiction de renvoi, les mesures litigieuses sont conformes au droit national et à l'article 8 de la CEDH. Toutefois, elle doute de leur compatibilité avec le droit de l'Union au regard de l'arrêt Tele2 Sverige et Watson e.a.

19. Dans ce contexte, la juridiction de renvoi a posé à la Cour les questions préjudicielles suivantes :

« 1) Vus l'article 4 TUE et l'article 1er, paragraphe 3, de la directive [2002/58], une exigence dans des instructions données par le secrétaire d'État à un fournisseur d'un réseau de communications électroniques qu'il doit fournir les données de communications en masse aux SSR d'un État membre, relève-t-elle du champ d'application du droit de l'Union et de la directive [2002/58] ?

2) En cas de réponse affirmative à la première question, les exigences Watson [14] ou toute autre exigence en plus de celles imposées par la CEDH s'imposent elles à de telles instructions du secrétaire d'État ? 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

[14] C'est-à-dire la jurisprudence établie dans l'arrêt Tele2 Sverige et Watson e.a.

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 ? »

20. La juridiction de renvoi replace ses questions dans leur contexte de la manière suivante :

« a) les capacités [des SSR] pour utiliser les [données de communication en masse] qui leur sont fournies sont essentielles pour la protection de la sécurité nationale du Royaume-Uni, notamment dans les domaines du contre-terrorisme, du contre-espionnage et de la lutte contre la prolifération ;

b) une caractéristique fondamentale de l'utilisation de [ces données] 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 [desdites données] en un endroit unique. Son utilité principale repose dans l'identification et l'établissement du profil 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 [données de communication en masse] (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 de [ces données] par les SSR sont conformes aux exigences de la CEDH ; et

e) la juridiction nationale a jugé que l'imposition des exigences spécifiées dans l'arrêt [Tele2 Sverige et Watson e.a.], 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. »

## III. La procédure devant la Cour

21. La demande de décision préjudicielle a été enregistrée au greffe de la Cour le 31 octobre 2017.

22. Les gouvernements allemand, belge, britannique, tchèque, chypriote, espagnol, estonien, français, hongrois, irlandais, letton, néerlandais, norvégien, polonais, portugais et suédois, ainsi que la Commission, ont déposé des observations écrites.

23. Une audience a eu lieu le 9 septembre 2019, qui s'est tenue conjointement avec les audiences dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a., ainsi qu'avec l'affaire C-520/18, Ordre des barreaux francophones et germanophone e.a., auxquelles ont comparu les parties des quatre renvois préjudiciels, les gouvernements précités ainsi que la Commission et le contrôleur européen de la protection des données.

## IV. Analyse

### A. Concernant le champ d'application de la directive 2002/58 et l'exclusion de la sécurité nationale (première question préjudicielle)

24. Dans les conclusions que je présente ce jour également dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a., j'explique les raisons pour lesquelles, à mon avis, la directive 2002/58 « s'applique, en principe, lorsque les fournisseurs de services électroniques sont tenus par la loi de conserver les données de leurs abonnés et de permettre aux autorités publiques d'y accéder. Que les obligations soient imposées aux fournisseurs pour des raisons de sécurité nationale n'y change rien » [15].

25. Tout en exposant mes arguments, j'évoque l'incidence des arrêts rendus par la Cour le 30 mai 2006, Parlement/Conseil et Commission [16], et Tele2 Sverige et Watson e.a., en préconisant une interprétation qui inclue les deux [17].

15 Conclusions dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a. (point 42).

16 C-317/04 et C-318/04, EU:C:2006:346.

17 Conclusions dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a. (points 44 à 76.)

26. Dans ces mêmes conclusions, après avoir affirmé l'applicabilité de la directive 2002/58, j'examine l'exclusion de la sécurité nationale qui y figure et l'incidence de l'article 4, paragraphe 2, TUE [18].

27. Sans préjudice de ce que j'exposerai dans les développements suivants, je renvoie à ce qui a déjà été dit dans les conclusions rappelées ci-dessus et dans celles de l'affaire C-520/18, Ordre des barreaux francophones et germanophone e.a.

### *1. L'application de la directive 2002/58 dans la présente affaire*

28. Aux termes des dispositions litigieuses en l'espèce, les fournisseurs de services de communications électroniques sont destinataires d'une obligation impliquant, outre leur conservation, un traitement des données en leur possession en raison du service qu'ils fournissent aux utilisateurs des réseaux publics de communications de l'Union [19].

