Recueil de la jurisprudence

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

Affaires jointes C-511/18 et C-512/18

La Quadrature du Net (C-511/18 et C-512/18),
French Data Network (C-511/18 et C-512/18),
Fédération des fournisseurs d'accès à Internet associatifs (C-511/18 et C-512/18),
Igwan.net (C-511/18)
contre
Premier ministre (C-511/18 et C-512/18),
Garde des Sceaux, ministre de la Justice (C-511/18 et C-512/18),
ministre de l'Intérieur (C-511/18),
ministre des Armées (C-511/18)

[demande de décision préjudicielle formée par le Conseil d'État (France)]

« Renvoi préjudiciel – Traitement des données à caractère personnel et protection de la vie privée dans le secteur des communications électroniques – Sauvegarde de la sécurité nationale et lutte contre le terrorisme – Directive 2002/58/CE – Champ d'application – Article 1er, paragraphe 3 – Article 15, paragraphe 3 – Article 4, paragraphe 2, TUE – Charte des droits fondamentaux de l'Union européenne – Articles 6, 7, 8, 11, 47 et 52, paragraphe 1 – Conservation généralisée et indifférenciée des données de connexion et des données permettant d'identifier les créateurs de contenu – Recueil de données relatives au trafic et de données de localisation – Accès aux données »

1. Ces dernières années, la Cour a maintenu une ligne jurisprudentielle constante en matière de conservation et d'accès aux données à caractère personnel, marquée par les jalons suivants :

– l'arrêt du 8 avril 2014, Digital Rights Ireland e.a. [2], dans lequel la Cour a constaté l'invalidité de la directive 2006/24/CE [3], au motif que cette dernière permettait une ingérence disproportionnée dans les droits consacrés par les articles 7 et 8 de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») ;

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

1 Langue originale : l'espagnol.

2 C-293/12 et C-594/12, ci-après l'« arrêt Digital Rights », EU:C:2014:238.

3 Directive du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO 2006, L 105, p. 54).

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

5 Directive du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37).

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

2. Ces arrêts (notamment le deuxième) préoccupent les autorités de certains États membres, car ils ont pour effet, selon elles, de les priver d'un instrument qu'elles estiment nécessaire à la sauvegarde de la sécurité nationale et à la lutte contre la criminalité et le terrorisme. Certains de ces États membres demandent donc que cette jurisprudence soit révoquée ou nuancée.

3. Des juridictions d'États membres ont fait part de cette même préoccupation dans quatre renvois préjudiciels[7] sur lesquels je présente ce jour mes conclusions.

4. Les quatre affaires soulèvent, tout d'abord, le problème de l'application de la directive 2002/58 à des activités liées à la sécurité nationale et à la lutte contre le terrorisme. Si cette directive s'applique dans un tel contexte, il conviendra alors de déterminer dans quelle mesure les États membres peuvent restreindre les droits en matière de vie privée qu'elle protège. Enfin, il y aura lieu d'examiner jusqu'à quel point les différentes réglementations nationales (belge[8], française[9] et du Royaume-Uni[10]) en la matière sont conformes au droit de l'Union, tel qu'interprété par la Cour.

I. Le cadre juridique

A. Le droit de l'Union

1. La directive 2002/58

5. Aux termes de l'article 1er (« Champ d'application et objectif ») de la directive 2002/58 :

« 1. La présente directive harmonise les dispositions des États membres nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et des services de communications électroniques dans la Communauté.

[...]

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du traité instituant la Communauté européenne, telles que celles visées dans les titres V et VI du traité sur l'Union européenne, et en tout état de cause, aux activités concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal. »

6 C-207/16, ci-après l'« arrêt Ministerio Fiscal », EU:C:2018:788.

7 Outre dans les deux présentes affaires (C-511/18 et C-512/18), dans les affaires Privacy International (C-623/17), et Ordre des barreaux francophones et germanophone e.a. (C-520/18).

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

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

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

6. L'article 3 (« Services concernés ») de la directive 2002/58 prévoit :

« La présente directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture des 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. »

7. L'article 5 (« Confidentialité des communications ») de la directive 2002/58 énonce, à son paragraphe 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. »

8. Aux termes de l'article 6 (« Données relatives au trafic ») de la directive 2002/58 :

« 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. L'article 15 (« Application de certaines dispositions de la directive 95/46/CE [11] ») de la directive 2002/58 dispose, à son paragraphe 1 :

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

11 Directive du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31).

2. La directive 2000/31/CE

10. L'article 14 de la directive 2000/31/CE [12] prévoit :

« 1. Les États membres veillent à ce que, en cas de fourniture d'un service de la société de l'information consistant à stocker des informations fournies par un destinataire du service, le prestataire ne soit pas responsable des informations stockées à la demande d'un destinataire du service à condition que :

[...]

3. Le présent article n'affecte pas la possibilité, pour une juridiction ou une autorité administrative, conformément aux systèmes juridiques des États membres, d'exiger du prestataire qu'il mette un terme à une violation ou qu'il prévienne une violation et n'affecte pas non plus la possibilité, pour les États membres, d'instaurer des procédures régissant le retrait de ces informations ou les actions pour en rendre l'accès impossible. »

11. Aux termes de l'article 15 de la directive 2000/31 :

« 1. Les États membres ne doivent pas imposer aux prestataires, pour la fourniture des services visée aux articles 12, 13 et 14, une obligation générale de surveiller les informations qu'ils transmettent ou stockent, ou une obligation générale de rechercher activement des faits ou des circonstances révélant des activités illicites.

2. Les États membres peuvent instaurer, pour les prestataires de services de la société de l'information, l'obligation d'informer promptement les autorités publiques compétentes d'activités illicites alléguées qu'exerceraient les destinataires de leurs services ou d'informations illicites alléguées que ces derniers fourniraient ou de communiquer aux autorités compétentes, à leur demande, les informations permettant d'identifier les destinataires de leurs services avec lesquels ils ont conclu un accord d'hébergement. »

3. Le règlement (UE) 2016/679

12. Conformément à l'article 2 (« Champ d'application matériel ») du règlement (UE) 2016/679 [13] :

« 1. Le présent règlement s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier.

2. Le présent règlement ne s'applique pas au traitement de données à caractère personnel effectué :

a) dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union ;

b) par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne ;

c) par une personne physique dans le cadre d'une activité strictement personnelle ou domestique ;

12 Directive 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 2000, L 178, p. 1).

13 Règlement 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/CEE (règlement général sur la protection des données) (JO 2016, L 119, p. 1).

d) par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces.

[...] »

13. L'article 23 (« Limitations »), paragraphe 1, du règlement 2016/679 dispose :

« 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, au sein d'une société démocratique, pour garantir :

a) la sécurité nationale ;

b) la défense nationale ;

c) la sécurité publique ;

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. »

14. L'article 95 (« Relation avec la directive 2002/58/CE ») du règlement 2016/679 est libellé comme suit :

« 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. »

B. Le droit français

1. Le code de la sécurité intérieure

15. Aux termes de l'article L. 851-1 du code de la sécurité intérieure :

« Dans les conditions prévues au chapitre 1er 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 nº 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. [...] »

16. Les articles L. 851-2 et L. 851-4 du code de la sécurité intérieure réglementent, pour des finalités et selon des modalités différentes, les accès administratifs en temps réel aux données de connexion ainsi conservées.

17. L'article L. 851-2 du code de la sécurité intérieure autorise, pour les seuls besoins de la prévention du terrorisme, le recueil des informations ou documents prévus à l'article L. 851-1 de ce code auprès des mêmes personnes. Ce recueil des informations ou documents, qui ne concerne qu'un ou plusieurs individus préalablement identifiés comme étant susceptibles d'être en lien avec une menace terroriste, s'effectue en temps réel. Il en va de même de l'article L. 851-4 dudit code, qui autorise la transmission en temps réel par les opérateurs des seules données techniques relatives à la localisation des équipements terminaux [14].

18. L'article L. 851-3 du code de la sécurité intérieure permet d'imposer aux opérateurs de communications électroniques et aux prestataires techniques « la mise en œuvre sur leurs réseaux de traitements automatisées destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste » [15].

19. L'article L. 851-5 du code de la sécurité intérieure précise que, dans certaines conditions, « peut être autorisée l'utilisation d'un dispositif technique permettant la localisation en temps réel d'une personne, d'un véhicule ou d'un objet ».

20. Conformément à l'article L. 851-6, paragraphe I, du code de la sécurité intérieure, dans certaines conditions, « peuvent être directement recueillies, au moyen d'un appareil ou d'un dispositif technique mentionné au 1° de l'article 226-3 du code pénal, les données techniques de connexion permettant l'identification d'un équipement terminal ou du numéro d'abonnement de son utilisateur ainsi que les données relatives à la localisation des équipements terminaux utilisés ».

14 Selon la juridiction de renvoi, ces techniques ne font pas peser sur les fournisseurs concernés une exigence de conservation supplémentaire par rapport à ce qui est nécessaire à la facturation de leurs services, à la commercialisation de ceux-ci et à la fourniture de services à valeur ajoutée.

15 Selon la juridiction de renvoi, cette technique, qui n'implique pas une conservation généralisée et indifférenciée, vise uniquement à recueillir pendant une durée limitée, parmi l'ensemble des données de connexion traitées par ces personnes, celles de ces données qui pourraient présenter un lien avec une telle infraction grave.

2. Le code des postes et des communications électroniques

21. Conformément à l'article L. 34-1 du code des postes et des communications électroniques, dans sa version applicable aux faits :

« 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'État, 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'État, par les opérateurs.

[...]

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 des 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. »

22. L'article R. 10-13, sous I, du code des postes et des communications électroniques prévoit que les opérateurs doivent conserver, pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales, les informations suivantes :

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

b) Les données relatives aux équipements terminaux de communications 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 ».

