COMMISSION EUROPÉENNE

Bruxelles, le 6 décembre 2018
sj.a(2018)7030259

Document de la procédure juridictionnelle

À MONSIEUR LE PRÉSIDENT ET AUX MEMBRES DE LA COUR DE JUSTICE DE L'UNION EUROPÉENNE

OBSERVATIONS ÉCRITES

déposées conformément à l'article 23 du protocole sur le statut de la Cour de justice de l'Union européenne, par la

COMMISSION EUROPÉENNE

représentée par M. Martin Wasmeier, M^me^ Piedade Costa de Oliveira, et M. Herke Kranenborg, en qualité d'agents, ayant élu domicile auprès du Service juridique, Greffe contentieux, BERL 1/169, 1049 Bruxelles, et consentant à la signification de tout acte de procédure via e-Curia,

dans les affaires jointes C-511/18 et C-512/18

La Quadrature du Net e.a.

ayant pour objet plusieurs questions préjudicielles présentées, conformément à l'article 267 TFUE, par le Conseil d'Etat (France) et portant sur l'interprétation de la directive 2002/58/CE et de la directive 2000/31/CE.

Index

1. LES FAITS, LA PROCEDURE ET LES QUESTIONS PREJUDICIELLES

L'affaire C-511/18

1. Il ressort de l'ordonnance de renvoi que les parties requérantes, la Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à internet associatifs, ainsi que l'association Igwan.net (ci-après, les parties requérantes) demandent au Conseil d'Etat d'annuler plusieurs décrets qui mettent en œuvre certaines dispositions du code de la sécurité intérieure.

2. Concrètement, les parties requérantes contestent la légalité des décrets n°s 2015-1185[1], 2015-1211[2], 2015-1639[3] et 2016-67[4]. Elles allèguent, en substance, que ces décrets et certaines dispositions législatives qu'ils mettent en oeuvre, à savoir les articles L. 851-1, L. 851-2 et L. 851-3 et L. 851-4 du code de la sécurité intérieure, méconnaissent le droit au respect de la vie privée et le droit à la protection des données personnelles ainsi que le droit au recours effectif, respectivement garantis aux articles 7, 8 et 47 de la Charte des droits fondamentaux (ci-après "la Charte").

3. Les parties défenderesses dans les différentes affaires au principal (le garde des sceaux, ministre de la justice, le Premier ministre et le ministre de l'intérieur), concluent au rejet des requêtes. Ils soutiennent qu'elles sont irrecevables et/ou non fondées.

4. Quant à la méconnaissance alléguée du droit au respect de la vie privée et le droit à la protection des données personnelles, la juridiction de renvoi met en exergue l'article 4 TUE selon lequel "*l'Union respecte les fonctions essentielles de l'Etat, notamment celles qui ont pour objet d'assurer son intégrité territoriale, de maintenir l'ordre et de sauvegarder la sécurité nationale. En particulier, la sécurité nationale reste de la seule responsabilité de chaque Etat membre.*" Elle met également en exergue l'article 51 de la Charte en ce qui concerne l'application de

---

1 Décret n° 2015-1185 du 28 septembre 2015 portant désignation des services spécialisés de renseignement.

2 Décret n° 2015-1211 du 1er octobre 2015 relatif au contentieux de la mise en œuvre des techniques de renseignement soumises à autorisation et des fichiers intéressant la sûreté de l'Etat.

3 Décret n° 2015-1639 du 11 décembre 2015 relatif à la désignation des services autres que les services spécialisés de renseignement, autorisés à recourir aux techniques mentionnées au titre V du livre VIII du code de la sécurité intérieure.

4 Décret n° 2016-67 du 29 janvier 2016 relatif aux techniques de recueil de renseignement.

celle-ci aux Etats membres ainsi que l'article 54 relatif à l'interdiction de l'abus de droit (point 16 de l'ordonnance).

5. Ensuite, se référant aux dispositions combinées de l'article 3, paragraphe 1, et 15, paragraphe 1, de la directive 2002/58/CE, la juridiction de renvoi constate que « *les Etats membres sont autorisés, pour des motifs tenant à la sûreté de l'Etat ou à la lutte contre les infractions pénales, à déroger, notamment à l'obligation de confidentialité des données à caractère personnel, ainsi que de confidentialité des données relatives au trafic y afférentes, qui découlent de l'article 5, paragraphe 1, et 6 de la directive* » (point 17 de l'ordonnance).

6. La juridiction de renvoi, sur la base de l'arrêt *Tele2 Sverige/Watson*[5] de la Cour, considère qu'en l'espèce, relèvent de la directive tant l'obligation de conservation généralisée et indifférenciée de données[6] induite par l'article L. 851-1 du code de la sécurité intérieure (ci-après, « données de trafic, de localisation et de connexion ») que les accès administratifs auxdites données, y compris l'accès temps réel aux données de connexion (points 19 et 20 de l'ordonnance).

7. La juridiction de renvoi se demande si une telle obligation de conservation des données ne doit pas être regardée, *notamment eu égard aux garanties et contrôles dont sont assortis les accès administratifs aux données conservées et l'utilisation de celles-ci, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls Etats-membres en vertu de l'article 4 TUE* (point 25 de l'ordonnance).

8. En ce qui concerne les autres obligations susceptibles d'être imposées aux fournisseurs d'un service de communications électroniques, en particulier le recueil, en temps réel, prévu à l'article L. 851-2 du code de la sécurité intérieure, des informations et documents mentionnés à l'article L. 851-1 de ce code, la juridiction de renvoi souligne qu'elles ne concernent qu'un ou plusieurs individus préalablement identifiés comme étant susceptibles d'être en lien avec une menace terroriste. Il en irait de même de l'article 851-4 du même code qui autorise la transmission en temps réel par les opérateurs des seules données techniques relatives à la localisation des

---

5 Affaires jointes C-203/15 et C-698/15, Tele2 Sverige/Watson, EU:C:2016:970.

6 NB : cette conservation ne concerne pas le contenu des communications.

équipements terminaux. Ces dispositions n'exigent pas une conservation généralisée et indifférenciée de données, comme ne l'exigeraient pas non plus les dispositions de l'article L. 851-3 du code de la sécurité intérieure (point 26 de l'ordonnance).

9. La juridiction de renvoi observe que les accès en temps réel aux données de connexion permettent de suivre, avec une forte réactivité, les comportements d'individus susceptibles de représenter une menace immédiate pour l'ordre public. Elle ajoute que la technique prévue à l'article L. 851-3 dudit code permet de détecter, sur le fondement de critères précisément définis à cette fin, les individus dont les comportements sont susceptibles de révéler une menace terroriste. Elle souligne que dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, ces techniques présentent une utilité opérationnelle sans équivalent (point 27 de l'ordonnance).

10. Elle se demande, dès lors, si la directive 2002/58/CE doit être interprétée en ce sens qu'elle autorise des mesures législatives relevant d'activités concernant la sécurité publique, la défense et la sûreté de l'Etat, telles que les mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés (point 29 de l'ordonnance).

11. En ce qui concerne les garanties procédurales entourant l'accès aux données par les autorités compétentes, la juridiction de renvoi, se demande s'il découle de l'arrêt *Tele2 Sverige/Watson* que la directive 2002/58/CE, lue à la lumière de la Charte, doit être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil de données à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou si de telles procédures peuvent être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, décrites aux points 8, 9 et 10 de l'ordonnance (points 30 et 31 de l'ordonnance).

12. Considérant que les réponses de la Cour seront déterminantes pour la solution des litiges dans les affaires au principal au sujet des quatre décrets attaqués, en tant qu'ils ont été pris pour la mise en œuvre des articles L. 851-1 à L. 851-4 du code de la sécurité intérieure, par ordonnance du 26 juillet 2018, le Conseil d'Etat a décidé de surseoir à statuer et de poser à la Cour les trois questions préjudicielles suivantes:

1° L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet2002, ne doit-elle pas être regardée, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls Etats-membres en vertu de l'article 4 du traité sur l'Union européenne?

2° La directive du 12 juillet 2002 lue à la lumière de la Charte des droits fondamentaux de l'Union européenne doit-elle être interprétée en ce sens qu'elle autorise des mesures législatives, telles que les mesures de recueil en temps réel des données relatives au trafic et à la localisation d'individus déterminés, qui, tout en affectant les droits et obligations des fournisseurs d'un service de communications électroniques, ne leur imposent pas pour autant une obligation spécifique de conservation de leurs données?

3° La directive du 12 juillet 2002, lue à la lumière de la Charte des droits fondamentaux de l'Union européenne, doit-elle être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou de telles procédures peuvent-elles être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que ces dernières assurent l'effectivité du droit au recours?

L'affaire C-512/18

13. Les mêmes parties requérantes que dans l'affaire C-511/18 (French Data Network, la Quadrature du Net et la Fédération des fournisseurs d'accès à internet associatifs), soutenues par Privacy International et le Center for Democracy and Technology, demandent au Conseil d'Etat d'annuler l'article R. 10-13 du code des postes et des communications électroniques ainsi que le décret n° 2011-219 du 25 février 2011.