18 Ibidem, points 77 à 90.

19 En vertu de l'article 2 de la directive 2002/58, les définitions figurant dans la directive 95/46 s'appliquent aux fins de la présente directive. Conformément à l'article 2, sous b), de cette dernière, on entend par « traitement de données à caractère personnel » « toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, *la communication par transmission*, diffusion ou toute autre *forme de mise à disposition*, le

29. En effet, les opérateurs susvisés doivent obligatoirement transmettre ces données aux SSR. La question qui se pose ici est de savoir si l'article 15, paragraphe 1, de la directive 2002/58 permet que cette transmission, compte tenu de son objectif, soit purement et simplement exclue du droit de l'Union.

30. Je ne le pense pas. On peut qualifier la conservation des données susvisées, suivie de leur transmission ultérieure, de traitement des données à caractère personnel effectué par les fournisseurs de services de télécommunications électroniques, de sorte qu'elles relèvent tout naturellement du champ d'application de la directive 2002/58.

31. Comme la juridiction de renvoi le suggère, les raisons de sécurité nationale ne peuvent pas prévaloir sur ce constat, avec pour conséquence que l'obligation litigieuse n'entrerait plus dans le champ d'application du droit de l'Union. À mon avis, je le répète, les fournisseurs sont tenus de procéder à un traitement des données dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications de l'Union, ce qui correspond justement au champ d'application de la directive 2002/58, conformément à son article 3, paragraphe 1.

32. Partant de cette prémisse, le débat porte non pas sur les activités des SSR (qui, comme je l'ai souligné précédemment, pourraient ne pas

rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction » (surlignement ajouté par nos soins).

être couvertes par le droit de l'Union si elles ne concernaient pas les fournisseurs de communications électroniques), mais sur la conservation et de la transmission ultérieure des données en possession de ces opérateurs. De ce point de vue, ce sont les droits fondamentaux garantis par l'Union qui sont en cause.

33. L'élément clé pour trancher ce débat réside, une fois de plus, dans l'obligation de conservation généralisée et indifférenciée des données qui sont rendues accessibles aux autorités publiques.

### *2. L'invocation de la sécurité nationale*

34. Étant donné que, dans cette affaire, la juridiction nationale accorde une importance particulière à l'activité des SSR concernant la sécurité nationale, je me permets de reproduire quelques-uns des points figurant dans mes conclusions de ce jour dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a., à ce sujet :

« 77. La sécurité nationale [...] fait l'objet d'une double considération dans la directive 2002/58. D'une part, elle constitue un motif d'exclusion (de l'application de cette directive) pour toutes les activités des États membres qui, spécifiquement, la "concernent". D'autre part, elle est (se présente comme) une cause de limitation, qui doit être mise en œuvre par la loi, des droits et des obligations prévus par la directive 2002/58, c'est-à-dire en ce qui concerne des activités de nature privée ou commerciale ne relevant pas du domaine des activités régaliennes.

78. Quelles sont les activités visées à l'article 1er, paragraphe 3, de la directive 2002/58/CE ? Selon moi, le Conseil d'État lui-même en offre un bon exemple en mentionnant les articles L. 851-5 et L. 851-6 du code de la sécurité intérieure et en se référant aux "techniques de recueil de renseignement directement mises en œuvre par l'État sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques". [...]

79. Je crois qu'il s'agit là de la clé pour discerner le champ de l'exclusion prévue à l'article 1er, paragraphe 3, de la directive 2002/58. Ne sont pas soumises au régime de cette dernière les *activités* menées, en vue de préserver la sécurité nationale, par les pouvoirs publics pour leur propre compte, sans requérir la collaboration de particuliers et, dès lors, sans leur imposer d'obligations dans leur gestion commerciale.

80. L'éventail des activités des pouvoirs publics dérogeant au régime général du traitement des données à caractère personnel doit toutefois faire l'objet d'une interprétation stricte. En particulier, la notion de *sécurité nationale*, dont la responsabilité incombe exclusivement à chaque État membre, conformément à l'article 4, paragraphe 2, TUE, ne saurait être étendue à d'autres secteurs, plus ou moins proches, de la vie publique.

[...]