23. L'article R. 10-13, paragraphe II, du code des postes et des communications électroniques prévoit que, pour les activités de téléphonie, l'opérateur doit, en outre, conserver les données permettant d'identifier l'origine et la localisation de la communication.

24. L'article R. 10-13, paragraphe III, du code des postes et des communications électroniques prévoit que les données mentionnées doivent être conservées pendant un an à compter du jour de leur enregistrement.

3. La loi nº 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique

25. L'article 6, paragraphe II, premier alinéa, de la loi nº 2004-575 prévoit que les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne et 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 « 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 ».

26. L'article 6, paragraphe II, troisième alinéa, de la loi nº 2004-575 indique que l'autorité judiciaire peut requérir communication auprès de ces personnes des données mentionnées au premier alinéa.

27. Aux termes de l'article 6, paragraphe II, dernier alinéa, de la loi nº 2004-575, un décret en Conseil d'État (France) « définit les données mentionnées au premier alinéa et détermine la durée et les modalités de leur conservation » [16].

16 Cette définition a été donnée par le décret nº 2011-219, du 25 février 2011, relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. Dans ce décret, les dispositions suivantes peuvent être soulignées : a) l'article 1er, paragraphe 1, qui établit que les personnes offrant accès à des services de communication en ligne doivent conserver les informations suivantes : l'identifiant de la connexion, l'identifiant attribué à l'abonné, l'identifiant du terminal utilisé pour la connexion, les dates et heure de début et de fin de la connexion, les caractéristiques de la ligne de l'abonné ; b) l'article 1er, paragraphe 2, conformément auquel les personnes 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 doivent conserver, pour chaque opération, les informations suivantes : l'identifiant de la connexion à l'origine de la communication, l'identifiant attribué par le système d'information au contenu, objet de l'opération, les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus, la nature de l'opération, les date et heure de l'opération, l'identifiant utilisé par l'auteur de l'opération ; et enfin c) l'article 1er, paragraphe 3, qui prévoit que les personnes mentionnées aux deux points précédents doivent conserver les informations suivantes fournies par un utilisateur lors de la souscription d'un contrat ou lors de la création d'un compte : l'identifiant de la connexion lors de la création du compte, les nom et prénom ou la raison sociale, les adresses postales associées, les pseudonymes utilisés, les adresses de courrier électronique ou de compte associées, les numéros de téléphone, le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour.

II. Les faits et les questions préjudicielles posées

A. Affaire C-511/18

28. La Quadrature du Net, French Data Network, Igwan.net et la Fédération des fournisseurs d'accès à Internet associatifs (ci-après les « requérants ») ont demandé au Conseil d'État d'annuler plusieurs décrets d'application de certaines dispositions du code de la sécurité intérieure [17].

29. Les requérants soutenaient, en substance, que tant les décrets attaqués que ces dispositions du code de la sécurité intérieure étaient contraires aux droits au respect de la vie privée, à la protection des données à caractère personnel et à un recours effectif, garantis respectivement par les articles 7, 8 et 47 de la Charte.

30. Dans ces conditions, le Conseil d'État a décidé de surseoir à statuer et de poser à la Cour les 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 [2002/58], 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] et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 du traité sur l'Union européenne ?

2) La directive [2002/58], lue à la lumière de la [Charte], 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 [2002/58], lue à la lumière de la [Charte], 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 ? »

B. Affaire C-512/18

31. Les requérants dans le litige ayant donné lieu à l'affaire C-511/18, à l'exception d'Igwan.net, ont également demandé au Conseil d'État d'annuler le rejet (par silence de l'administration) de leur demande d'abrogation de l'article R. 10-13 du code des postes et des communications électroniques ainsi que du décret nº 2011-219.

17 Les décrets attaqués étaient les suivants : a) décret nº 2015-1885, du 28 septembre 2015, portant désignation des services spécialisés de renseignement ; b) décret nº 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'État ; c) décret nº 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, et d) décret nº 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement.

32. Selon eux, les dispositions attaquées imposent la conservation de données relatives au trafic, de données de localisation et de données de connexion, obligation qui, en raison de son caractère général, constitue une atteinte disproportionnée aux droits au respect de la vie privée et familiale, à la protection des données à caractère personnel et à la liberté d'expression, protégés par les articles 7, 8 et 11 de la Charte, en violation de l'article 15, paragraphe 1, de la directive 2002/58.

33. Dans cette procédure, le Conseil d'État a décidé de surseoir à statuer et de poser les 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 [2002/58], 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] et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 du traité sur l'Union européenne ?

2) Les dispositions de la directive [2000/31], lues à la lumière des articles 6, 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la [Charte], doivent-elles être interprétées en ce sens qu'elles permettent à un État 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 ? »

III. La procédure devant la Cour et les positions des parties

34. Les demandes de décision préjudicielle ont été enregistrées au greffe de la Cour le 3 août 2018.

35. La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, French Data Network, les gouvernements belge, tchèque, danois, allemand, estonien, irlandais, espagnol, français, chypriote, hongrois, polonais, suédois et du Royaume-Uni ainsi que la Commission ont présenté des observations écrites.

36. Une audience s'est tenue le 9 septembre 2019, conjointement à celles des affaires Privacy International (C-623/17) et Ordre des barreaux francophones et germanophone e.a. (C-520/18) ; y ont comparu les parties aux quatre renvois préjudiciels, les gouvernements susmentionnés ainsi que ceux des Pays-Bas et de la Norvège, la Commission et le contrôleur européen de la protection des données personnelles.

IV. Analyse

37. Les questions du Conseil d'État peuvent être regroupées en trois questions :

– En premier lieu, une réglementation nationale qui impose aux fournisseurs de services de communications électroniques de conserver de manière généralisée et indifférenciée les données de connexion (première question dans l'affaire C-511/18 et dans l'affaire C-512/18) et, en particulier, les données permettant d'identifier les créateurs des contenus offerts par ces fournisseurs (deuxième question dans l'affaire C-512/18) est-elle conforme au droit de l'Union ?

– En deuxième lieu, la licéité des procédures de recueil des données de connexion est-elle, en tout état de cause, subordonnée à l'obligation d'informer les personnes concernées, lorsque cela ne compromet pas les enquêtes (troisième question dans l'affaire C-511/18) ?

– En troisième lieu, le recueil en temps réel des données relatives au trafic et des données de localisation, sans obligation de les conserver, est-elle compatible – et si oui sous quelles conditions – avec la directive 2002/58 (deuxième question dans l'affaire C-511/18) ?

38. Il s'agit, en définitive, de se prononcer sur la conformité au droit de l'Union d'une réglementation nationale qui impose aux fournisseurs de services de communications électroniques deux types d'obligations : a) d'une part, le *recueil* de certaines données, mais non leur conservation ; b) d'autre part, la *conservation* des données de connexion et des données facilitant l'identification des créateurs des contenus des services offerts par ces fournisseurs.

39. À titre liminaire, il y a lieu de déterminer si, précisément en raison du contexte [18] dans lequel cette réglementation nationale a été adoptée (à savoir dans des circonstances où la sécurité nationale peut être compromise), la directive 2002/58 est applicable.

A. Quant à l'applicabilité de la directive 2002/58

40. La juridiction de renvoi tient pour acquis que la réglementation litigieuse relève du champ d'application de la directive 2002/58. C'est ce qui ressort, selon elle, de la jurisprudence établie dans l'arrêt Tele2 Sverige et Watson et confirmée dans l'arrêt Ministerio Fiscal.

41. En revanche, certains des gouvernements qui sont intervenus dans la procédure soutiennent que la réglementation litigieuse ne relève pas de ce domaine. À l'appui de leur position, ils invoquent, entre autres, l'arrêt du 30 mai 2006, Parlement/Conseil et Commission [19].

42. Je partage l'avis du Conseil d'État, selon lequel l'arrêt Tele2 Sverige et Watson a tranché cette partie du débat en confirmant que la directive 2002/58 s'applique, en principe, lorsque les fournisseurs de services électroniques sont tenus par la loi de conserver les données de leurs abonnés et de permettre aux autorités publiques d'y accéder. Que les obligations soient imposées aux fournisseurs pour des raisons de sécurité nationale n'y change rien.

43. J'indique dès maintenant que, s'il existait une quelconque divergence entre l'arrêt Tele2 Sverige et Watson et les arrêts l'ayant précédé, il conviendrait de considérer que c'est l'arrêt Tele2 Sverige et Watson qui prime, en tant qu'arrêt postérieur et confirmé par l'arrêt Ministerio Fiscal. Je considère toutefois qu'une telle divergence n'existe pas, comme je tenterai de l'expliquer.

18 « Un contexte [de] menaces graves et persistantes pour la sécurité nationale, notamment [de] risque terroriste », comme spécifié dans la première question dans l'affaire C-511/18.

19 C-317/04 et C-318/04, ci-après l'« arrêt Parlement/Conseil et Commission », EU:C:2006:346.

1. L'arrêt Parlement/Conseil et Commission

44. Les affaires tranchées par l'arrêt Parlement/Conseil et Commission concernaient :

– l'accord entre la Communauté européenne et les États-Unis d'Amérique concernant le traitement et le transfert de données PNR [Passenger Name Records (données des dossiers passagers)] par les transporteurs aériens aux autorités des États-Unis [20];

– le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés auxdites autorités [21].

45. La Cour a conclu que le transfert de telles données constituait un traitement ayant pour objet la sécurité publique et les activités de l'État relatives à des domaines du droit pénal. Conformément à l'article 3, paragraphe 2, premier tiret, de la directive 95/46, les deux décisions litigieuses ne relevaient pas du champ d'application de cette directive.

46. Les données étaient initialement collectées par les compagnies aériennes dans le cadre d'une activité – la vente de billets – relevant du droit de l'Union. Cependant, leur traitement, tel qu'il était prévu dans la décision litigieuse, n'était pas « nécessaire à la réalisation d'une prestation de services, mais considéré comme nécessaire pour sauvegarder la sécurité publique et à des fins répressives » [22].