14. Elles allèguent, pour l'essentiel, que les dispositions attaquées imposent une obligation de conservation de données de trafic, de localisation et de connexion, qui revêt un caractère général sans être limitée à des personnes ou circonstances particulières. Une telle obligation porterait une atteinte disproportionnée au droit au respect de la vie privée et familiale, au droit à la protection des données à caractère personnel et à la liberté d'expression, tels qu'ils sont garantis par les articles 7, 8 et 11 de la Charte, et méconnaîtrait l'article 15, paragraphe 1, de la directive 2002/58/CE, tel qu'interprété par la Cour.

15. La Commission comprend l'ordonnance de renvoi comme faisant une distinction entre deux catégories de données: d'une part, celles que les dispositions pertinentes qualifient comme « *données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques* »[7] et, d'autre part, « *des données de connexion* » et d'autres données « *de nature à permettre l'identification de quiconque a contribué à la création de contenu* »[8] (points 4 et 12 de l'ordonnance).

16. Concernant la première catégorie, la juridiction de renvoi développe, pour l'essentiel, les mêmes considérations que celles relatives à l'obligation générale de conservation des données dans l'affaire C-511/18 (voir les points 6 à 10 de l'ordonnance).

17. Elle se demande, dès lors, à l'instar de la première question dans l'affaire C-511/18, si ladite obligation de conservation généralisée et indifférenciée des données ne doit pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte et les exigences de la sécurité nationale, dont la seule responsabilité incombe aux seuls Etats membres en vertu de l'article 4 TUE (point 11 de l'ordonnance).

18. Concernant la deuxième catégorie de données, la juridiction de renvoi estime que de telles données n'entrent pas dans le champ d'application de la directive 2002/58, tel que défini à son article 3, mais relèveraient plutôt du champ d'application de la directive 2000/31/CE, compte tenu, notamment, des services visés par la législation nationale qui correspondraient à ceux visés aux articles 12 et 14 de cette directive (points 13 et 14 de l'ordonnance).

19. Considérant que la directive 2000/31/CE n'instaure pas, par elle-même, une interdiction de principe quant à la conservation des données relatives à la création de contenu, la juridiction de renvoi cherche à savoir si les dispositions précitées ainsi que l'article 15 de cette directive permettent à un Etat membre d'instaurer une réglementation nationale, telle que celle en l'espèce, qui impose « *aux personnes*

---

7 Voir le I de l'article L.34- du code des postes et des communications électroniques.

8 Voir le II de l'article L.34-1 et l'article 6 de la loi n° 2004-575 du 21 juin 2004 et le décret n° 2011/219.

dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services, qu'ils détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale » (point 14 et 15 de l'ordonnance).

20. En vertu des considérations qui précèdent, par ordonnance du 26 juillet 2018, le Conseil d'Etat a décidé de poser à la Cour les deux questions préjudicielles suivantes:

« 1° L'obligation de conservation généralisée et indifférenciée, imposée aux fournisseurs sur le fondement des dispositions permissives de l'article 15, paragraphe 1, de la directive du 12 juillet 2002, ne doit-elle pas être regardée, notamment eu égard aux garanties et contrôles dont sont assortis ensuite le recueil et l'utilisation de ces données de connexion, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte des droits fondamentaux de l'Union européenne et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls Etats-membres en vertu de l'article 4 du traité sur l'Union européenne?

2° Les dispositions de la directive du 8 juin 2000, lues à la lumière des articles 6, 7, 8 et Il ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doivent-elles être interprétées en ce sens qu'elles permettent à un Etat d'instaurer une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale? »

2. CADRE JURIDIQUE

2.1. Dispositions du droit de l'Union

21. Dans le domaine des communications électroniques, 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»)[9] établit une réglementation spécifique. Il convient de souligner les dispositions suivantes de cette directive:

« Article 3
Services concernés

La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans la Communauté, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification.

(...)

Article 5
Confidentialité des communications

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

(...)

Article 6
Données relatives au trafic

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.

(…)

---

[9] JO L 201 du 31.7.2002, p. 37, texte consolidé 2002L0058-ES-19.12.2009.

Article 15
Application de certaines dispositions de la directive 95/46/CE

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. »

[…]

22. La directive 95/46/CE[10] a été abrogée, conformément à l'article 94 du règlement (UE) 2016/679[11], avec effet au 25 mai 2018. Le paragraphe 2 de l'article 94 de ce règlement stipule que « *[le]s références faites à la directive abrogée s'entendent comme faites au présent règlement. […]* »

23. L'article 23 du règlement 2016/679 est libellé comme suit :

« Article 23
Limitations

1. Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir:

a) la sécurité nationale ;

b) la défense nationale ;

c) la sécurité publique ;

---

[10] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO L 281 du 23.11.1995, p. 31.

[11] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), JO L 119 du 4.5.2016, p. 1.

d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ;

e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale;

f) la protection de l'indépendance de la justice et des procédures judiciaires ;

g) la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière;

h) une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g) ;

i) la protection de la personne concernée ou des droits et libertés d'autrui;

j) l'exécution des demandes de droit civil.

2. […] »

24. L'article 95 du même règlement porte sur sa relation avec la directive 2002/58/CE. Il est libellé comme suit :

« Article 95
Relation avec la directive 2002/58/CE

Le présent règlement n'impose pas d'obligations supplémentaires aux personnes physiques ou morales quant au traitement dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union en ce qui concerne les aspects pour lesquels elles sont soumises à des obligations spécifiques ayant le même objectif énoncées dans la directive 2002/58/CE. »

25. La directive 2000/31/CE[12] dispose à son article 1, paragraphe 5, sous b) que celle-ci ne s'applique pas « *aux questions relatives aux services de la société de l'information couvertes par la directive 96/46/CE et 97/66/CE »*[13].

2.2. Dispositions du droit national

26. Compte tenu du nombre de dispositions nationales concernées, la Commission se limitera à citer celles du code de la sécurité intérieure qui lui semblent les plus pertinentes, notamment, celles mises en œuvre par les décrets attaqués, deux

---

[12] Directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur («directive sur le commerce électronique»), JO L 178 du 17.7.2000, p. 1.

[13] Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, JO L 24 du 30/01/1998 p. 1. Cette directive a été abrogée et remplacée par la directive 2002/58.

dispositions du code des postes et des communications électroniques ainsi que l'article 6 de la loi n° 2004-575 de 21 juin 2004[14].

27. Les articles L. 851-1, L. 851-2, L. 851-3 et L. 851-4 du code de la sécurité intérieure sont libellés comme suit:

« Article L851-1

Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que des personnes mentionnées aux 1 et 2 du I de l'article 6 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, des informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques, y compris les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

Par dérogation à l'article L. 821-2, les demandes écrites et motivées portant sur les données techniques relatives à l'identification des numéros d'abonnement ou de connexion à des services de communications électroniques, ou au recensement de l'ensemble des numéros d'abonnement ou de connexion d'une personne désignée sont directement transmises à la Commission nationale de contrôle des techniques de renseignement par les agents individuellement désignés et habilités des services de renseignement mentionnés aux articles L. 811-2 et L. 811-4. La commission rend son avis dans les conditions prévues à l'article L. 821-3.

Un service du Premier ministre est chargé de recueillir les informations ou documents auprès des opérateurs et des personnes mentionnés au premier alinéa du présent article. La Commission nationale de contrôle des techniques de renseignement dispose d'un accès permanent, complet, direct et immédiat aux informations ou documents collectés.

Les modalités d'application du présent article sont fixées par décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés et de la Commission nationale de contrôle des techniques de renseignement.

Article L851-2

I.-Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, peut être individuellement autorisé le recueil en temps réel, sur les réseaux des opérateurs et des personnes mentionnés à l'article L. 851-1, des informations ou documents mentionnés au même article L. 851-1 relatifs à une personne préalablement identifiée susceptible d'être en lien avec une menace. Lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par

[14] Toutes les dispositions législatives pertinentes ainsi que les décrets contestés sont accessibles sur le site « Legifrance.gouv.fr ».

l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes.

I bis.-Le nombre maximal des autorisations délivrées en application du présent article en vigueur simultanément est arrêté par le Premier ministre, après avis de la Commission nationale de contrôle des techniques de renseignement. La décision fixant ce contingent et sa répartition entre les ministres mentionnés au premier alinéa de l'article L. 821-2 ainsi que le nombre d'autorisations d'interception délivrées sont portés à la connaissance de la commission.

II.-L'article L. 821-5 n'est pas applicable à une autorisation délivrée en application du présent article.

Article L851-3

I.- Dans les conditions prévues au chapitre Ier du titre II du présent livre et pour les seuls besoins de la prévention du terrorisme, il peut être imposé aux opérateurs et aux personnes mentionnés à l'article L. 851-1 la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste.