82. J'estime [...] que le critère de la décision-cadre 2006/960/JAI, dont l'article 2, sous a), établit une distinction entre, d'une part, les services de sécurité au sens large – à savoir "un service national de police, de

douane ou autre qui est autorisé par le droit national à dépister et à prévenir les infractions ou les activités criminelles, à enquêter à leur propos, et à exercer l'autorité publique et à prendre des mesures coercitives dans le cadre de ces activités" – et, d'autre part, les "agences ou les unités spécialisées dans les questions de sécurité nationale", peut servir d'orientation.

[...]

84. Il y a [...] une continuité entre la directive 95/46 et la directive 2002/58 en ce qui concerne les compétences des États membres en matière de sécurité nationale. Aucune des deux n'a pour objet la protection des droits fondamentaux dans ce domaine spécifique, dans lequel les activités des États membres ne sont pas "régies par le droit [de l'Union]".

85. L'"équilibre" mentionné dans [le] considérant [onze de la directive 2002/58] résulte de la nécessité de respecter les compétences des États membres en matière de sécurité nationale, lorsque ceux-ci les exercent *directement et par leurs propres moyens*. En revanche, lorsque, y compris pour ces mêmes raisons de sécurité nationale, le concours de particuliers, auxquels certaines obligations sont imposées, est requis, cela détermine l'entrée dans un domaine (la protection de la vie privée pouvant être exigée de ces acteurs privés) régi par le droit de l'Union.

86. Tant la directive 95/46 que la directive 2002/58 cherchent à atteindre cet équilibre en permettant que les droits des particuliers puissent être limités par des mesures législatives adoptées par les États

en vertu, respectivement, de l'article 13, paragraphe 1, de la directive 95/46 et de l'article 15, paragraphe 1, de la directive 2002/58. Il n'y a sur ce point aucune différence entre les deux directives.

[...]

89. L'identification de ces activités de l'autorité publique doit nécessairement être restrictive, sous peine de priver d'effet utile la réglementation de l'Union en matière de protection de la vie privée. Le règlement 2016/679 établit, à son article 23 – dans la même ligne que l'article 15, paragraphe 1, de la directive 2002/58 –, la limitation, *au moyen de mesures législatives*, des droits et des obligations qu'il prévoit, lorsque cela est nécessaire pour garantir, entre autres objectifs, la sécurité nationale, la défense nationale ou la sécurité publique. Une fois encore, si la protection de ces objectifs suffisait pour entraîner l'exclusion du champ d'application du règlement 2016/679, l'invocation de la sûreté de l'État aux fins de justifier la restriction, par des mesures législatives, des droits garantis par ce règlement serait superflue. »

### *3. Les conséquences liées à l'application de l'arrêt Tele2 Sverige et Watson e.a. à la présente affaire*

35. La juridiction de renvoi s'est concentrée sur l'interprétation faite par la Cour dans l'arrêt Tele2 Sverige et Watson e.a., en exposant les difficultés que comporterait, selon elle, son application à la présente affaire.

36. En effet, l'arrêt Tele2 Sverige et Watson e.a. indique les conditions que doit remplir une réglementation nationale instaurant l'obligation de conserver les données relatives au trafic et les données de localisation, pour que 'celles-ci soient ultérieurement accessibles aux autorités publiques.

37. Comme dans les affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a., et pour les mêmes raisons, je considère que les règles nationales sur lesquelles porte le présent renvoi ne respectent pas les conditions fixées dans l'arrêt Tele2 Sverige et Watson e.a. puisqu'elles impliquent une conservation généralisée et indifférenciée de données à caractère personnel qui fournit un récit détaillé de la vie des personnes concernées pendant une longue période.

38. Dans les conclusions afférentes à ces affaires, je m'interroge sur le point de savoir s'il serait possible d'atténuer ou de compléter les enseignements dégagés dans cet arrêt compte tenu de ses conséquences sur la lutte contre le terrorisme ou sur la protection de l'État en présence d'autres menaces similaires contre la sécurité nationale.

39. Je me permets également de reproduire ci-après certains des points tirés de ces conclusions, dans lesquels je soutiens, en substance, que, puisqu'il est possible de nuancer la jurisprudence précitée, il convient de la confirmer dans son principe :

« 135. Bien que ce soit difficile, il n'est pas impossible de déterminer avec précision et conformément à des critères objectifs tant les catégories de données dont la conservation est jugée indispensable que

le cercle des personnes concernées. La conservation générale et indifférenciée de toutes les données susceptibles d'être recueillies par les fournisseurs de services de communication électronique serait certes la solution la plus *pratique et* la plus *efficace* ; toutefois [...] la question ne saurait se poser en termes d'*efficacité pratique* mais en termes d'*efficacité juridique* et dans le contexte d'un État de droit.