47. La Cour a ainsi adopté une approche téléologique, au regard de l'objectif visé par le traitement des données : si sa finalité était la protection de la sécurité publique, le traitement des données devait être considéré comme ne relevant pas du champ d'application de la directive 95/46. Toutefois, cet objectif n'était pas le seul critère déterminant [23]; la Cour a donc souligné dans l'arrêt qu'il « s'insère dans un cadre institué par les pouvoirs publics et visant la sécurité publique » [24].

48. L'arrêt Parlement/Conseil et Commission permet donc d'apprécier la différence entre la clause d'exclusion et les clauses de restriction ou de limitation de la directive 95/46 (analogues à celles de la directive 2002/58). Il est toutefois vrai que les unes et les autres mentionnent des objectifs d'intérêt général similaires, ce qui entraîne une certaine confusion quant à leur portée respective, comme l'avocat général Bot l'avait relevé à l'époque [25].

20 Décision nº 2004/496/CE du Conseil, du 17 mai 2004, concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure (JO 2004, L 183, p. 83, et rectificatif JO 2005, L 255, p. 168) (affaire C-317/04).

21 Décision 2004/535/CE de la Commission, du 14 mai 2004, relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique (JO 2004, L 235, p. 11) (affaire C-318/04).

22 Voir arrêt Parlement/Conseil et Commission, point 57. La Cour souligne, au point 58 de cet arrêt, que le « fait que les données [...] ont été collectées par des opérateurs privés à des fins commerciales et que ce sont ces derniers qui organisent leur transfert vers un État tiers » n'implique pas que ce transfert ne constitue pas l'un des cas de non-application de la directive 95/46 énumérées à l'article 3, paragraphe 2, premier tiret, de cette directive, étant donné que « ce transfert s'insère dans un cadre institué par les pouvoirs publics et visant la sécurité publique ».

23 Ainsi que le soulignera, par la suite, le regretté avocat général Bot dans ses conclusions dans l'affaire Irlande/Parlement et Conseil (C-301/06, EU:C:2008:558), indiquant que l'arrêt Parlement/Conseil et Commission « ne saurait ainsi signifier [...] que seul l'examen de la finalité poursuivie par un traitement de données à caractère personnel est pertinent pour inclure ou bien exclure un tel traitement du champ d'application du système de protection des données mis sur pied par la directive 95/46. Il importe également de vérifier dans le cadre de quel type d'activités s'effectue un traitement de données. Ce n'est que dans le cas où un tel traitement est mis en œuvre pour l'exercice d'activités propres aux États ou aux autorités étatiques et étrangères aux domaines d'activités des particuliers qu'il se trouve exclu du système communautaire de protection des données à caractère personnel issu de la directive 95/46, et ce en application de l'article 3, paragraphe 2, premier tiret, de cette directive » (point 122).

24 Arrêt Parlement/Conseil et Commission, point 58. L'accord avait pour principal objet d'exiger des compagnies aériennes ayant des services de transport de passagers entre l'Union européenne et les États-Unis de fournir aux autorités des États-Unis un accès électronique aux données PNR figurant dans leurs systèmes informatiques de contrôle des réservations et des départs. Il instaurait donc une forme de coopération internationale entre l'Union européenne et les États-Unis en vue de lutter contre le terrorisme et d'autres crimes graves, en tentant de concilier cet objectif avec celui de la protection des données à caractère personnel des passagers. Dans ce contexte, l'obligation imposée aux compagnies n'était pas très différente d'un échange direct de données entre autorités publiques.

25 Conclusions de l'avocat général Bot dans l'affaire Irlande/Parlement et Conseil (C-301/06, EU:C:2008:558, point 127).

49. Cette confusion est probablement à l'origine de la thèse défendue par les États membres qui plaident en faveur de l'inapplicabilité de la directive 2002/58 en l'espèce. Selon eux, l'intérêt de la sécurité nationale n'est sauvegardé que par l'exclusion prévue à l'article 1er, paragraphe 3, de la directive 2002/58. Les limitations autorisées par l'article 15, paragraphe 1, de cette directive, dont celle relative à la sécurité nationale, servent pourtant également ce même intérêt. Cette dernière disposition serait superflue si toute invocation de la sécurité nationale entraînait l'inapplicabilité de la directive 2002/58.

2. L'arrêt Tele2 Sverige et Watson

50. L'affaire Tele2 Sverige et Watson portait sur le point de savoir si certains régimes nationaux qui imposaient aux fournisseurs de services de communications électroniques accessibles au public une obligation générale de conserver les données relatives à ces communications étaient conformes au droit de l'Union. Les situations étaient donc, en substance, identiques à celles examinées dans les présentes demandes de décision préjudicielle.

51. La question de l'applicabilité du droit de l'Union étant à nouveau posée – cette fois en ce qui concerne la directive 2002/58 –, la Cour a commencé par indiquer que « l'étendue du champ d'application de la directive 2002/58 doit être appréciée en tenant compte notamment de l'économie générale de cette dernière » [26].

52. Sous cet angle, la Cour a fait observer que, « [c]ertes, les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 se rapportent à des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers [...]. En outre, les finalités auxquelles, en vertu de cette disposition, de telles mesures doivent répondre, en l'occurrence la sauvegarde de la sécurité nationale [...], recoupent substantiellement les finalités poursuivies par les activités visées à l'article 1er, paragraphe 3, de cette directive » [27].

53. Par conséquent, la finalité des mesures qui, conformément à l'article 15, paragraphe 1, de la directive 2002/58, peuvent être prises par les États membres afin de limiter le droit à la vie privée coïncide (sur ce point) avec celle qui justifie d'exonérer certaines activités étatiques du régime de la directive, conformément à l'article 1er, paragraphe 3, de celle-ci.

54. La Cour a toutefois considéré que, « eu égard à l'économie générale de la directive 2002/58 », cette circonstance ne permettait pas de « conclure que les mesures législatives visées à l'article 15, paragraphe 1, de la directive 2002/58 seraient exclues du champ d'application de cette directive, sauf à priver cette disposition de tout effet utile. En effet, ladite disposition présuppose nécessairement que les mesures nationales qui y sont visées [...] relèvent du champ d'application de cette même directive, puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit » [28].

55. À cela s'ajoute que les limitations autorisées par l'article 15, paragraphe 1, de la directive 2002/58 « régissent, aux fins mentionnées à cette disposition, l'activité des fournisseurs de services de communications électroniques ». Il s'ensuit que cette disposition, lue en combinaison avec l'article 3 de cette directive, « doit être interprété[e] en ce sens que de telles mesures législatives relèvent du champ d'application de cette même directive » [29].

26 Arrêt Tele2 Sverige et Watson, point 67.

27 Arrêt Tele2 Sverige et Watson, point 72.

28 Arrêt Tele2 Sverige et Watson, point 73.

29 Arrêt Tele2 Sverige et Watson, point 74.

56. En conséquence, la Cour a jugé que relèvent du champ d'application de la directive 2002/58 tant une mesure législative qui impose aux fournisseurs « de conserver les données relatives au trafic et les données de localisation, puisqu'une telle activité implique nécessairement un traitement, par ceux-ci, de données à caractère personnel » [30], qu'une mesure législative portant sur l'accès des autorités aux données conservées par ces fournisseurs [31].

57. L'interprétation de la directive 2002/58 retenue par la Cour dans l'arrêt Tele2 Sverige et Watson a été réitérée dans l'arrêt Ministerio Fiscal.

58. Peut-on affirmer que l'arrêt Tele2 Sverige et Watson constitue un revirement, plus ou moins implicite, par rapport à la jurisprudence établie dans l'arrêt Parlement/Conseil et Commission ? C'est ce que considère, par exemple, le gouvernement irlandais, pour qui seule la jurisprudence établie dans l'arrêt Parlement/Conseil et Commission est compatible avec la base légale de la directive 2002/58 et conforme à l'article 4, paragraphe 2, TUE [32].

59. Le gouvernement français estime, quant à lui, que la contradiction peut être surmontée si l'on considère que la jurisprudence de l'arrêt Tele2 Sverige et Watson se réfère aux activités des États membres dans le domaine du droit pénal, alors que celle établie dans l'arrêt Parlement/Conseil et Commission concerne la sûreté de l'État et la défense. Ainsi, la jurisprudence de l'arrêt Tele2 Sverige et Watson ne serait pas applicable à la situation examinée en l'espèce, dans laquelle il conviendrait de se fonder sur la solution retenue dans l'arrêt Parlement/Conseil et Commission [33].

60. Comme je l'ai déjà indiqué, je crois qu'il est possible de trouver une voie de conciliation entre ces deux arrêts, autre que celle préconisée par le gouvernement français. Je ne partage pas cette dernière, car, selon moi, les considérations de l'arrêt Tele2 Sverige et Watson qui font explicitement référence à la lutte contre le terrorisme [34] peuvent être étendues à toute autre menace contre la sécurité nationale (le terrorisme n'étant qu'une menace parmi d'autres).

3. La possibilité d'une interprétation conciliant l'arrêt Parlement/Conseil et Commission et l'arrêt Tele2 Sverige et Watson

61. À mon sens, dans les arrêts Tele2 Sverige et Watson et Ministerio Fiscal, la Cour a tenu compte de la raison d'être des clauses d'exclusion et de restriction ainsi que du lien systématique entre les deux types de clauses.

62. Si, dans l'affaire Parlement/Conseil et Commission, la Cour a jugé que le traitement des données ne relevait pas du champ d'application de la directive 95/46, c'est parce que, ainsi que je l'ai déjà rappelé, dans le contexte de la coopération entre l'Union européenne et les États-Unis, dans un cadre typiquement international, la dimension étatique de l'activité devait prévaloir sur le fait que ce traitement comportait également une dimension commerciale ou privée. L'une des questions dont il était alors débattu était, précisément, la base légale appropriée pour la décision litigieuse.