Ces traitements automatisés utilisent exclusivement les informations ou documents mentionnés à l'article L. 851-1, sans recueillir d'autres données que celles qui répondent à leurs paramètres de conception et sans permettre l'identification des personnes auxquelles les informations ou documents se rapportent.

Dans le respect du principe de proportionnalité, l'autorisation du Premier ministre précise le champ technique de la mise en œuvre de ces traitements.

II. -La Commission nationale de contrôle des techniques de renseignement émet un avis sur la demande d'autorisation relative aux traitements automatisés et les paramètres de détection retenus. Elle dispose d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies. Elle est informée de toute modification apportée aux traitements et paramètres et peut émettre des recommandations.

La première autorisation de mise en œuvre des traitements automatisés prévue au I du présent article est délivrée pour une durée de deux mois. L'autorisation est renouvelable dans les conditions de durée prévues au chapitre Ier du titre II du présent livre. La demande de renouvellement comporte un relevé du nombre d'identifiants signalés par le traitement automatisé et une analyse de la pertinence de ces signalements.

III. -Les conditions prévues à l'article L. 871-6 sont applicables aux opérations matérielles effectuées pour cette mise en œuvre par les opérateurs et les personnes mentionnés à l'article L. 851-1.

IV. -Lorsque les traitements mentionnés au I du présent article détectent des données susceptibles de caractériser l'existence d'une menace à caractère terroriste, le Premier ministre ou l'une des personnes déléguées par lui peut autoriser, après avis de la Commission nationale de contrôle des techniques de renseignement donné dans les conditions prévues au chapitre Ier du titre II du présent livre, l'identification de la ou des personnes concernées et le recueil des données y afférentes. Ces données sont exploitées dans un délai de soixante jours à compter de ce recueil et sont détruites à l'expiration de ce délai, sauf en cas d'éléments sérieux

confirmant l'existence d'une menace terroriste attachée à une ou plusieurs des personnes concernées.

V. -L'article L. 821-5 n'est pas applicable à une autorisation délivrée en application du présent article.

Article L851-4

Dans les conditions prévues au chapitre Ier du titre II du présent livre, les données techniques relatives à la localisation des équipements terminaux utilisés mentionnées à l'article L. 851-1 peuvent être recueillis sur sollicitation du réseau et transmis en temps réel par les opérateurs à un service du Premier ministre. »

28. L'article **L. 811-3** du code de la sécurité intérieure dispose :

« Pour le seul exercice de leurs missions respectives, les services spécialisés de renseignement peuvent recourir aux techniques mentionnées au titre V du présent livre pour le recueil des renseignements relatifs à la défense et à la promotion des intérêts fondamentaux de la Nation suivants :

1° L'indépendance nationale, l'intégrité du territoire et la défense nationale ;

2° Les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France et la prévention de toute forme d'ingérence étrangère ;

3° Les intérêts économiques, industriels et scientifiques majeurs de la France ;

4° La prévention du terrorisme ;

5° La prévention :

a) Des atteintes à la forme républicaine des institutions ;

b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;

c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;

6° La prévention de la criminalité et de la délinquance organisées ;

7° La prévention de la prolifération des armes de destruction massive. »

29. L'article L. 34-1 du code des postes et des communications électroniques est rédigé comme suit :

« Article L34-1

I. – Le présent article s'applique au traitement des données à caractère personnel dans le cadre de la fourniture au public de services de communications électroniques ; il s'applique notamment aux réseaux qui prennent en charge les dispositifs de collecte de données et d'identification.

II. – Les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne, effacent ou rendent anonyme toute donnée relative au trafic, sous réserve des dispositions des III, IV, V et VI.

Les personnes qui fournissent au public des services de communications électroniques établissent, dans le respect des dispositions de l'alinéa précédent, des procédures internes permettant de répondre aux demandes des autorités compétentes.

Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent article.

III. – Pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales ou d'un manquement à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle ou pour les besoins de la prévention des atteintes aux systèmes de traitement automatisé de données prévues et réprimées par les articles 323-1 à 323-3-1 du code pénal, et dans le seul but de permettre, en tant que de besoin, la mise à disposition de l'autorité judiciaire ou de la haute autorité mentionnée à l'article L. 331-12 du code de la propriété intellectuelle ou de l'autorité nationale de sécurité des systèmes d'information mentionnée à l'article L. 2321-1 du code de la défense, il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques. Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, détermine, dans les limites fixées par le VI, ces catégories de données et la durée de leur conservation, selon l'activité des opérateurs et la nature des communications ainsi que les modalités de compensation, le cas échéant, des surcoûts identifiables et spécifiques des prestations assurées à ce titre, à la demande de l'Etat, par les opérateurs.

IV. – […]

VI. – Les données conservées et traitées dans les conditions définies aux III, IV et V portent exclusivement sur l'identification des personnes utilisatrices des services fournis par les opérateurs, sur les caractéristiques techniques des communications assurées par ces derniers et sur la localisation des équipements terminaux.

Elles ne peuvent en aucun cas porter sur le contenu des correspondances échangées ou des informations consultées, sous quelque forme que ce soit, dans le cadre de ces communications.

La conservation et le traitement de ces données s'effectuent dans le respect des dispositions de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

Les opérateurs prennent toutes mesures pour empêcher une utilisation de ces données à des fins autres que celles prévues au présent article. »

30. L'article R. 10-13 du code des postes et des communications électroniques est libellé comme suit:

« Article R10-13

I. – En application du III de l'article L. 34-1 les opérateurs de communications électroniques conservent pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales :

a) Les informations permettant d'identifier l'utilisateur ;

b) Les données relatives aux équipements terminaux de communication utilisés ;

c) Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;

d) Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;

e) Les données permettant d'identifier le ou les destinataires de la communication.

II. – Pour les activités de téléphonie l'opérateur conserve les données mentionnées au II et, en outre, celles permettant d'identifier l'origine et la localisation de la communication.

III. – La durée de conservation des données mentionnées au présent article est d'un an à compter du jour de l'enregistrement.

IV. – Les surcoûts identifiables et spécifiques supportés par les opérateurs requis par les autorités judiciaires pour la fourniture des données relevant des catégories mentionnées au présent article sont compensés selon les modalités prévues à l'article R. 213-1 du code de procédure pénale. »

31. L'article **6 de la loi n° 2004-575 du 21 juin 2004** pour la confiance dans l'économie numérique dispose:

« I.-1. Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.

[…]

2. Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible.

[…]

II. -Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.

Elles fournissent aux personnes qui éditent un service de communication au public en ligne des moyens techniques permettant à celles-ci de satisfaire aux conditions d'identification prévues au III.

L'autorité judiciaire peut requérir communication auprès des prestataires mentionnés aux 1 et 2 du I des données mentionnées au premier alinéa.

Les dispositions des articles 226-17,226-21 et 226-22 du code pénal sont applicables au traitement de ces données.

Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation. »

3. EN DROIT

3.1. Considérations générales

32. La Commission note, tout d'abord, que les articles 5, paragraphe 1, et 6 de la directive 2002/58 visent à garantir la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, et des données relatives au trafic y afférentes.

33. Ensuite, en vertu de l'article 15, paragraphe 1, de la même directive, les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus, entre autres, aux articles 5 et 6 de cette 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'Etat – 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 [23, paragraphe 1, du règlement 2016/979]. 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 à cette disposition doivent être prises dans le respect des principes généraux du droit de l'Union, conformément à l'article 15, paragraphe 1, troisième phrase, de la directive.

34. Il apparaît donc qu'en application de l'article 15, paragraphe 1, de la directive 2002/58, les États membres peuvent adopter des mesures législatives prévoyant la conservation de données relatives aux communication et de trafic y afférentes pendant une durée limitée en vue de sauvegarder la sécurité nationale ainsi que pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou pour un des autres objectifs mentionnés à cette disposition, dans les conditions y énoncées et pourvu que ladite conservation soit par ailleurs compatible avec le droit de l'Union.

35. La jurisprudence de la Cour relative à l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 confirme que les mesures législatives qu'il vise et qui dérogent au principe de confidentialité des communications et des données relatives au trafic y afférentes sont d'interprétation stricte[15]. De telles mesures ne pourraient être justifiées que si elles poursuivent l'un des objectifs mentionnés à cette disposition[16], e qui, conformément à l'article 52, paragraphe 1, de la Charte, respectent le contenu essentiel des droits garantis par les articles 7 et 8 de la Charte et, dans le respect du principe de proportionnalité, sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui[17].

3.2. Sur la première question dans les deux affaires (C-511/18 et C-512/18)

3.2.1. Remarques préliminaires

36. Par sa première question dans les deux affaires, le Conseil d'Etat souhaite essentiellement savoir si l'article 15, paragraphe 1, de la directive 2002/58 doit être interprété en ce sens qu'il permet aux Etats membres d'imposer aux fournisseurs de services de communications électroniques au public, et autres personnes telles que celles offrant un accès à des services de communication au public ligne ou des services d'hébergement de contenu pour mise à disposition du public par des services de communication au public en ligne[18], l'obligation de conserver les données de trafic, de localisation et de connexion, afin de les rendre accessibles aux autorités compétentes, en tant qu'ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte et les exigences de la sécurité nationale.

