Recueil de la jurisprudence

ARRÊT DE LA COUR (grande chambre)

6 octobre 2020*

[Texte rectifié par ordonnance du 16 novembre 2020]

Table des matières

* Langue de procédure : le français.

« Renvoi préjudiciel – Traitement des données à caractère personnel dans le secteur des communications électroniques – Fournisseurs de services de communications électroniques – Fournisseurs de services d'hébergement et fournisseurs d'accès à Internet – Conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation – Analyse automatisée des données – Accès en temps réel aux données – Sauvegarde de la sécurité nationale et lutte contre le terrorisme – Lutte contre la criminalité – Directive 2002/58/CE – Champ d'application – Article 1er, paragraphe 3, et article 3 – Confidentialité des communications électroniques – Protection – Article 5

et article 15, paragraphe 1 – Directive 2000/31/CE – Champ d'application – Charte des droits fondamentaux de l'Union européenne – Articles 4, 6 à 8 et 11 et article 52, paragraphe 1 – Article 4, paragraphe 2, TUE »

Dans les affaires jointes C-511/18, C-512/18 et C-520/18,

ayant pour objet des demandes de décision préjudicielle au titre de l'article 267 TFUE, introduites par le Conseil d'État (France), par décisions du 26 juillet 2018, parvenues à la Cour le 3 août 2018 (C-511/18 et C-512/18), et par la Cour constitutionnelle (Belgique), par décision du 19 juillet 2018, parvenue à la Cour le 2 août 2018 (C-520/18), dans les procédures

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), en présence de :

Privacy International (C-512/18),

Center for Democracy and Technology (C-512/18),

et

Ordre des barreaux francophones et germanophone,

Académie Fiscale ASBL,

UA,

Liga voor Mensenrechten ASBL,

Ligue des Droits de l'Homme ASBL,

VZ,

WY,

XX

contre

Conseil des ministres,

en présence de :

Child Focus (C-520/18),

LA COUR (grande chambre),

composée de M. K. Lenaerts, président, M^me^ R. Silva de Lapuerta, vice-présidente, MM. J.-C. Bonichot, A. Arabadjiev, M^me^ A. Prechal, MM. M. Safjan, P. G. Xuereb et M^me^ L. S. Rossi, présidents de chambre, MM. J. Malenovský, L. Bay Larsen, T. von Danwitz (rapporteur), M^mes^ C. Toader, K. Jürimäe, MM. C. Lycourgos et N. Piçarra, juges,

avocat général : M. M. Campos Sánchez-Bordona,

greffier : M^me^ C. Strömholm, administratrice,

vu la procédure écrite et à la suite de l'audience des 9 et 10 septembre 2019,

considérant les observations présentées :

– pour la Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net et le Center for Democracy and Technology, par M^e^ A. Fitzjean Ò Cobhthaigh, avocat,

– pour French Data Network, par M^e^ Y. Padova, avocat,

– pour Privacy International, M^e^ H. Roy, avocat,

– pour l'Ordre des barreaux francophones et germanophone, par M^es^ E. Kiehl, P. Limbrée, E. Lemmens, A. Cassart et J.-F. Henrotte, avocats,

– pour l'Académie Fiscale ASBL et UA, par M. J.-P. Riquet,

– pour la Liga voor Mensenrechten ASBL, par M^e^ J. Vander Velpen, avocat,

– pour la Ligue des Droits de l'Homme ASBL, par M^es^ R. Jespers et J. Fermon, avocats,

– pour VZ, WY et XX, par M^e^ D. Pattyn, avocat,

– pour Child Focus, par M^es^ N. Buisseret, K. De Meester et J. Van Cauter, avocats,

– pour le gouvernement français, initialement par MM. D. Dubois, F. Alabrune et D. Colas ainsi que par M^mes^ E. de Moustier et A.-L. Desjonquères, puis par MM. D. Dubois et F. Alabrune ainsi que par M^mes^ E. de Moustier et A.-L. Desjonquères, en qualité d'agents,

– pour le gouvernement belge, par MM. J.-C. Halleux et P. Cottin ainsi que par M^me^ C. Pochet, en qualité d'agents, assistés de M^es^ J. Vanpraet, Y. Peeters, S. Depré et E. de Lophem, avocats,

– pour le gouvernement tchèque, par MM. M. Smolek, J. Vláčil et O. Serdula, en qualité d'agents,

– pour le gouvernement danois, initialement par M. J. Nymann-Lindegren ainsi que par M^mes^ M. Wolff et P. Ngo, puis par M. J. Nymann-Lindegren et M^me^ M. Wolff, en qualité d'agents,

– pour le gouvernement allemand, initialement par MM. J. Möller, M. Hellmann, E. Lankenau, R. Kanitz et T. Henze, puis par MM. J. Möller, M. Hellmann, E. Lankenau et R. Kanitz, en qualité d'agents,