63. En revanche, en ce qui concerne les mesures nationales examinées dans les arrêts Tele2 Sverige et Watson et Ministerio Fiscal, la Cour a fait prévaloir la portée interne du traitement des données : le cadre réglementaire dans lequel ce traitement était mis en œuvre était purement national et donc dépourvu de la dimension externe qui caractérisait l'objet de l'arrêt Parlement/Conseil et Commission.

30 Arrêt Tele2 Sverige et Watson, point 75.

31 Arrêt Tele2 Sverige et Watson, point 76.

32 Points 15 et 16 des observations écrites du gouvernement irlandais.

33 Points 34 à 50 des observations écrites du gouvernement français.

34 Arrêt Tele2 Sverige et Watson, points 103 et 119.

64. La différence de poids des dimensions internationale et nationale (commerciale et privée) du traitement des données a eu pour conséquence que, dans le premier cas, la clause d'exclusion du droit de l'Union s'est imposée comme étant la plus à même de protéger l'intérêt général qui se traduit dans la sécurité nationale. Dans le second cas, en revanche, ce même intérêt pouvait être efficacement servi par la clause de limitation prévue à l'article 15, paragraphe 1, de la directive 2002/58.

65. Une autre divergence pourrait également être observée, liée au contexte réglementaire : chacun de ces deux arrêts s'est centré sur l'interprétation de deux dispositions qui, au-delà de leur apparence, ne sont pas les mêmes.

66. Ainsi, dans l'arrêt Parlement/Conseil et Commission, la Cour s'est prononcée sur l'interprétation de l'article 3, paragraphe 2, de la directive 95/46, alors que, dans l'arrêt Tele2 Sverige et Watson, la disposition interprétée était l'article 1er, paragraphe 3, de la directive 2002/58. Une lecture attentive de ces articles révèle une divergence suffisante pour étayer le sens des décisions de la Cour dans l'un et l'autre cas.

67. Aux termes de l'article 3, paragraphe 2, de la directive 95/46, « [l]a présente directive *ne s'applique pas au traitement de données à caractère personnel* [...] mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire [...] et, en tout état de cause, *aux traitements* ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces *traitements* sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal » [35].

68. Pour sa part, l'article 1er, paragraphe 3, de la directive 2002/58 indique que celle-ci « *ne s'applique pas aux activités* qui ne relèvent pas du traité instituant la Communauté européenne [...] et, en tout état de cause, *aux activités* concernant la sécurité publique, la défense, la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'*activités* liées à la sûreté de l'État) ou aux activités de l'État dans des domaines relevant du droit pénal » [36].

69. Alors que l'article 3, paragraphe 2, de la directive 95/46 exclut le *traitement des données* ayant pour objet – pour ce qui nous intéresse ici – la sûreté de l'État, l'article 1er, paragraphe 3, de la directive 2002/58 exclut les *activités* visant à préserver – également pour ce qui importe ici – la sûreté de l'État.

70. La différence n'est pas anodine. La directive 95/46 excluait de son champ d'application une activité (le « traitement de données à caractère personnel ») pouvant être effectuée par tout un chacun. Étaient spécifiquement exclus de cette activité les traitements ayant, entre autres, pour objet la sûreté de l'État. En revanche, la nature du sujet procédant au traitement des données était dénuée d'importance. L'approche adoptée pour identifier les actions exclues était donc téléologique ou finaliste, sans opérer de distinction en fonction de l'auteur de l'action.

71. On comprend dès lors que, dans l'affaire Parlement/Conseil et Commission, la Cour ait avant tout tenu compte de la finalité poursuivie par le traitement des données. Le « fait que les données [...] ont été collectées par des opérateurs privés à des fins commerciales et que ce sont ces derniers qui organisent leur transfert vers un États tiers » n'importait pas, l'essentiel étant que « ce transfert s'insère dans un cadre institué par les pouvoirs publics et visant la sécurité publique » [37].

72. En revanche, « les activités concernant la sûreté de l'État », étrangères au champ d'application de la directive 2002/58 examiné dans l'affaire Tele2 Sverige et Watson, peuvent être menées non pas par tout sujet, mais uniquement par l'État lui-même. En outre, elles n'incluent pas les fonctions normatives ou réglementaires de l'État, mais uniquement les actions matérielles des pouvoirs publics.

35 Mise en italique par mes soins.

36 Mise en italique par mes soins.

37 Arrêt Parlement/Conseil et Commission, point 58.

73. En effet, les *activités* citées à l'article 1er, paragraphe 3, de la directive 2002/58 « sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers »[38]. Si elles incluaient toutes les actions, toutes les dispositions prises par les États membres relativement au traitement de données à caractère personnel seraient exclues du champ d'application de la directive 2002/58, pour peu d'être justifiées comme étant nécessaires pour garantir la sûreté de l'État.

74. D'une part, cela entraînerait une perte notable d'effet utile de la directive 2002/58, puisque la simple invocation d'une notion juridique aussi floue que celle de la sécurité nationale suffirait pour ne pas pouvoir opposer aux États membres les sauvegardes conçues par le législateur de l'Union aux fins de protéger les données personnelles des citoyens. Cette protection est irréalisable sans le concours des États membres et sa garantie est assurée, pour le citoyen, également vis-à-vis des pouvoirs publics nationaux.

75. D'autre part, une interprétation de la notion d'« activités étatiques » entendant comme telles les activités qui se traduisent par l'adoption de règles et de dispositions juridiques priverait de sens l'article 15 de la directive 2002/58, qui permet précisément aux États membres d'adopter, pour des raisons de protection, entre autres, de la sécurité nationale, des « mesures législatives » afin de limiter la portée de certains droits et obligations prévus par cette directive[39].

76. Ainsi que la Cour l'a souligné dans l'arrêt Tele2 Sverige et Watson, « l'étendue du champ d'application de la directive 2002/58 doit être appréciée en tenant compte notamment de l'économie générale de cette dernière »[40]. Sous cet angle, l'interprétation de l'article 1er, paragraphe 3, et de l'article 15, paragraphe 1, de la directive 2002/58 qui leur donne un sens sans leur ôter tout effet utile est celle qui identifie, dans la première des deux dispositions, une exclusion matérielle se rapportant aux *activités* menées par les États membres dans le domaine de la sécurité nationale (et dans des domaines équivalents) et, dans la seconde disposition, le droit de prendre des *mesures légales* (c'est-à-dire des règles de portée générale) qui, à des fins de sécurité nationale, concernent les activités des personnes soumises à l'imperium des États membres, en limitant les droits garantis par la directive 2002/58.

4. L'exclusion de la sécurité nationale dans la directive 2002/58

77. La sécurité nationale (autrement dénommée, la « sûreté de l'État », comme le souligne l'article 15, paragraphe 1, de la directive 2002/58) fait l'objet d'une double considération dans cette directive. D'une part, elle constitue un motif d'*exclusion* (de l'application de ladite directive) pour toutes les activités des États membres qui, spécifiquement, la « concernent ». D'autre part, elle se présente comme une cause de *limitation*, qui doit être mise en œuvre par la loi, des droits et des obligations prévus par la même directive, c'est-à-dire ayant trait à des activités de nature privée ou commerciale ne relevant pas du domaine des activités régaliennes[41].

38 Arrêt Ministerio Fiscal, point 32 ; voir, dans le même sens, arrêt Tele2 Sverige et Watson, point 72.

39 Il serait en effet difficile de soutenir que l'article 15, paragraphe 1, de la directive 2002/58 permet de limiter les droits et les obligations que cette directive proclame dans un domaine qui, tel que celui de la sécurité nationale, serait, par principe, exclu de son champ d'application, en vertu de l'article 1er, paragraphe 3, de ladite directive. Comme la Cour l'a jugé au point 73 de son arrêt Tele2 Sverige et Watson, l'article 15, paragraphe 1, de la même directive « présuppose nécessairement que les mesures nationales qui y sont visées [...] relèvent du champ d'application de [la] directive [2002/58], puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit ».

40 Arrêt Tele2 Sverige et Watson, point 67.

41 Comme l'indiquait, de manière incidente, l'avocat général Saugmandsgaard Øe au point 47 de ses conclusions dans l'affaire Ministerio Fiscal (C-207/16, EU:C:2018:300), « il convient de ne pas confondre, d'une part, les données à caractère personnel traitées *directement* dans le cadre des activités – de nature régalienne – de l'État en un domaine relevant du droit pénal et, d'autre part, celles traitées dans le cadre des activités – de nature commerciale – d'un prestataire de services de communications électroniques qui sont *ensuite* utilisées par les autorités étatiques compétentes ».

78. Quelles sont les activités visées à l'article 1er, paragraphe 3, de la directive 2002/58/CE ? Selon moi, le Conseil d'État lui-même en offre un bon exemple en mentionnant les articles L. 851-5 et L. 851-6 du code de la sécurité intérieure et en se référant aux « techniques de recueil de renseignement directement mises en œuvre par l'État sans régir les activités des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques »[42].

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

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

81. Étant donné que, dans les présentes demandes de décision préjudicielle, il y a une implication de particuliers (à savoir ceux fournissant aux utilisateurs les services de communications électroniques) et non une simple intervention des autorités étatiques, il n'est pas nécessaire de s'attarder davantage sur la délimitation des contours de la notion de « sécurité nationale » stricto sensu.

82. J'estime cependant qu'une orientation peut être donnée par le critère de la décision-cadre 2006/960/JAI[43], dont l'article 2, sous a), établit une distinction entre, d'une part, les services de sécurité au sens large – à savoir « un service national de police, de douane ou autre qui est autorisé par le droit national à dépister et à prévenir les infractions ou les activités criminelles, à enquêter à leur propos, et à exercer l'autorité publique et à prendre des mesures coercitives dans le cadre de ces activités » – et, d'autre part, les « agences ou les unités spécialisées dans les questions de sécurité nationale »[44].