37. La Commission souhaite observer, d'emblée, au sujet de l'article 6 de la Charte mentionné à la première question préjudicielle, que la référence dans la jurisprudence de la Cour à cette disposition de la Charte ne devrait pas être entendue comme signifiant que la Cour aurait reconnu que le droit garantit par l'article 6 de la Charte impliquerait l'existence d'un droit à la sécurité qui serait, en soi-même,

---

15 Tele2 Sverige/Watson, point 89.

16 Tele2 Sverige/Watson, points 90 et 115. La Cour y a précisé qu'« *une telle énumération revêt un caractère exhaustif* ».

17 Tele2 Sverige/Watson, point 94.

18 Personnes mentionnées à l'article L. 34-1 du code des postes et des communications électroniques ainsi que celles mentionnées au I de l'article 6 de la loi n° 2004-575 du 21 juin 2004.

capable d'imposer une obligation positive à l'Union d'adopter des mesures en vue de protéger les personnes contre des actes criminels.

38. En effet, d'une part, quand la Cour a mentionné que « l'article 6 énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté », cette référence était faite dans le contexte de l'examen d'objectifs d'intérêt général poursuivis par la législation en cause et non pas en tant qu'objectif en lui-même[19]. D'autre part, le droit consacré à l'article 6 de la Charte correspond à l'article 5 de la CEDH et, en accord avec les explications relatives à la Charte (JO 2007, C 303, p. 17), les droits et obligations prévus audit article 6 ont, conformément à l'article 52, paragraphe 3, de la Charte, le même sens et la même portée que l'article 5 de la CEDH[20],[21].

39. Dans le présent contexte, il suffit donc de constater que la poursuite d'objectifs d'intérêt général tels que celui de sauvegarder la sécurité publique ou celui d'assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales, visés à l'article 15, paragraphe 1, de la directive 2002/58 contribue également à la protection des droits et des libertés d'autrui[22].

40. Sur la base de ce qui précède, la Commission comprend la référence à l'article 6 de la Charte dans l'ordonnance de renvoi comme visant à garantir la protection de l'intégrité physique des personnes. Ainsi, la Commission suggère de reformuler la première question dans les deux affaires, comme cherchant à savoir si l'article 15, paragraphe 1, de la directive 2002/58 doit être interprété en ce sens que l'ingérence dans les droits fondamentaux garantis par les articles 7 et 8 de la Charte découlant de l'obligation de conservation généralisée et indifférenciée de données de trafic, de localisation et de connexion peut être justifiée par l'objectif de sauvegarder la sécurité nationale ainsi que par l'objectif assurer la prévention, la recherche, la

---

19 Voir, notamment, l'arrêt dans les affaires jointes C-293/12 et C-594/12, Digital Rights Ireland e.a., EU:C:2014:238, points 42 et 44.

20 C-237/15, Minister for Justice and Equality v Francis Lanigan, EU:C:2015:474, points. 54-57, C-294/16, JZ V Prokuratura Rejonowa Łódź — Śródmieście, EU:C:2016:610, points 42-52, C-601/15, J. N. v. Staatssecretaris voor Veiligheid en Justitie [GC], EU:C:2016:84, points 44 and 47.

21 Sur l'interprétation de l'article 5 CEDH, voir, CeDH Al Nashiri v. Romania, N° 33234/12, 31 mai 2018, points 686-687; Ireziyevy v. Russia, N° 21135/09, 2 April 2015, points. 78 and 80; Çiçek v. Turkey [GC], N° 25704/94, 27 février 2001 point 104, Mikiyeva and Others v. Russia, N°s. 61536/08, 6647/09, 6659/09, 63535/10 et 15695/11, 30 janvier 2014, point 170.

22 Voir l'Avis A-1/15 sur le projet d'accord entre l'Union européenne et le Canada sur le transfert de données PNR, EU:C:2017:592, point 149.

détection et la poursuite d'infractions pénales qui visent à garantir la protection de l'intégrité physique des personnes.

3.2.2. La jurisprudence de la Cour en matière de conservation et d'utilisation de données personnelles

41. La Commission rappellera tout d'abord que la Cour, dans son arrêt *Digital Rights Ireland*, a confirmé sa jurisprudence selon laquelle constitue un objectif d'intérêt général de l'Union la lutte contre le terrorisme international en vue du maintien de la paix et de la sécurité internationales. La Cour a ajouté qu'il en va de même de la lutte contre la criminalité grave afin de garantir la sécurité publique[23].

42. Dans son avis A-1/15, la Cour a confirmé que l'objectif d'assurer la sécurité publique au moyen d'un transfert des données PNR vers le Canada et de l'utilisation de celles-ci dans le cadre de la lutte contre les infractions terroristes et la criminalité transnationale grave constitue un objectif d'intérêt général de l'Union susceptible de justifier des ingérences, même graves, dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte[24].

43. Dans les affaires jointes *Tele2 Sverige/Watson*, la Cour a examiné les dispositions nationales en cause par rapport à l'objectif de lutte contre la criminalité. A cet égard, la Cour a décidé que, au vu de la gravité de l'ingérence dans les droits fondamentaux en cause que constitue une réglementation nationale prévoyant, aux fins de la lutte contre la criminalité, la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure[25]. La nécessité d'une relation entre les données à conserver et l'objectif poursuivi par leur conservation est un principe clé qui garantit lui-même le principe de la limitation des finalités. Ce principe constitue une pierre angulaire de l'acquis de l'Union en matière de la protection des données.

44. Même si la Cour a reconnu que l'efficacité de la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme peut dépendre, dans une

---

23 Digital Rights Ireland, EU:C:2014:238, point 42.

24 Avis 1-15, point 149.

25 Tele2 Sverige/Watson, précité, point 102.

large mesure, de l'utilisation des techniques modernes d'enquête, elle a ajouté qu'un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une telle réglementation nationale soit considérée comme nécessaire aux fins de ladite lutte[26].

45. La Cour a dit pour droit qu'une réglementation nationale, qui ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique, n'est pas limitée à une période temporelle et/ou une zone géographique et/ou sur un cercle de personnes susceptibles d'être mêlées d'une manière ou d'une autre à une infraction grave, soit sur des personnes qui pourraient, pour d'autres motifs, contribuer, par la conservation de leurs données, à la lutte contre la criminalité, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte[27].

3.2.3. Les opérateurs concernés, les catégories de données et les autorités susceptibles d'y avoir accès en l'espèce

46. En ce qui concerne les opérateurs, la Commission constate, premièrement, que l'article 851-1 du code de la sécurité intérieure renvoie à l'article L. 34-1 du code des postes et des communications électroniques et à l'article 6 de la loi du 21 juin 2004. En bref, il semble s'agir des « *fournisseurs de services de communications électroniques*, des *fournisseurs d'accès à des services de communications au public en ligne* ainsi que des *personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services* ».

47. Ces opérateurs doivent conserver les données identifiées à l'article R. 10-13, I. e II, du code des postes et des communications électroniques (c'est-dire, notamment, les informations permettant d'identifier l'utilisateur et le destinataire d'une communication, la date, horaire, durée, les données relatives aux équipements terminaux, la localisation), pendant un an à compter de leur enregistrement. Pour leur part, les opérateurs visés par le II. de l'article 6 de la loi du 21 juin 2004,

---

26 Tele2 Sverige/Watson, précité, point 103.

27 Tele2 Sverige/Watson, précité, point 106.

doivent conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou d'un des contenus des services dont elles sont prestataires. Le décret n° 2011-219, du 25 février 2011, qui met en œuvre cette dernière disposition, identifie les catégories de données à conserver et fixe leur durée de conservation à un an.

48. Quant aux autorités susceptibles d'avoir accès aux données conservées, la Commission comprend qu'en vertu des dispositions combinées de l'article L851-1 et L. 811-3 du code de la sécurité intérieure et des décrets n°s 2015/1185 et 2015-1639, sont susceptibles d'être autorisés à y avoir accès les agents des services de renseignement (spécialisés ou non) désignés par ces décrets.

49. La Commission commencera par examiner l'obligation de conservation des données en cause à la lumière de chacun des objectifs poursuivis, tels qu'expliqués plus en détail ci-dessous. Ensuite, la Commission examinera les conditions relatives à l'accès aux données conservées.

3.2.4. La sauvegarde de la sécurité nationale

50. La première question préjudicielle fait spécifiquement référence à l'objectif de sauvegarder la sécurité nationale, *dont la responsabilité incombe aux seuls Etats membres en vertu de l'article 4 TUE*.

51. La Cour ne s'est pas encore prononcée sur la compatibilité d'une mesure nationale de conservation généralisée et indifférenciée de données personnelles, adoptée sur la base de l'article 15, paragraphe 1, de la directive 2002/58, avec le droit de l'Union en vue de poursuivre l'objectif de sauvegarder de la sécurité nationale[28].