136. Ce travail de détermination relève typiquement du domaine de la loi, dans les limites fixées par la jurisprudence de la Cour [...]

137. En partant du principe que les opérateurs ont recueilli les données en respectant les dispositions de la directive 2002/58 et que ces données ont été conservées conformément à l'article 15, paragraphe 1, [...] l'accès des autorités compétentes à ces informations doit se faire dans les conditions que la Cour a exigées, et que j'analyse, pour ma part, dans mes conclusions relatives à l'affaire C-520/18, Ordre des barreaux francophones et germanophone e.a., auxquelles je renvoie.

138. Par conséquent, dans ce cas aussi, la réglementation nationale doit prévoir les conditions matérielles et procédurales régissant l'accès des autorités compétentes aux données conservées. [...] Dans le cadre de ces renvois préjudiciels, ces conditions autoriseraient l'accès aux données des personnes soupçonnées de projeter, de commettre, d'avoir commis ou d'être impliquées dans un acte terroriste. [...]

139. Toutefois, l'essentiel est que, sauf dans les cas d'urgence dûment justifiés, l'accès aux données en question soit soumis au contrôle préalable d'une juridiction ou d'une autorité administrative

indépendante, dont la décision réponde à une demande motivée des autorités compétentes. [...] Ainsi, là où le contrôle abstrait de la loi ne peut être obtenu, le contrôle in concreto de cette autorité indépendante, tout aussi attachée à la garantie de la sécurité de l'État qu'à la défense des droits fondamentaux des citoyens, est garanti »

## B. Concernant la seconde question préjudicielle

40. La juridiction de renvoi formule sa seconde question pour le cas où la réponse à la première serait affirmative. Dans ce cas, elle souhaiterait savoir quelle « autre exigence en plus de celles imposées par la CEDH » ou de celles découlant de l'arrêt Tele2 Sverige et Watson e.a. il conviendrait d'exiger.

41. À cet égard, elle déclare que l'imposition des conditions spécifiées dans l'arrêt Tele2 Sverige et Watson e.a. « ferait échec aux mesures prises par les SSR pour protéger la sécurité nationale ».

42. Étant donné la réponse que je suggère d'apporter à la première question, il n'est pas indispensable d'aborder la seconde. Comme le souligne la juridiction de renvoi elle-même, celle-ci est subordonnée à la reconnaissance de la compatibilité avec le droit de l'Union de « l'acquisition de masse et [d]es techniques de traitement automatisé » des données à caractère personnel de tous les utilisateurs du Royaume-Uni, que les opérateurs de services de communications électroniques devraient transmettre aux SSR.

43. Dans l'hypothèse où la Cour estimerait qu'il est indispensable de répondre à la seconde question, je pense qu'elle devrait confirmer les conditions précitées tirées de l'arrêt Tele2 Sverige et Watson e.a. concernant :

– l'interdiction de l'accès généralisé aux données ;

– la nécessité d'une autorisation préalable d'un juge ou d'une entité indépendante pour légitimer cet accès ;

– l'obligation d'informer les personnes concernées, sauf si cela compromettait l'efficacité de la mesure ;

– la conservation des données dans l'Union.

44. Il suffirait, je le répète, de confirmer ces conditions, qui sont impératives, pour les raisons que j'ai exposées dans les conclusions relatives aux affaires jointes C-511/18 et C-512/18, La Quadrature du Net e.a., ainsi qu'à l'affaire C-520/18, Ordre des barreaux francophones et germanophone e.a., sans qu'il soit nécessaire d'en fixer d'« autres » au sens où l'entend la juridiction de renvoi.

## V. Conclusion

45. À la lumière des considérations qui précèdent, je propose à la Cour de répondre à l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête, Royaume-Uni) dans les termes suivants :

L’article 4 TUE et l’article 1er, paragraphe 3, 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), doivent être interprétés en ce sens qu’ils s’opposent à une réglementation nationale imposant à un fournisseur de réseau de communication électronique l’obligation de fournir aux services de sécurité et de renseignement d’un État membre les « données de communications en masse » qui impliquent au préalable leur collecte généralisée et indifférenciée.

À titre subsidiaire :

L’accès, par les services de sécurité et de renseignement d’un État membre, aux données transmises par les fournisseurs de réseau de communication électronique doit respecter les conditions établies dans l’arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, EU:C:2016:970).