83. Il est affirmé, dans le considérant 11 de la directive 2002/58, que, « [à] l'instar de la directive 95/46/CE, la présente directive ne traite pas des questions de protection des droits et libertés fondamentaux liées à des activités qui ne sont pas régies par le droit [de l'Union] ». La directive 2002/58 « ne modifie donc pas l'équilibre existant entre le droit des personnes à une vie privée et la possibilité dont disposent les États membres de prendre des mesures telles que celles visées à l'article 15, paragraphe 1, de la présente directive, nécessaires pour la protection de la [...] sûreté de l'État ».

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

42 Points 18 et 21 de la décision de renvoi dans l'affaire C-511/18.

43 Décision-cadre du Conseil, du 18 décembre 2016, relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne (JO 2006, L 386, p. 89).

44 Dans le même ordre d'idées, l'article 1er, paragraphe 4, de la décision-cadre 2008/977/JAI du Conseil, du 27 novembre 2008, relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale (JO 2008, L 350, p. 60), prévoyait que cette décision-cadre « est sans préjudice des intérêts essentiels en matière de sécurité nationale et des activités de renseignement spécifiques dans le domaine de la sécurité nationale ».

85. L'« équilibre » mentionné dans le considérant 11 de la directive 2002/58 résulte de la nécessité de respecter les compétences des États membres en matière de sécurité nationale lorsque ceux-ci les exercent *directement et par leurs propres moyens*. En revanche, lorsque, y compris pour ces mêmes raisons de sécurité nationale, le concours de particuliers auxquels certaines obligations sont imposées est requis, cette circonstance détermine l'entrée dans un domaine (la protection de la vie privée qui peut être exigée de ces acteurs privés) régi par le droit de l'Union.

86. Tant la directive 95/46 que la directive 2002/58 s'efforcent d'atteindre cet équilibre en permettant que les droits des particuliers soient limités par des actes normatifs adoptés par les États en vertu, respectivement, de l'article 13, paragraphe 1, de la directive 95/46 et de l'article 15, paragraphe 1, de la directive 2002/58. Il n'y a sur ce point aucune différence entre ces deux directives.

87. Quant au règlement 2016/679, qui crée un (nouveau) cadre général de protection des données à caractère personnel, son article 2, paragraphe 2, exclut qu'il y ait « traitement de données à caractère personnel » lorsque les États membres exercent des « activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne ».

88. Alors que, dans la directive 95/46, le traitement de données à caractère personnel n'était qualifié qu'au regard de sa finalité, quel que soit le sujet l'exerçant, dans le règlement 2016/679, les traitements exclus sont identifiés en fonction tant de leur finalité que de leurs auteurs : sont écartés les traitements effectués par les États membres dans le cadre d'une *activité* qui ne relève pas du champ d'application du droit de l'Union [article 2, paragraphe 2, sous a) et b)] ainsi que les traitements effectués par les autorités *à des fins de lutte contre les infractions pénales et de protection* contre les menaces pour la sécurité publique [45].

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

90. Tout comme pour la directive 2002/58, il ne serait pas cohérent que les mesures législatives prévues à l'article 23 du règlement 2016/679 (qui, je le répète, autorise les limitations étatiques des droits à la vie privée des citoyens pour des raisons de sûreté de l'État) relèvent du champ d'application de ce règlement et que, simultanément, l'invocation de la sûreté de l'État rende ledit règlement tout bonnement inapplicable, ce qui impliquerait l'absence de reconnaissance de tout droit subjectif.

B. La confirmation et les possibilités de développement de la jurisprudence Tele2 Sverige et Watson

91. Dans mes conclusions dans l'affaire C-520/18, j'ai effectué une analyse détaillée [46] de la jurisprudence de la Cour en cette matière, dont je propose ici de confirmer le résultat, tout en suggérant une voie d'interprétation pour en préciser le contenu.

45 En effet, le règlement 2016/679 exclut le traitement de données effectué par les États membres dans le cadre d'une *activité* qui ne relève pas du champ d'application du droit de l'Union, outre le traitement effectué par les autorités *à des fins de protection* de la sécurité publique.

46 Ordre des barreaux francophones et germanophone e.a. (EU:C:2020:7, points 27 à 68).

92. Je renvoie à cette analyse, que je ne juge pas nécessaire de reproduire ici, pour de simples raisons d'économie de la procédure. Les réflexions suivantes sur les questions préjudicielles posées par le Conseil d'État doivent donc s'entendre comme faites sur la prémisse des points correspondants des conclusions dans l'affaire C-520/18.

C. La réponse aux questions préjudicielles

1. Sur l'obligation de conservation des données (première question préjudicielle dans les affaires C-511/18 et C-512/18 et deuxième question dans l'affaire C-512/18)

93. Quant à l'obligation de conservation de données imposée aux fournisseurs de services de communications électroniques, la juridiction de renvoi souhaite notamment savoir :

– si cette obligation, exigible en vertu de l'article 15, paragraphe 1, de la directive 2002/58, constitue une ingérence justifiée par le « droit à la sûreté » garanti à l'article 6 de la Charte et par des exigences de sécurité nationale (première question dans les affaires C-511/18 et C-512/18 et troisième question dans l'affaire C-511/18) et

– si la directive 2000/31 autorise la conservation de données de nature à permettre l'identification de ceux qui ont contribué à la création de contenus accessibles au public en ligne (deuxième question dans l'affaire C-512/18).

a) Considération liminaire

94. Le Conseil d'État se réfère aux droits fondamentaux reconnus aux articles 7 (respect de la vie privée et familiale), 8 (protection des données personnelles) et 11 (liberté d'expression et d'information) de la Charte. Ce sont là, en effet, les droits qui, selon la Cour, pourraient être affectés par l'obligation de conserver des données relatives au trafic imposée par les autorités nationales aux fournisseurs de services de communications électroniques [47].

95. La juridiction de renvoi mentionne également le droit à la sûreté protégé par l'article 6 de la Charte. Plus qu'en tant que droit éventuellement affecté, elle l'invoque comme facteur qui pourrait justifier l'imposition d'une telle obligation.

96. Je partage l'avis de la Commission selon lequel l'invocation de l'article 6 de la Charte en ces termes peut être équivoque. De même que la Commission, je considère que cette disposition ne doit pas être interprétée comme apte à « imposer une obligation positive à l'Union d'adopter des mesures en vue de protéger les personnes contre des actes criminels » [48].

97. La sûreté garantie par l'article 6 de la Charte ne s'identifie pas avec la sécurité publique ou, si l'on préfère, n'a pas plus à voir avec cette dernière que tout autre droit fondamental, dans la mesure où la sécurité publique est une condition indispensable à la jouissance des droits et libertés fondamentaux.

47 Voir, en ce sens, arrêt Tele2 Sverige et Watson, point 92, qui renvoie, par analogie, à l'arrêt Digital Rights, points 25 et 70.

48 Point 37 des observations écrites de la Commission.

98. Ainsi que la Commission le rappelle, l'article 6 de la Charte correspond à l'article 5 de la convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (ci-après la « CEDH »), comme il découle des explications qui l'accompagnent. Il ressort de la lecture de l'article 5 de la CEDH que la « sûreté » qui y est protégée est strictement la sécurité personnelle, entendue en tant que garantie du droit à la liberté physique contre l'arrestation ou la détention arbitraires ; c'est en définitive l'assurance que nul ne peut être privé de sa liberté, sauf dans les cas, selon les conditions et conformément aux procédures établies par la loi.

99. Il s'agit donc de la *sécurité personnelle*, relative aux conditions dans lesquelles la liberté physique des personnes peut être restreinte [49], et non de la *sécurité publique* inhérente à l'existence de l'État, condition indispensable, au sein d'une société développée, pour concilier l'exercice des pouvoirs publics et la jouissance des droits individuels.

100. Certains gouvernements demandent toutefois que le droit à la sécurité soit davantage pris en considération dans le second sens. En réalité, la Cour ne l'a pas ignoré ; elle l'a même expressément mentionné dans ses arrêts [50] et avis [51]. Elle n'a jamais nié l'importance des objectifs d'intérêt général que sont la protection de la sécurité nationale et de l'ordre public [52], la lutte contre le terrorisme international en vue du maintien de la paix et de la sécurité internationales et la lutte contre les infractions graves afin de garantir la sécurité publique [53], importance qu'elle a qualifiée, à juste titre, de « primordiale » [54]. Comme elle l'a indiqué à l'époque, « la protection de la sécurité publique contribue également à la protection des droits et libertés d'autrui » [55].

101. On pourrait profiter de l'opportunité offerte par les présentes demandes de décision préjudicielle pour proposer plus clairement la recherche d'un équilibre entre, d'une part, le droit à la sécurité et, d'autre part, le droit à la vie privée et le droit à la protection des données à caractère personnel. Cela permettrait d'éviter les critiques selon lesquelles les seconds seraient favorisés au détriment du premier.

102. C'est à cet équilibre que se réfèrent, selon moi, le considérant 11 et l'article 15, paragraphe 1, de la directive 2002/58, lorsqu'ils mentionnent les exigences de nécessité et de proportionnalité des mesures *au sein d'une société démocratique*. Le droit à la sécurité, je le répète, est inhérent à l'existence même et à la survie d'une démocratie, ce qui justifie qu'il soit pleinement pris en compte dans le cadre de l'appréciation de cette proportionnalité. En d'autres termes, si la préservation du principe de confidentialité des données est primordiale dans une société démocratique, l'importance de la sécurité au sein de cette société ne doit pas être sous-estimée.