52. A cet égard, la Commission souhaite observer, d'emblée, au sujet de la référence par la juridiction de renvoi à l'article 4 TUE, que l'affirmation selon laquelle *la sécurité nationale reste de la seule responsabilité des Etats 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 Etats membres, dont la sécurité

[28] Il faut noter qu'un tel objectif est en cause dans l'affaire C-623/17, Privacy International, à la différence toutefois que dans cette affaire la mesure nationale attaquée n'impose pas une obligation de conservation des données par les prestataires de services.

nationale est un élément (voir l'article 4, paragraphe 2, TUE première et deuxième phrases)[29].

53. 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 mesure concerne la sécurité nationale, la sécurité publique ou de la sûreté de l'État[30].

54. La Commission note que ni le TUE ni le TFUE ne définissent 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».

55. La Commission estime cependant qu'il existe des similitudes entre la notion de «sécurité nationale» à l'article 4, paragraphe 2, TUE et les «intérêts essentiels de [la] sécurité» d'un État membre, à l'article 346, paragraphe 1, TFUE.

56. 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[31]. Aussi, la notion de « sécurité nationale » constitue, de l'avis de la Commission, une notion autonome du droit de l'Union, qui requiert une interprétation autonome. En effet, le caractère contraignant du droit de l'Union se verrait gravement compromis si un Etat membre pouvait éviter l'application de celui-ci en invoquant simplement qu'une mesure sert l'objectif de sa sécurité nationale. Cela dit, la Commission reconnaît que les Etats membres devraient bénéficier d'un large pouvoir d'appréciation en ce qui concerne la définition de ce qu'ils considèrent être leurs intérêts essentiels de sécurité ainsi que des mesures de sauvegarde de la sécurité nationale.[32]

57. Il peut être déduit de ce qui précède que la notion de «sécurité nationale» se rapporte à la nécessité de préserver et de défendre un ensemble de base d'intérêts essentiels

---

29 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).

30 Coir 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; voir aussi l'affaire C-187/16, Commission/Autriche, EU:C:2018:194, points 76-78.

31 Voir 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, points 46 et suivants.

32 Voir, par analogie, C-187/16, *Commission/Autriche*, EU:C:2018:194, point 78.

de l'État, qui sont nécessaires pour garantir son existence et son ordre constitutionnel[33].

58. La Commission rappelle, à cet égard, que la Cour a déjà admis qu'un objectif d'intérêt général important, tel que la lutte contre des infractions terroristes et la criminalité transnationale grave, est susceptible de justifier des ingérences, même graves, dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte[34]. De l'avis de la Commission, la sauvegarde de la sécurité nationale (et d'autres objectifs particulièrement importants) devrait être capable de justifier un tel niveau d'ingérence.

59. Quant à l'analyse de la compatibilité d'une ingérence, telle que celle en espèce, avec les exigences l'article 15, paragraphe 1, de la directive 2002/58 ainsi que les articles 7, 8 et 52, paragraphe 1, de la Charte, lus à la lumière de la jurisprudence de la Cour, pour les finalités de sauvegarder la sécurité nationale il est nécessaire de procéder par étapes[35], à commencer par le constat d'ingérence et, ensuite, à déterminer si, et à quelles conditions l'ingérence peut être justifiée.

60. Concernant le niveau d'ingérence, force est de constater que les catégories de données dont la conservation est requise par la réglementation en cause dans les présentes affaires correspondent, en substance, à celles examinées par la Cour l'arrêt *Tele2 Sverige/Watson*[36]. Dans ces circonstances, à l'instar du constat de la Cour[37] à cet égard, il y a lieu de considérer qu'il s'agit d'une ingérence particulièrement grave.

61. Quant aux exigences qui doivent être satisfaites afin que la mesure soit justifiée, outre le fait que l'obligation de conservation doit avoir une base légale et respecter le contenu essentiel des droits consacrés aux articles 7 et 8 de la Charte, la mesure en cause doit poursuivre un objectif d'intérêt général reconnu par l'Union, être appropriée à la poursuite de cet objectif, être nécessaire et être proportionnée à la poursuite du même objectif.

---

33 Voir, l'arrêt rendu dans l'affaire C-601/15 PPU, *J.N.*, EU:C:2016:84, point 66.

34 Avis A-1/15, précité, point 149.

35 Voir les conclusions de l'Avocat Général Saugmandsgaard Øe dans les affaires *Tele2 Sverige/Watson*, EU:C:2016:572, points 216 et suivants.

36 Tele2 Sverige/Watson, point 98.

37 Tele2 Sverige/Watson, point 100.

62. Etant donné que l'obligation de conservation en cause est prévue par la loi et que cette obligation ne porte pas sur le contenu des communications[38], ces deux exigences semblent remplies en l'espèce.

63. La sauvegarde de la sécurité nationale, qui fait partie des objectifs d'intérêt général mentionnés à l'article 15, paragraphe 1, de la directive 2002/58 constitue, en principe, un objectif différent de l'objectif poursuivi dans l'affaire *Tele2 Sverige/Watson*, susceptible de recevoir une réponse différente.

64. Il s'agit maintenant d'évaluer si la mesure en cause répond *véritablement* à l'objectif consistant à sauvegarder la sécurité nationale et si elle est *capable* d'atteindre l'objectif recherché et ne dépasse pas les limites de ce qui est approprié et nécessaire à la poursuite de cet objectif.

65. La Commission souhaite observer, premièrement, qu'en ce qui concerne les intérêts essentiels de la sécurité nationale, le décret n° 2015-1639 prévoit que les services qu'il désigne ne pourront être autorisés à utiliser la technique mentionnée à l'article L. 851-1 du code de la sécurité intérieure que pour des finalités spécifiques énumérées à l'article L. 811-3 du même code, auxquelles ce décret renvoie. Ces finalités visent « *la défense et la promotion des intérêts fondamentaux de la Nation*», et incluent, notamment, «*l'indépendance nationale, l'intégrité du territoire et la défense nationale*», «*la prévention du terrorisme*», «*la prévention de la criminalité et de la délinquance organisées*», « *la prévention de la prolifération des armes de destruction massive* ».

66. Deuxièmement, en ce qui concerne la nécessité de l'ingérence, la Commission ne peut pas exclure que les besoins des Etats membres en vue de sauvegarder la sécurité nationale puissent être substantiellement différents des besoins en matière de lutte contre la criminalité en général, même grave, et puissent être capables de justifier une ingérence grave dans les droits garantis par les articles 7 et 8 de la Charte.

67. En effet, la sauvegarde de la sécurité nationale requiert, en fait, une évaluation permanente des risques et l'efficacité des mesures de prévention repose sur l'identification de menaces potentielles. A ce propos, la Commission observe que

---

[38] Voir, au sujet du respect du contenu essentiel des droits garantis par les articles 7 et 8 de la Charte, les points 39 et 40 de l'arrêt *Digital Rights Ireland*.

dans son ordonnance de renvoi, le Conseil d'Etat souligne qu'il est «*constant qu'une conservation préventive et indifférenciée permet aux services de renseignement d'accéder aux données relatives aux communications*[39] *qu'un individu a effectuées avant que soient identifiées les raisons de penser qu'il présente une menace pour la sécurité publique, la défense ou la sûreté de l'Etat* ». Il ajoute que, « *dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, une telle conservation présente une utilité sans équivalent par rapport au recueil de ces mêmes données à partir du moment où l'individu en cause aurait été identifié comme susceptible de présenter une menace pour la sécurité publique, la défense ou la sûreté de l'Etat*» (point 23 de l'ordonnance dans l'affaire C-511/18). (soulignement ajouté).

68. A cet égard, il convient de noter qu'une différenciation, telle que celle indiquée par la Cour au point 106 de l'arrêt *Tele2 Sverige/Watson* (en fonction des périodes temporelles et/ou des zones géographiques et/ou des cercles de personnes), semble très difficile, voire impossible, à appliquer lorsqu'il s'agit de sauvegarder l'objectif susvisé.

69. Concrètement, dans un contexte tel que celui souligné par la juridiction de renvoi, il apparaît extrêmement difficile de limiter dans la loi l'obligation de conserver les données à une période temporelle, dès lors que cette conservation n'est pas liée à la des événements concrets. Le même constat s'impose quant à la limitation à des zones géographiques, car bien qu'imaginable en théorie, celle-ci pourrait être aisément contournée rendant ainsi la mesure complètement inefficace. En outre, la définition de critères permettant une limitation géographique apparaît très difficile à réaliser sans encourir le risque de stigmatisation des habitants des zones visées. Enfin, en ce qui concerne les cercles de personnes susceptibles d'être en rapport avec une menace pour la sécurité nationale, il paraît impossible d'identifier à l'avance de tels personnes ou cercles de personnes étant donné que la conservation généralisée et indifférenciée des données vise, précisément, à identifier des menaces potentielles inconnues précédemment.