103. Le contexte des menaces graves et persistantes pour la sécurité nationale, notamment le risque de terrorisme, doit donc être pris en considération, dans la droite ligne de ce qui est indiqué dans la dernière phrase du point 119 de l'arrêt Tele2 Sverige et Watson. Un système national peut répondre de manière proportionnée à la nature et à l'intensité des menaces auxquelles il est confronté sans que cette réponse doive nécessairement être identique à celle d'autres États membres.

49 C'est ainsi que la Cour européenne des droits de l'homme l'a interprété, notamment dans l'arrêt du 5 juillet 2016, Buzadji c. République de Moldavie, ECHR:2016 :0705JUD002375507, au point 84 duquel il est affirmé que le but essentiel du droit reconnu par l'article 5 de la CEDH est de prévenir la privation de liberté individuelle arbitraire ou injustifiée.

50 Arrêt Digital Rights, point 42.

51 Avis 1/15 (accord PNR UE-Canada), du 26 juillet 2017 (EU:C:2017:592, point 149 et jurisprudence citée) (ci-après l'« avis 1/15 »).

52 Arrêt du 15 février 2016, N. (C-601/15 PPU, EU:C:2016:84, point 53).

53 Arrêt Digital Rights (point 42 et jurisprudence citée).

54 Arrêt Digital Rights, point 51.

55 Avis 1/15, point 149.

104. Enfin, je dois ajouter que les réflexions qui précèdent ne s'opposent pas à ce que, dans des situations réellement *exceptionnelles*, caractérisées par une menace imminente ou par un risque extraordinaire justifiant la déclaration officielle d'une situation d'urgence dans un État membre, la législation nationale prévoie, pour une période limitée, la possibilité d'imposer une obligation de conservation de données aussi étendue et générale qu'il est jugé indispensable [56].

105. Par conséquent, la première question posée dans les deux demandes de décision préjudicielle devrait être reformulée et plutôt orientée sur la possibilité de justifier l'ingérence par des motifs de sécurité nationale. Le doute porterait donc sur le point de savoir si l'obligation imposée aux opérateurs de services de communications électroniques est compatible avec l'article 15, paragraphe 1, de la directive 2002/58.

b) Appréciation

1) La caractérisation des règles nationales, telles qu'elles sont exposées dans les deux demandes de décision préjudicielle, à la lumière de la jurisprudence de la Cour

106. Conformément aux décisions de renvoi, la réglementation litigieuse dans les procédures au principal impose l'obligation de conservation des données :

– aux opérateurs de communications électroniques, notamment à ceux qui offrent 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 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 [57].

107. Les opérateurs doivent conserver, pendant un an à compter du jour de leur enregistrement, les informations permettant d'identifier l'utilisateur, les données relatives aux équipements terminaux de communication utilisés, les caractéristiques techniques, la date, l'horaire et la durée de chaque appel, les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ainsi que les données qui permettent d'identifier le destinataire de la communication et, pour les activités de téléphonie, l'origine et la localisation de la communication [58].

108. S'agissant, notamment, des services d'accès à Internet et des services de stockage, la réglementation nationale semble exiger la conservation des adresses IP [59], des clefs d'accès et, en cas de souscription payante d'un contrat ou d'un compte, le type de paiement utilisé ainsi que la référence du paiement, le montant, la date et l'heure de la transaction [60].

56 Voir mes conclusions dans l'affaire Ordre des barreaux francophones et germanophone e.a. (C-520/18, EU:C:2020:7, points 105 à 107).

57 C'est ce qui résulte de l'article L. 851-1 du code de la sécurité intérieure, qui renvoie à l'article L. 34-1 du code des postes et des communications électroniques ainsi qu'à l'article 6 de la loi nº 2004-575.

58 C'est ce que prévoit l'article R. 10-13 du code des postes et des communications électroniques.

59 Il appartient à la juridiction de renvoi de vérifier ce point, sur lequel des divergences sont apparues lors de l'audience.

60 Article 1er du décret 2011-219.

109. Cette conservation est exigée pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales [61]. En d'autres termes, contrairement à ce qui a lieu – comme je le montrerai ci-après – avec l'obligation de *recueillir* des données relatives au trafic et des données de localisation, l'obligation de *conserver* de telles données n'a pas pour seul objectif la prévention du terrorisme [62].

110. En ce qui concerne les conditions d'*accès* aux données conservées, il ressort des informations figurant dans le dossier soit qu'il s'agit des conditions prévues pour le régime commun (intervention de l'autorité judiciaire), soit que cet accès est limité à des agents individuellement désignés et habilités, après autorisation du Premier ministre délivrée sur la base de l'avis non contraignant d'une autorité administrative indépendante [63].

111. Il est facile de constater que, ainsi que la Commission l'a souligné [64], les données dont la conservation est exigée par les règles nationales correspondent, en substance, à celles examinées par la Cour dans les arrêts Digital Rights et Tele2 Sverige et Watson [65]. Tout comme alors, ces données font l'objet d'une « obligation de conservation généralisée et indifférenciée », ainsi que le Conseil d'État le souligne clairement au début de ses questions préjudicielles.

112. Si tel est le cas, point qu'il appartient en définitive à la juridiction de renvoi d'apprécier, force est de conclure que la réglementation en cause constitue une « ingérence [...] dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte [qui] s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave » [66].

113. Aucune des parties étant intervenues n'a mis en doute le fait qu'une telle réglementation constitue une ingérence dans ces droits. Il n'est pas nécessaire de s'attarder ici sur ce point, pas même pour rappeler que l'atteinte à ces droits porte inévitablement atteinte aux fondements mêmes d'une société qui entend respecter, entre autres valeurs, le droit à la vie privée consacré par la Charte.

114. L'application de la jurisprudence établie dans l'arrêt Tele2 Sverige et Watson et confirmée dans l'arrêt Ministerio Fiscal conduirait naturellement à affirmer qu'une réglementation telle que celle en cause en l'espèce « 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, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte » [67].

115. En effet, à l'instar de la réglementation examinée dans l'arrêt Tele2 Sverige et Watson, celle qui nous occupe ici couvre elle-aussi « de manière généralisée tous les abonnés et utilisateurs inscrits et vise tous les moyens de communication électronique ainsi que l'ensemble des données relatives au trafic [et] ne prévoit aucune différenciation, limitation ou exception en fonction de l'objectif poursuivi » [68]. Par conséquent, « [e]lle s'applique [...] même à des personnes pour lesquelles il n'existe

61 Article R. 10-13 du code des postes et des communications électroniques.

62 Tant la Quadrature du Net que la Fédération des fournisseurs d'accès à Internet associatifs soulignent l'ampleur des finalités de la conservation, le pouvoir d'appréciation discrétionnaire conféré aux autorités, l'absence de critères objectifs quant à la définition de ces finalités et l'importance accordée à des formes de criminalité ne pouvant pas être qualifiées de graves.

63 La commission nationale de contrôle des techniques de renseignement (France) ; voir, à cet égard, points 145 à 148 des observations écrites du gouvernement français.

64 Point 60 des observations écrites de la Commission.

65 En réalité, elles vont un peu au-delà, puisque, dans le cas des services d'accès à Internet, la conservation de l'adresse IP ou des clefs d'accès semble également être prévue.

66 Arrêt Tele2 Sverige et Watson, point 100.

67 Arrêt Tele2 Sverige et Watson, point 107.

68 Arrêt Tele2 Sverige et Watson, point 105.

aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec des infractions pénales graves », et ce sans aucune exception, « de telle sorte qu'elle s'applique même à des personnes dont les communications sont soumises, selon les règles du droit national, au secret professionnel »[69].

116. De même, la réglementation litigieuse « ne requiert aucune relation entre les données dont la conservation est prévue et une menace pour la sécurité publique. Notamment, elle n'est pas limitée à une conservation portant soit sur des données afférentes 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 »[70].

117. Il ressort de ce qui précède que cette réglementation « 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, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte »[71].

118. Ce qui précède a suffi pour que la Cour conclue que les règles nationales concernées n'étaient pas compatibles avec l'article 15, paragraphe 1, de la directive 2002/58, dans la mesure où elles consacraient, « à des fins de lutte contre la criminalité, une 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 »[72].

119. La question qui se pose maintenant est de savoir si la jurisprudence de la Cour en matière de conservation de données à caractère personnel peut être, si ce n'est reconsidérée, à tout le moins nuancée, lorsque la finalité de cette conservation « généralisée et indifférenciée » est la lutte contre le terrorisme. La première question posée dans l'affaire C-511/18 est justement formulée « dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste ».

120. Toutefois, s'il s'agit là du *contexte factuel* dans lequel l'obligation de conserver les données est imposée, dans son *contexte réglementaire*, le terrorisme n'est pas la seule justification possible. Le régime de conservation et d'accès aux données litigieux dans la procédure devant le Conseil d'État subordonne cette obligation, de manière générale, aux besoins de la recherche, de la constatation et de la poursuite des infractions pénales.

121. En tout état de cause, je rappellerai que la lutte contre le terrorisme n'est pas restée en marge de l'argumentation dans l'arrêt Tele2 Sverige et Watson, la Cour ayant alors toutefois considéré que cette forme de criminalité grave n'entraînait pas un besoin de modifier sa jurisprudence[73].

122. Dès lors et par principe, je considère qu'il conviendrait de répondre à la question posée par la juridiction de renvoi, axée sur la spécificité de la menace terroriste, dans le sens où la Cour a statué dans l'arrêt Tele2 Sverige et Watson.

69 Arrêt Tele2 Sverige et Watson, point 105.
70 Arrêt Tele2 Sverige et Watson, point 106.
71 Arrêt Tele2 Sverige et Watson, point 107.
72 Arrêt Tele2 Sverige et Watson, point 112.
73 Arrêt Tele2 Sverige et Watson, point 103.

123. Comme je l'ai soutenu dans mes conclusions dans l'affaire Stichting Brein, « [l]a certitude dans l'application du droit exige sinon que les juridictions appliquent le principe stare decisis à proprement parler, du moins qu'elles aient la prudence de s'en tenir à ce qu'elles ont elles-mêmes décidé, après mûre réflexion, à l'égard d'un problème juridique déterminé » [74].

2) La conservation restreinte des données, eu égard aux menaces contre la sûreté de l'État, y compris la menace terroriste

124. Serait-il néanmoins possible de nuancer ou de compléter cette jurisprudence, au vu de ses conséquences en matière de lutte contre le terrorisme ou de protection de l'État face à d'autres menaces analogues contre la sécurité nationale ?

125. J'ai déjà souligné que la simple conservation de données à caractère personnel implique une ingérence dans les droits garantis par les articles 7, 8 et 11 de la Charte [75]. Outre le fait qu'elle vise, en fin de compte, à permettre l'*accès*, rétrospectif ou simultané, aux données à un moment déterminé [76], la simple conservation de données au-delà de ce qui est strictement nécessaire pour la transmission d'une communication ou pour la facturation des services fournis par le prestataire entraîne le non-respect des limites prévues aux articles 5 et 6 de la directive 2002/58.

126. Les utilisateurs de ces services (en réalité la quasi-totalité des citoyens dans les sociétés les plus développées) ont ou devraient pouvoir avoir l'attente légitime que, en l'absence de leur consentement, ne seront pas conservées plus de données les concernant que celles stockées conformément à ces dispositions. Les dérogations prévues à l'article 15, paragraphe 1, de la directive 2002/58 doivent s'entendre sur le fondement de cette prémisse.

127. Comme je l'ai déjà expliqué, la Cour a rejeté, dans l'arrêt Tele2 Sverige et Watson, la conservation généralisée et indifférenciée des données à caractère personnel également en ce qui concerne la lutte contre le terrorisme [77].

128. Concernant les critiques formulées, je ne crois pas que la jurisprudence établie dans cet arrêt sous-estime la menace terroriste, forme de criminalité particulièrement grave comportant un dessein explicite de contestation de l'autorité de l'État et de déstabilisation ou de destruction de ses institutions. La lutte contre le terrorisme est littéralement vitale pour l'État et la mener à bien constitue un objectif d'intérêt général auquel un État de droit ne saurait renoncer.

74 C-527/15, EU:C:2016:938, point 41.

75 Ainsi que la Cour l'a rappelé au point 124 de son avis 1/15, « la communication de données à caractère personnel à un tiers, telle qu'une autorité publique, constitue une ingérence dans le droit fondamental consacré à l'article 7 de la Charte, quelle que soit l'utilisation ultérieure des informations communiquées. Il en va de même de la conservation des données à caractère personnel ainsi que de l'accès auxdites données en vue de leur utilisation par les autorités publiques. À cet égard, il importe peu que les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou que les intéressés aient ou non subi d'éventuels inconvénients en raison de cette ingérence ».

76 Comme l'indiquait l'avocat général Cruz Villalón dans ses conclusions dans l'affaire Digital Rights, C-293/12 et C-594/12 (EU:C:2013:845, point 72), « la collecte [...] et, surtout, la conservation [...], dans de gigantesques bases de données, des multiples données générées ou traitées dans le cadre de la plus grande partie des communications électroniques courantes des citoyens de l'Union [...] constituent une ingérence caractérisée dans leur vie privée, quand bien même elles ne feraient que créer les conditions de possibilité d'un contrôle rétrospectif de leurs activités tant personnelles que professionnelles. La collecte de ces données crée les conditions d'une surveillance qui, pour ne s'exercer que rétrospectivement à l'occasion de leur exploitation, menace néanmoins de manière permanente, pendant toute la durée de leur conservation, le droit des citoyens de l'Union au secret de leur vie privée. Le sentiment diffus de surveillance [...] généré pose de manière particulièrement aiguë la question de la durée de conservation des données ».

77 Arrêt Tele2 Sverige et Watson, point 103 : un objectif d'intérêt général tel que la lutte contre le terrorisme « ne saurait à lui seul justifier qu'une réglementation nationale prévoyant la conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation soit considérée comme nécessaire aux fins de ladite lutte ».

129. Presque tous les gouvernements qui sont intervenus dans la procédure ainsi que la Commission ont indiqué que, outre ses difficultés techniques, une conservation partielle et différenciée des données à caractère personnel priverait les services de renseignement nationaux de la possibilité d'accéder à des informations indispensables à l'identification des menaces pour la sécurité publique et la défense de l'État et pour poursuivre les auteurs d'attentats terroristes [78].

130. Face à cette appréciation, il me semble pertinent d'indiquer que la lutte antiterroriste ne doit pas être envisagée uniquement au regard de son efficacité ; d'où sa difficulté, mais aussi sa grandeur lorsque ses moyens et ses méthodes répondent aux exigences de l'État de droit, à savoir avant tout la soumission du pouvoir et de la force aux limites du droit et, en particulier, à un ordre juridique dont la défense des droits fondamentaux constitue la raison d'être et la finalité.

131. Si la justification des moyens du terrorisme ne répond à aucun autre critère que celui de l'efficacité pure (et maximale) de ses atteintes à l'ordre établi, pour l'État de droit, l'effectivité se mesure en des termes qui ne tolèrent pas de passer outre, lors de sa défense, les procédures et les garanties qui en font un ordre légitime. S'il s'abandonnait à la simple efficacité, l'État de droit perdrait la qualité qui le distingue et pourrait devenir, dans des cas extrêmes, une menace pour le citoyen. Si les pouvoirs publics étaient dotés d'instruments démesurés aux fins de la poursuite de l'infraction, leur permettant d'ignorer ou de dénaturer les droits fondamentaux, rien ne pourrait faire obstacle à ce que leur action incontrôlée et entièrement libre s'exerce en fin de compte au détriment de la liberté de tous.

132. L'efficacité des pouvoirs publics, je le répète, se heurte à la barrière infranchissable des droits fondamentaux des citoyens, dont les limitations ne peuvent, conformément à l'article 52, paragraphe 1, de la Charte, être prévues que par la loi et dans le respect de leur contenu essentiel « si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et des libertés d'autrui » [79].

133. En ce qui concerne les conditions dans lesquelles, selon l'arrêt Tele2 Sverige et Watson, une conservation *ciblée* de données serait permise, je renvoie à mes conclusions dans l'affaire C-520/18 [80].

134. Un cas légitime d'imposition de l'obligation de conserver certaines données peut être constitué par la situation dans laquelle les informations disponibles détenues par les services de sécurité étayent le soupçon fondé de la préparation d'un attentat terroriste. Il peut à plus forte raison en aller ainsi lorsqu'un attentat est effectivement commis. Si, dans ce dernier cas, la perpétration de l'infraction peut à elle seule constituer une circonstance justifiant l'adoption d'une telle mesure, en cas de simple soupçon d'un éventuel attentat, il serait nécessaire que les circonstances qui la fondent offrent un degré minimal de plausibilité, indispensable aux fins d'une évaluation objective des éléments pouvant justifier une telle mesure.

78 C'est, par exemple, l'interprétation faite par le gouvernement français, qui illustre cette affirmation avec des exemples concrets de l'utilité de la conservation généralisée des données, qui a permis à l'État de réagir face aux graves attentats terroristes subis dans son pays ces dernières années (points 107 et 122 à 126 des observations écrites du gouvernement français).

79 Arrêt du 15 février 2016, N. (C-601/15 PPU, EU:C:2016:84, point 50). Il s'agit donc du difficile équilibre entre l'ordre public et la liberté auquel j'ai déjà fait référence et auquel aspire par principe l'ensemble du droit de l'Union. Citons à titre d'exemple 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 2017, L 88, p. 6). Tout en prévoyant, à son article 20, paragraphe 1, que les États membres doivent veiller à ce que les personnes chargées des enquêtes ou des poursuites concernant les infractions terroristes disposent d'« outils d'enquête efficaces », elle déclare, dans son considérant 21, que l'utilisation de ces outils efficaces doit « être ciblée et tenir compte du principe de proportionnalité et de la nature et de la gravité des infractions qui font l'objet de l'enquête, et respecter le droit à la protection des données à caractère personnel ».

80 Ordre des barreaux francophones et germanophone e.a. (EU:C:2020:7, points 87 à 95).

135. Bien que ce soit difficile, il n'est pas impossible de déterminer avec précision et conformément à des critères objectifs tant les catégories de données dont la conservation est jugée indispensable que le cercle des personnes concernées. La conservation générale et indifférenciée de toutes les données susceptibles d'être recueillies par les fournisseurs de services de communication électronique serait certes la solution la plus *pratique* et la plus *efficace* ; toutefois, comme je l'ai déjà indiqué, la question ne saurait être posée en termes d'*efficacité pratique*, mais en termes d'*efficacité juridique* et dans le contexte d'un État de droit.

136. Ce travail de détermination relève typiquement du domaine de la loi, dans les limites fixées par la jurisprudence de la Cour. Je renvoie à nouveau à ce que j'ai exposé sur ce point dans mes conclusions dans l'affaire C-520/18 [81].

3) L'accès aux données conservées

137. En partant de la prémisse que les opérateurs ont recueilli les données en respectant les dispositions de la directive 2002/58 et que ces données ont été conservées conformément à l'article 15, paragraphe 1, de cette directive [82], l'accès des autorités compétentes à ces informations doit se faire dans les conditions exigées par la Cour et que, pour ma part, j'analyse dans mes conclusions dans l'affaire C-520/18, auxquelles je renvoie [83].

138. Par conséquent, dans ce cas aussi, la réglementation nationale doit prévoir les conditions matérielles et procédurales régissant l'accès des autorités compétentes aux données conservées [84]. Dans le cadre des présentes demandes de décision préjudicielle, ces conditions autoriseraient l'accès aux données des personnes soupçonnées de projeter, de commettre, d'avoir commis ou d'être impliquées dans un acte terroriste [85].