70. La Commission souhaite ajouter que dans sa jurisprudence, la CeDH a reconnu une grande marge d'appréciation aux autorités nationales pour choisir comment assurer

[39] NB : cette conservation ne concerne pas le contenu des communications.

la protection de l'intérêt légitime de la sécurité nationale et a reconnu qu'une interception générale (*bulk interception*) ne tombait pas en soi hors de cette marge d'appréciation[40].

71. Dans ces circonstances, selon la Commission, la conservation généralisée et indifférenciée des données en cause pourrait être justifiée par l'objectif de sauvegarder la sécurité nationale dès lors que ces données revêtiraient une importance essentielle, à condition que ladite conservation soit, en ce qui concerne les catégories de données, les moyens de communication et la durée de conservation, limitée au strict nécessaire.

3.2.5. La prévention, la recherche, la détection et la poursuite d'infractions pénales particulièrement graves

72. De l'avis de la Commission, au-delà de la sécurité nationale, il ne devrait pas être catégoriquement exclu que d'autres objectifs importants soient aussi capables de justifier une conservation généralisée et indifférenciée des données de trafic et de localisation. Selon la Commission, tel pourrait être le cas de l'objectif de la prévention, la recherche, la détection et la poursuite d'infractions pénales particulièrement graves, telles qu'expliquées plus en détail ci-dessous, lorsque ces données revêtiraient, aussi pour atteindre cet objectif, une importance essentielle.

73. La Commission considère qu'il y a un lien étroit entre l'objectif de sauvegarder la sécurité nationale et l'objectif de la prévention, la détection, la recherche, et la poursuite de certaines infractions pénales, spécialement lorsque celles-ci représentent des menaces pour la sécurité nationale, comme en matière de terrorisme. Par conséquent, pour autant que la lutte contre de tels crimes puisse être considérée comme servant les intérêts de la sécurité nationale, cet objectif devrait aussi être capable de justifier une ingérence grave dans les droits garantis par la directive 2002/58 et les articles 7 et 8 de la Charte. Cependant, il serait incohérent et inapproprié que le droit de l'Union accepte une telle ingérence dans les droits fondamentaux comme étant justifiée pour la lutte contre le terrorisme dès lors que cette lutte serait effectuée par les services spécialement chargés de la sauvegarde de la sécurité nationale (services de sécurité et de renseignement), mais pas par les autorités en charge de la prévention et la répression de crimes de terrorisme.

---

[40] Arrêt *Big Brother Watch, e.a. c/ Royaume-Uni, 13 septembre 2018, requêtes n° 58170/13, 62322/14 et 24960/15), points 308 et 314 et jurisprudence citée.*

74. Il semble évident que les crimes de terrorisme constituent une forme de criminalité particulièrement grave[41]. Toutefois, la Commission ne peut pas exclure que certaines autres formes de criminalité puissent aussi relever de cette catégorie, par exemple, des attaques contre des systèmes d'information (cyberattaques) de services essentiels, tels que ceux d'infrastructures critiques. En effet, ces formes de criminalité sont susceptibles d'affecter substantiellement les fonctions essentielles de l'Etat et présenter des risques sérieux pour la sécurité nationale. La prévention, la recherche, la détection et la poursuite de ces formes de criminalité devrait, par conséquent, être capable de justifier la conservation généralisée et indifférenciée de données de trafic et de localisation.

75. En outre, selon la Commission, la lutte contre d'autre formes de criminalité particulièrement grave, susceptibles d'affecter les intérêts essentiels de la société, devrait aussi pouvoir justifier une telle conservation de données, dès lors que cet instrument est le seul à même de permettre de lutter efficacement contre de tels crimes, lesquels pourraient inclure, notamment, l'exploitation sexuelle des enfants via l'utilisation des systèmes électroniques de communication.

76. Les formes de criminalité mentionnées aux deux points qui précèdent sont susceptibles d'affecter considérablement la sécurité nationale, les fonctions essentielles de l'Etat ou d'autres intérêts essentiels de la société, aussi parce qu'ils représentent des violations grossières et à grande échelle des droits et libertés d'autrui. Pour ces raisons, l'Union a elle aussi identifié la prévention et la lutte contre de telles formes de criminalité comme une haute priorité[42].

77. En réalité, la lutte effective contre des infractions de cette nature constitue, d'une part, le complément logique et indispensable du système mis en place par les Etats membres pour sauvegarder la sécurité nationale et, d'autre part, permet d'assurer d'autres intérêts essentiels de la société. En plus, il est possible que la conservation

---

41 Ceci ne veut pas nécessairement dire que cette notion couvre toutes les infractions pénales énumérées dans la directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, JO L 88, 31.3.2017, p. 6.

42 Cf. Directive 2013/40/UE du Parlement européen et du Conseil du 12 août 2013 relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil, JO L 201, 14.8.2013, p. 8 (considérants 2 et 3) ; Directive 2011/93/UE du Parlement européen et du Conseil du 13 décembre 2011 relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil, JO L 335, 17.12.2011, p. 1 (considérants 1-4).

généralisée et indifférenciée des données revêtirait une importance fondamentale pour la prévention, la recherche, la détection et la poursuite de ces formes de criminalité particulièrement grave, dans la mesure où il pourrait être établi à partir des caractéristiques spécifiques de ces formes de criminalité que, sans disposer de l'instrument de cette conversation généralisée et indifférenciée, les autorités nationales de répression pénale ne disposeraient pas d'instruments efficaces pour prévenir et poursuivre cette criminalité.

78. En outre, sans vouloir nier la gravité de l'ingérence dans les droits fondamentaux d'un régime de conservation généralisée et indifférenciée des données de trafic et de localisation, telle que mise en exergue aux points 99 et 100 de l'arrêt *Tele2 Sverige/Watson*, la Commission n'exclurait pas toute possibilité de justifier une telle ingérence, dans le but de lutter contre les formes de criminalité particulièrement grave susvisées, sur la base d'une *appréciation globale* d'une législation nationale, lorsque celle-ci, *à la fois*, limiterait le but du régime de conservation des données strictement à la lutte contre ces mêmes formes de criminalité *et* érigerait des limites et garanties strictes en matière d'accès auxdites données ainsi que de sécurité pour leur conservation.

79. L'arrêt *Tele2 Sverige/Watson* pourrait être compris en ce sens que pour la Cour, la gravité particulière de l'ingérence d'un régime de conservation généralisée et indifférenciée de données, notamment en raison des possibilités offertes par un tel régime d'établir des profils de toute personne innocente et du sentiment, généré dans l’esprit des personnes concernées, que leur vie privée fait l’objet d’une surveillance constante, était à elle seule déterminante pour exclure la compatibilité d'un tel régime avec la Charte.

80. Toutefois, selon la Commission, ne serait pas satisfaisante une approche qui consisterait à apprécier un régime de conservation de données exclusivement au niveau de l'ingérence posée par la conservation généralisée et indifférenciée des données, sans prendre en considération également l'étendue des garanties législatives limitant l'accès auxdites données et le dispositif de contrôle et de sanctions qui serait mis en place pour prévenir tout non-respect desdites garanties et, dès lors, tout abus du système.

81. Si une législation nationale, dans le but d'assurer la sécurité nationale ou de lutter uniquement contre certaines formes de criminalité particulièrement grave comme définies plus haut, instaure un régime de rétention de données et l'assortit de garanties très strictes d'accès auxdits données ainsi que d'un dispositif prévenant de manière efficace et crédible tout abus, en particulier toute activité illégale de *profiling*, alors l'ingérence dans les droits fondamentaux découlant d'un tel régime, pour importante qu'elle soit, pourrait néanmoins être justifiée, moyennant une appréciation globale de la législation dans son ensemble.

82. Sur la base des considérations qui précèdent, la Commission invite la Cour à reconsidérer sa jurisprudence en matière de conservation généralisée et indiscriminée des données telle qu'elle découle de l'arrêt *Tele2 Sverige/Watson*, afin de prendre en considération les besoins des autorités nationales en charge de la prévention, la détection, la recherche, et la poursuite des infractions pénales particulièrement graves.

83. De l'avis de la Commission, le législateur national devrait disposer d'un certain pouvoir discrétionnaire pour déterminer quelles formes de criminalité revêtent une importance particulière pour la sécurité nationale ou d'autres intérêts essentiels de la société et pour lesquelles une conservation généralisée et indifférenciée des données apparaît indispensable.

3.2.6. Autres formes de criminalité

84. Quant à d'autres formes de criminalité, même grave, la Commission rappelle que la Cour a déjà dit pour droit qu'une réglementation nationale, comme celle en cause au principal, excède les limites du strict nécessaire et ne saurait être considérée comme étant justifiée, dans une société démocratique, par l'objectif de lutter contre la criminalité grave, ainsi que l'exige l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte[43].