139. L'essentiel est toutefois que, sauf cas d'urgence dûment justifiés, l'accès aux données concernées soit soumis au contrôle préalable d'une juridiction ou d'une autorité administrative indépendante dont la décision réponde à une demande motivée des autorités compétentes [86]. Ainsi, là où le contrôle abstrait de la loi ne peut être obtenu, le contrôle in concreto de cette autorité indépendante, tout aussi attachée à la garantie de la sûreté de l'État et à la défense des droits fondamentaux des citoyens, est garanti.

81 Ordre des barreaux francophones et germanophone e.a. (EU:C:2020:7, points 100 à 107).

82 Étant entendu que les conditions mentionnées au point 122 de l'arrêt Tele2 Sverige et Watson sont respectées : la Cour y a rappelé que l'article 15, paragraphe 1, de la directive 2002/58 ne permet pas de déroger à l'article 4, paragraphes 1 et 1 bis, de cette directive, qui exige que les fournisseurs prennent des mesures permettant d'assurer la protection des données conservées contre les risques d'abus et contre l'accès illicite. À cet égard, la Cour a jugé que, « [c]ompte tenu de la quantité de données conservées, du caractère sensible de ces données ainsi que du risque d'accès illicite à celles-ci, les fournisseurs de services de communication électronique doivent, aux fins d'assurer la pleine intégrité et la confidentialité desdites données, garantir un niveau particulièrement élevé de protection et de sécurité par des mesures techniques et organisationnelles appropriées. En particulier, la réglementation nationale doit prévoir la conservation sur le territoire de l'Union ainsi que la destruction irrémédiable des données au terme de la durée de conservation de celles-ci ».

83 Ordre des barreaux francophones et germanophone e.a. (EU:C:2020:7, points 52 à 60).

84 Arrêt Tele2 Sverige et Watson, point 118.

85 Arrêt Tele2 Sverige et Watson, point 119.

86 Arrêt Tele2 Sverige et Watson, point 120.

4) L'obligation de conservation des données permettant d'identifier les auteurs de contenu, à la lumière de la directive 2000/31 (deuxième question préjudicielle dans l'affaire C-512/18)

140. La juridiction de renvoi mentionne la directive 2000/31 en tant que point de référence aux fins de déterminer s'il est possible d'obliger certaines personnes [87] et les opérateurs offrant des services de communication au public à 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 ».

141. Je partage l'avis de la Commission selon lequel il serait inapproprié d'examiner la compatibilité d'une telle obligation avec la directive 2000/31 [88], dès lors que l'article 1er, 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 », réglementations qui correspondent désormais au règlement 2006/679 et à la directive 2002/58 [89], dont respectivement l'article 23, paragraphe 1, et l'article 15, paragraphe 1, doivent être interprétés, selon moi, dans les termes précédemment exposés.

2. Sur l'obligation de recueillir en temps réel des données relatives au trafic et des données de localisation (deuxième question préjudicielle dans l'affaire C-511/18)

142. Pour la juridiction de renvoi, l'article L. 851-2 du code de la sécurité intérieure autorise, pour les seuls besoins de la prévention du terrorisme, le recueil, en temps réel, d'informations relatives à des personnes préalablement identifiées comme étant susceptibles d'être en lien avec une menace terroriste. De même, l'article L. 851-4 de ce code autorise la transmission en temps réel, par les opérateurs, des données techniques relatives à la localisation des équipements terminaux.

143. Selon la juridiction de renvoi, ces techniques ne font pas peser sur les fournisseurs une exigence de conservation supplémentaire par rapport à ce qui est nécessaire pour la facturation et la commercialisation de leurs services.

144. En outre, conformément à l'article L. 851-3 du code de la sécurité intérieure, les opérateurs de communications électroniques et les prestataires techniques peuvent se voir imposer « la mise en œuvre sur leurs réseaux de traitements automatisées destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste ». Cette technique n'implique pas de conservation généralisée et indifférenciée de données et vise à recueillir, pendant une durée limitée, les données de connexion qui pourraient présenter un lien avec une infraction à caractère terroriste.

145. Selon moi, les conditions requises pour l'accès aux données à caractère personnel conservées doivent également s'appliquer à l'accès en temps réel aux données produites lors des communications électroniques. Je renvoie donc à ce qui a été dit à ce sujet. Il est dénué d'importance qu'il s'agisse de données conservées ou obtenues instantanément, puisque, dans les deux cas, il est pris connaissance de données à caractère personnel, qu'elles soient passées ou présentes.

87 Celles qui « assurent [...] 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 ».

88 Cette directive est mentionnée par la juridiction de renvoi, en termes généraux et sans en préciser aucune disposition, dans la deuxième question de l'affaire C-512/18.

89 Points 112 et 113 des observations écrites de la Commission.

146. En particulier, si l'accès en temps réel résulte de connexions détectées au moyen d'un traitement automatisé tel que ceux visés à l'article L. 851-3 du code de la sécurité intérieure, les modèles et critères préétablis pour un tel traitement doivent être spécifiques, fiables et non discriminatoires, afin de faciliter l'identification d'individus sur lesquels pèse un soupçon raisonnable de participation à des activités terroristes [90].

3. Sur l'obligation d'informer les personnes concernées (troisième question dans l'affaire C-511/18)

147. La Cour a affirmé que les autorités auxquelles l'accès aux données est accordé doivent en informer les personnes concernées, à condition que cela ne compromette pas les enquêtes en cours. La raison de cette obligation est que cette information est nécessaire pour que ces personnes puissent exercer leur droit de recours, expressément prévu à l'article 15, paragraphe 2, de la directive 2002/58, en cas de violation de leurs droits [91].

148. Le Conseil d'État souhaite savoir, par sa troisième question dans l'affaire C-511/18, si cette exigence d'information est en tout état de cause impérative ou si elle peut être écartée lorsque d'autres garanties, telles que celles qu'il décrit dans sa décision de renvoi, ont été prévues.

149. Selon l'exposé de la juridiction de renvoi [92], ces garanties se traduisent par la possibilité, pour ceux qui souhaitent vérifier si une technique d'information a été mise en œuvre irrégulièrement, de s'adresser au Conseil d'État lui-même. Ce dernier pourrait, le cas échéant, annuler l'autorisation de la mesure et ordonner la destruction de ce qui a été recueilli, dans le cadre d'une procédure ne prévoyant pas le principe du contradictoire habituel dans les procédures juridictionnelles.

150. La juridiction de renvoi considère que cette réglementation ne porte pas atteinte au droit à un recours effectif. Je crois que l'on pourrait admettre qu'il en va ainsi, en théorie, pour ceux qui décident de vérifier s'ils font l'objet d'une opération de renseignement. En revanche, ce droit n'est pas respecté si ceux qui font ou ont fait l'objet d'une telle opération ne sont pas avertis de cette circonstance et ne peuvent donc pas même se demander si leurs droits ont été violés ou non.

151. Les garanties juridictionnelles mentionnées par la juridiction de renvoi semblent dépendre de l'initiative de celui qui pense faire l'objet d'une collecte d'informations le concernant. Toutefois, l'accès à la justice aux fins de la défense de ses droits doit être effectif pour tous, ce qui implique que celui qui a fait l'objet d'un traitement de ses données à caractère personnel doit avoir la possibilité de contester judiciairement la légalité de ce traitement et doit donc avoir été informé de l'existence de ce dernier.

152. L'action en justice peut certes, ainsi qu'il ressort des informations fournies, être déclenchée d'office ou en vertu d'une plainte administrative ; néanmoins, la personne concernée doit en tout état de cause avoir la possibilité de l'engager elle-même, ce pour quoi il est nécessaire qu'elle soit informée que ses données à caractère personnel ont fait l'objet d'un traitement. La défense de ses droits ne saurait dépendre du fait qu'elle ait pris connaissance de ce traitement par des tiers ou par ses propres moyens.

153. Par conséquent, pour autant que le cours des enquêtes au titre desquelles l'accès aux données conservées a été accordé ne soit pas compromis, la personne concernée doit être informée de cet accès.

90 Arrêt Digital Rights, point 59.

91 Arrêt Tele2 Sverige et Watson, point 121.

92 Points 8 à 11 de la décision de renvoi.

154. Une chose distincte est que, alors que l'action en justice a été engagée par la personne concernée après qu'elle a été informée de l'accès à ses données, la procédure juridictionnelle consécutive respecte les exigences de confidentialité et de réserve inhérentes au contrôle de l'action des pouvoirs publics dans des domaines sensibles tels que celui de la sécurité et de la défense de l'État. Cette question est toutefois étrangère aux présentes demandes de décision préjudicielle, de sorte qu'il n'y a pas lieu, selon moi, que la Cour se prononce à cet égard.

V. Conclusion

155. Eu égard à ce qui précède, je propose à la Cour de répondre au Conseil d'État (France) dans les termes suivants :

L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), lu en combinaison avec les articles 7, 8, 11 et 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens que :

1) il s'oppose à une réglementation nationale qui, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, et en particulier par le risque terroriste, impose aux opérateurs et aux prestataires de services de communications électroniques de conserver, de manière générale et indifférenciée, les données relatives au trafic et les données de localisation de tous les abonnés ainsi que les données permettant d'identifier les créateurs de contenus offerts par les fournisseurs de ces services ;

2) il s'oppose à une réglementation nationale qui n'instaure pas l'obligation d'informer les personnes concernées du traitement de leurs données à caractère personnel effectué par les autorités compétentes pour autant que cette communication ne compromette pas l'action de ces autorités ;

3) il ne s'oppose pas à une réglementation nationale qui permet de recueillir en temps réel les données relatives au trafic et les données de localisation de personnes spécifiques, pour autant que ces actions soient menées conformément aux procédures prévues pour l'accès aux données à caractère personnel légalement conservées et avec les mêmes garanties.