85. Par conséquent, seule une conservation ciblée (effectuée à titre préventif), telle qu'indiquée par la Cour au point 108 de l'arrêt *Tele2 Sverige/Watson* et répondant aux critères établis par la Cour aux points 109 à 111 pourrait, le cas échéant, être justifiée par l'objectif de lutter contre la criminalité qualifiée de « grave ». *A fortiori*,

[43] Tele2 Sverige/Watson, points 106 et 107.

une telle réglementation nationale ne saurait être justifiée par un objectif de prévention, de recherche, de détection et de poursuite « d'infractions pénales » en général ni pour d'autres objectifs.

86. Enfin, il convient de préciser que si de tels objectifs d'intérêt général ne sauraient être capables de justifier la conservation généralisée et indifférenciée de données, ils ne pourraient pas non plus justifier l'accès à ces mêmes données lorsque celles-ci auraient été légalement retenues pour d'autres objectifs. En effet, cela serait contraire à l'article 52, paragraphe 1, de la Charte qui exige que les critères de nécessité et proportionnalité soient examinés par rapport à un (ou plusieurs) objectif(s) spécifique(s). Cette exigence découle aussi de l'article 5, sous b) et c) du règlement 2016/679 qui exigent que les données soient « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ((limitation des finalités)*; qu'elles soient *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données)* ».

3.2.7. Garanties au niveau de l'accès aux données légalement conservées

87. En qui concerne l'accès par les autorités compétentes aux données légalement conservées, la Commission rappelle qu'une mesure législative visée à l'article 15, paragraphe 1, de la directive 2002/58, tel qu'interprété par la Cour, doit prévoir des règles claires et précises indiquant en quelles circonstances et sous quelles conditions les fournisseurs de services concernés doivent accorder aux autorités nationales compétentes l'accès auxdites données[44].

88. A cet égard, la Commission signale que la Cour a énoncé les conditions matérielles et procédurales suivantes aux points 119 à 123 de l'arrêt *Tele2 Sverige/Watson*.

i. 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

[44] Tele2 Sverige/Watson, point 117.

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*);

ii. 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);

iii. 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);

iv. 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);

v. 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.

89. De l'avis de la Commission, les conditions énumérées au point précédent devraient s'appliquer dans leur entièreté lorsque les autorités compétentes poursuivent l'objectif de la prévention ou de la lutte contre la criminalité particulièrement grave telle que référé ci-dessus.

90. Cependant, en ce qui concerne l'objectif de sauvegarder la sécurité nationale en tant que tel, la situation est différente de celle dans l'affaire *Tele2 Sverige/Watson*, compte tenu, en particulier, des spécificités de cet objectif ainsi que du fait que, conformément à l'article 4, paragraphe, TUE, la sécurité nationale reste de la seule responsabilité des Etats membres.

91. Il s'ensuit que les conditions formulées par la Cour dans l'arrêt *Tele2 Sverige/Watson*, rappelées au point 88 ci-dessus, ne doivent pas nécessairement être transposées telles quelles lorsqu'il s'agit de la poursuite dudit objectif.[45]

92. Par ailleurs, la Commission estime que, lorsque la mesure nationale poursuit *véritablement* l'objectif de sauvegarde de la sécurité nationale et est capable de l'atteindre – ce qui incombe à la juridiction nationale de vérifier -, 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, points 34 et 64).

93. Il appartient à la juridiction de renvoi de vérifier si et dans quelle mesure la réglementation nationale en cause au principal respecte les exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, tels qu'interprétés par la Cour.

3.3. Sur la question 2 dans l'affaire C-511/18 - Autres mesures de collecte de données qui n'imposent pas leur conservation aux opérateurs économiques

94. Par sa deuxième question dans affaire C-511/18, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58 lu à la lumière des articles 7, 8 et 52, paragraphe 1 de la Charte, doit être interprété en ce sens qu'il autorise les Etats membres à mettre en place une réglementation, telle que celle en cause dans l'affaire au principal, qui permet la mise en œuvre de mesures de recueil, en temps réel, de données de trafic et de localisation des équipements terminaux d'une personne préalablement identifiée, susceptible d'être en lien avec une menace terroriste.

95. Cette question semble viser les mesures de recueil de données en temps réel, prévues à l'article L. 851-2 du code de la sécurité intérieure ainsi que les traitements automatisés sur les réseaux, prévus à l'article L. 851-3 du même code[46]. En tant que telles, ces mesures constituent des ingérences dans le droit à la confidentialité des communications garanti par la directive 2002/58.

---

45 Voir l'arrêt de la CeDH dans l'affaire *Big Brother Watch, e.a. c/ Royaume-Uni*, précité, point 317.

46 Voir les points 26 et 27 de l'ordonnance de renvoi.

96. La Commission note que l'article L. 851-2 porte sur les informations et documents mentionnés à l'article L. 851-1 qui pourront faire l'objet d'une mesure individuelle, pour les seuls besoins de la prévention du terrorisme, de recueil en temps réel desdites informations et documents relatifs à une personne préalablement identifiée (ou relatifs à des personnes appartenant à l'entourage de la personne concernée - voir la deuxième phrase du I de l'article L. 851-2).

97. Cette disposition établit donc un lien entre les personnes concernées dont les données sont susceptibles de faire l'objet de la mesure de recueil en temps réel et l'objectif poursuivi[47].

98. De l'avis de la Commission, dans le cas où des autorités susceptibles de recourir à ce type de mesures poursuivraient l'objectif de lutter contre la criminalité grave (*law enforcement*), les conditions relatives à l'accès rappelées au point 88 ci-dessus devraient s'appliquer.

99. En ce qui concerne les autorités poursuivant l'objectif de la sauvegarde de la sécurité nationale, il appartient à la juridiction nationale de vérifier si la mesure respecte les exigences découlant de l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7 et 8 ainsi que de l'article 52, paragraphe 1, de la Charte, telles qu'interprétées par la Cour.

100. Quant à l'article L. 851-3 du code de la sécurité intérieure, il permet, aussi pour les seules fins de la prévention du terrorisme, *d'imposer aux opérateurs […] la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans la demande, à détecter des connexions susceptibles de révéler une menace terroriste*.

101. Il convient de noter, que ces traitements ne permettent pas, en eux-mêmes, l'identification des personnes auxquels les informations ou documents traités se rapportent (voir 2ème paragraphe du I de L. 851-3). Ce n'est que lorsque lesdits traitements détectent des données susceptibles de révéler une menace à caractère terroriste, que l'accès aux données d'identification pourra, le cas échéant, être autorisé (voir le IV de l'article L. 851-3).

---

47 Voir, par analogie, les points 110 et 111 de l'arrêt Tele2 Sverige/Watson.

102. Dans son Avis A-1/15, la Cour a examiné des traitements automatisés de données à caractère personnel et a conclu que ceux-ci pouvaient être admis sous certaines conditions. Il convient de citer, en particulier, les points 172 et 173 de l'Avis :

« 172. Cela étant, l'étendue de l'ingérence que comportent les analyses automatisées des données PNR dans les droits consacrés aux articles 7 et 8 de la Charte dépend essentiellement des modèles et des critères préétablis ainsi que des bases de données sur lesquels se fonde ce type de traitement de données. Ainsi, et eu égard aux considérations figurant aux points 169 et 170 du présent avis, les modèles et les critères préétablis devraient être, d'une part, spécifiques et fiables, permettant d'aboutir, comme l'a relevé M. l'avocat général au point 256 de ses conclusions, à des résultats ciblant les individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes ou de criminalité transnationale grave et, d'autre part, non discriminatoires. De même, il devrait être précisé que les bases de données avec lesquelles les données PNR sont recoupées doivent être fiables, actuelles et limitées à des bases de données exploitées par le Canada en rapport avec la lutte contre le terrorisme et la criminalité transnationale grave.

173. En outre, dans la mesure où les analyses automatisées des données PNR comportent nécessairement, ainsi que cela a été constaté au point 169 du présent avis, un certain taux d'erreur, tout résultat positif obtenu à la suite d'un traitement automatisé desdites données doit, en vertu de l'article 15 de l'accord envisagé, être soumis à un réexamen individuel par des moyens non automatisés avant l'adoption d'une mesure individuelle produisant des effets préjudiciables à l'égard des passagers aériens concernés. Ainsi, une telle mesure ne saurait, en vertu dudit article 15, être fondée de manière décisive sur le seul résultat d'un traitement automatisé des données PNR. »

103. La Commission estime que ces considérations pourraient être transposées aux traitements automatisés en cause dans l'affaire au principal, prévus à l'article L. 851-3 du code de la sécurité intérieure.

104. La Commission signalera, par ailleurs, le point II l'article L. 851-3 du code de la sécurité intérieure selon lequel la Commission nationale de contrôle des techniques de renseignement émet un avis sur la demande d'autorisation relative aux traitements automatisés et les paramètres de détection retenus. Cette Commission dispose, en outre, d'un accès permanent, complet et direct à ces traitements ainsi qu'aux informations et données recueillies. Par ailleurs, les autorisations sont limitées dans le temps (deux mois, renouvelables sous conditions).

105. Il appartient à la juridiction de renvoi de vérifier si la réglementation nationale contient des garanties suffisantes afin que les modèles soient spécifiques et fiables, comme relevé par la Cour aux points 172 et 173 de son Avis A-1/15.

3.4. Sur la troisième question dans l'affaire C-511/18

106. Par sa troisième question dans l'affaire C-511/18, la juridiction de renvoi demande si la directive 2002/58, lue à la lumière de la Charte, doit être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes ou si de telles procédures peuvent être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales existantes, dès lors que celles-ci assureraient l'effectivité du droit au recours.

107. Il ressort des points 8, 9 et 10 de l'ordonnance de renvoi que les « autres garanties procédurales existantes » consistent, pour l'essentiel, en un mécanisme de contrôle des activités de renseignement par la Commission nationale de contrôle des techniques de renseignement et la possibilité pour cette Commission de saisir une juridiction (la formation spécialisée du Conseil d'Etat). Un requérant qui pense faire l'objet d'une mesure de surveillance n'a pas la possibilité de saisir directement un juge pour en contester la régularité mais il peut former une réclamation à cette fin auprès de ladite Commission. Si à la suite de cette réclamation, la Commission saisi le Conseil d'Etat (formation spécialisée), celui-ci pourra prendre connaissance des éléments de preuve couverts par le secret défense mais ne peut pas les communiquer à la personne concernée.

108. La Commission considère qu'en principe l'absence d'information des personnes concernées, lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes, ne serait pas conforme aux articles 7, 8 et 47 de la Charte.

109. La Commission note que la CeDH admet que la notification à la personne concernée lorsque celle-ci a fait l'objet d'une mesure de surveillance n'est pas une exigence absolue sous l'article 8 CEDH[48].

110. Cependant, la Cour de justice a confirmé que l'information des personnes concernées, dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes, s'avère, de fait, nécessaire pour permettre aux personnes

[48] Arrêt de la CeDH, Big Brother Watch, précité, points 213 et 310.

concernées d'exercer leurs droits de demander l'accès auxdites données les concernant et, le cas échéant, la rectification de celles-ci ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la Charte, un recours effectif devant un tribunal[49].

3.5. Sur la deuxième question dans l'affaire C-512/18

111. Par sa deuxième question dans l'affaire C-512/18, la juridiction de renvoi demande, en substance, si l'article 15 de la directive 2000/31 sur le commerce électronique, lu à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte doit être interprété en ce sens qu'il permet à un Etat membre d'imposer à des fournisseurs d'accès aux services communication au public en ligne[50] ainsi qu'aux personnes physiques ou morales qui assurent, même à titre gratuit, des services d'hébergement de contenu[51],[52] pour mise à disposition du public, l'obligation de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale.

112. Contrairement à la position de la juridiction de renvoi (points 13 et 14 de l'ordonnance), la Commission considère que la Directive 2000/31 n'est pas pertinente pour l'analyse de l'obligation objet de cette question préjudicielle.

113. En effet, premièrement, l'article 1, paragraphe 5, sous b) de cette directive exclut de son champ d'application « *les questions relatives aux services de la société de l'information couvertes par les directives 95/46/CE et 97/66/CE* » (ces deux directives correspondent désormais, respectivement, au règlement 2016/679 et à la directive 2002/58).

---

49 Voir, par analogie, point 220 et jurisprudence citée.

50 Qui semblent correspondre aux fournisseurs de services qualifiés de "Simple transport ("*Mere conduit*") visés l'article 12 de la directive 2000/31.

51 Qui semblent correspondre aux services qualifiés d'"hébergement" visés à l'article 14 de la directive 2000/31.

52 (« *stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par les destinataires de ces services* »).

114. Or, s'agissant d'une obligation de conserver des données visant à identifier des personnes physiques (personnes identifiées ou identifiables), de telles données doivent être considérées comme des « *données à caractère personnel* » au sens de l'article 4, point 1, du règlement 2016/679. Selon cette disposition, « *est réputée être une « personne physique identifiable », toute personne qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant, tel qu'un numéro d'identification, des données de localisation ou un identifiant en ligne* »[53].

115. Deuxièmement, s'agissant des fournisseurs des services concernés, il est possible que certains relèvent de la directive 2002/58 en application de l'article 3 de celle-ci[54], tandis que d'autres, tels que des services de la société de l'information qui offrent des services de stockage de contenu, relèveraient, pour ce qui concerne des traitements de données à caractère personnel, du règlement 2016/679.

116. Ainsi, la Commission suggère de reformuler la question comme visant à savoir si l'article 15, paragraphe 1, de la directive 2002/58 ainsi que l'article 23, paragraphe 1, du règlement 2016/979 doivent être interprétés en ce sens qu'ils permettre à un Etat membre d'instaurer une réglementation nationale, telle que celle en l'espèce, qui prévoit une obligation de conservation d'informations et données de nature à permettre l'identification de quiconque a contribué à la création de contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale.

117. S'agissant de l'article 15, paragraphe 1, de la directive 2002/58, la Commission a déjà conclu qu'une réglementation nationale imposant une obligation de conservation généralisée et indifférenciée de données personnelles ne saurait être justifiée par un objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales graves. *A fortiori*, elle ne pourrait pas être justifiée pour lutter contre des « infractions pénales » en général (voir les points 84 à 86 ci-dessus).

---

53 La Cour déjà jugé qu'une adresse IP dynamique constitue une donnée à caractère personnel si le fournisseur qui a enregistré ladite adresse IP dispose des moyens légaux lui permettant de faire identifier la personne concernée, notamment, grâce aux informations supplémentaires dont dispose le fournisseur de l'accès à Internet de cette personne. Voir arrêt dans l'affaire C-582/14, Breyer, EU:C:2016:779.

54 Par exemple, il n'est pas exclu que des fournisseurs de services de communications électroniques fournissent aussi l'accès à des services de communications au public en ligne.

118. Concernant l'article 23, paragraphe 1, du règlement 2016/679, il permet aussi de limiter la portée des certaines obligations et droits (ceux prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5), notamment, pour des objectifs prévus aux alinéas d) « *la prévention et la détection d'infractions pénales […]* » et j) « *l'exécution des demandes de droit civil* ».

119. De l'avis de la Commission, l'article 23, paragraphe 1, ne devrait pas être interprété de manière différente de l'article 15, paragraphe 1, de la directive 2002/58 à l'égard d'une mesure nationale qui poursuit des objectifs essentiellement équivalents couverts par les deux actes. En effet, à l'instar de l'article 15, paragraphe 1, de la directive 2002/58, l'article 23, paragraphe 1, du règlement exige qu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique, reflétant ainsi les exigences de l'article 52, paragraphe 1, de la Charte.

4. CONCLUSION

Eu égard aux considérations qui précèdent, la Commission propose à la Cour d'apporter les réponses suivantes aux questions posées par le Conseil d'Etat, telles que reformulées :

1. **L'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale qui prévoit une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic, des données de localisation et de connexion de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication à des fins de protection de la sécurité nationale ou de la prévention, la détection, la recherche et la poursuite de certains crimes particulièrement graves pour lesquels une telle conservation revêtirait une importance essentielle, à condition que ladite conservation soit, en ce qui concerne les catégories de données, les moyens de communication et la durée de conservation, limitée au strict nécessaire et que l'accès soit limité au strict nécessaire et assorti de garanties appropriés.**

2. **L'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale, telle que celle en l'espèce, qui, sans prévoir une conservation des données permet, pour les seuls besoins de la prévention du terrorisme, l'accès à des données relatives au trafic, des données de localisation et de connexion relatives à une personne préalablement identifiée susceptible d'être en lien avec une menace**

terroriste et permet que des traitements automatisés de données destinés, sur la base de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste, à condition que les paramètres utilisés dans le cadre du traitement automatisé des données soient spécifiques et fiables ainsi que non discriminatoires.

3. **L'article 15, paragraphe 1, de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 52, paragraphe 1, et 47 de la Charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale qui, tout en prévoyant un mécanisme de contrôle des activités de renseignement par une commission et la possibilité pour cette commission de saisir une formation spécialisée d'une haute juridiction administrative n'exige pas l'information des personnes concernées par une mesure secrète de surveillance dès le moment où cette communication n'est pas susceptible de compromettre les enquêtes menées par ces autorités.**

4. **L'article 15, paragraphe 1, de la directive 2002/58/CE et l'article 23, paragraphe 1, d) et j), du règlement (UE) 2016/679, lus à la lumière des articles 7, 8, 11 et 52, paragraphe 1, de la de la Charte des droits fondamentaux de l'Union européenne, doivent être interprétés en ce sens qu'ils s'opposent à une réglementation nationale imposant aux personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et aux personnes physiques et morales qui assurent, même à titre gratuit, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services, pour mise à disposition du public par des services de communication au public en ligne, de conserver les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires, afin que l'autorité judiciaire puisse, le cas échéant, en requérir communication en vue de faire respecter les règles relatives à la responsabilité civile ou pénale.**

Piedade Costa de Oliveira Martin Wasmeier Herke Kranenborg
Agents de la Commission