– pour le gouvernement estonien, par M^mes^ N. Grünberg et A. Kalbus, en qualité d'agents,

– pour le gouvernement irlandais, par M. A. Joyce ainsi que par M^mes^ M. Browne et G. Hodge, en qualité d'agents, assistés de M. D. Fennelly, BL,

– pour le gouvernement espagnol, initialement par MM. L. Aguilera Ruiz et A. Rubio González, puis par M. L. Aguilera Ruiz, en qualité d'agent,

– pour le gouvernement chypriote, par M^me^ E. Neofytou, en qualité d'agent,

– pour le gouvernement letton, par M^me^ V. Soņeca, en qualité d'agent,

– pour le gouvernement hongrois, initialement par M. M. Z. Fehér et M^me^ Z. Wagner, puis par M. M. Z. Fehér, en qualité d'agent,

– pour le gouvernement néerlandais, par M^mes^ M. K. Bulterman et M. A. M. de Ree, en qualité d'agents,

– pour le gouvernement polonais, par M. B. Majczyna ainsi que par M^mes^ J. Sawicka et M. Pawlicka, en qualité d'agents,

– pour le gouvernement suédois, initialement par M^mes^ H. Shev, H. Eklinder, C. Meyer-Seitz, et A. Falk, puis par M^mes^ H. Shev, H. Eklinder, C. Meyer-Seitz et J. Lundberg, en qualité d'agents,

– pour le gouvernement du Royaume-Uni, par M. S. Brandon, en qualité d'agent, assisté de M. G. Facenna, QC, et de M. C. Knight, barrister,

– [tiret supprimé par ordonnance du 16 novembre 2020],

– pour la Commission européenne, initialement par MM. H. Kranenborg et M. Wasmeier ainsi que par M^me^ P. Costa de Oliveira, puis par MM. H. Kranenborg et M. Wasmeier, en qualité d'agents,

– pour le Contrôleur européen de la protection des données, par M T. Zerdick et M^me^ A. Buchta, en qualité d'agents,

ayant entendu l'avocat général en ses conclusions à l'audience du 15 janvier 2020,

rend le présent

Arrêt

1 Les demandes de décision préjudicielle portent sur l'interprétation, d'une part, de l'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) (JO 2002, L 201, p. 37), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009 (JO 2009, L 337, p. 11) (ci-après la directive 2002/58), et, d'autre part, des articles 12 à 15 de la directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique ») (JO 2000, L 178, p. 1), lus à la lumière des articles 4, 6 à 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne (ci-après la « Charte ») et de l'article 4, paragraphe 2, TUE.

2 La demande dans l'affaire C-511/18 a été présentée dans le cadre de litiges opposant la Quadrature du Net, French Data Network, la Fédération des fournisseurs d'accès à Internet associatifs et Igwan.net au Premier ministre (France), au Garde des Sceaux, ministre de la Justice (France), au ministre de l'Intérieur (France) et au ministre des Armées (France) au sujet de la légalité du décret nº 2015-1185, du 28 septembre 2015, portant désignation des services spécialisés de renseignement (JORF du 29 septembre 2015, texte 1 sur 97, ci-après le « décret nº 2015-1185 »), du 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 (JORF du 2 octobre 2015, texte 7 sur 108, ci-après le « décret nº 2015-1211 »), du 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, pris en application de l'article L. 811-4 du code de la sécurité intérieure (JORF du 12 décembre 2015, texte 28 sur 127, ci-après le « décret nº 2015-1639 »), ainsi que du décret nº 2016-67, du 29 janvier 2016, relatif aux techniques de recueil de renseignement (JORF du 31 janvier 2016, texte 2 sur 113, ci-après le « décret nº 2016-67 »).

3 La demande dans l'affaire C-512/18 a été présentée dans le cadre de litiges opposant French Data Network, la Quadrature du Net et la Fédération des fournisseurs d'accès à Internet associatifs, au Premier ministre (France) et au Garde des Sceaux, ministre de la justice (France), au sujet de la légalité de l'article R. 10-13 du code des postes et des communications électroniques (ci-après le « CPCE ») et du 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 (JORF du 1er mars 2011, texte 32 sur 170, ci-après le « décret nº 2011-219 »).

4 La demande dans l'affaire C-520/18 a été présentée dans le cadre de litiges opposant l'Ordre des barreaux francophones et germanophone, l'Académie Fiscale ASBL, UA, la Liga voor Mensenrechten ASBL, la Ligue des Droits de l'Homme ASBL, VZ, WY et XX au Conseil des ministres (Belgique) au sujet de la légalité de la loi du 29 mai 2016 relative à la collecte et à la conservation des données dans le secteur des communications électroniques (*Moniteur belge* du 18 juillet 2016, p. 44717, ci-après la « loi du 29 mai 2016 »).

Le cadre juridique

Le droit de l'Union

La directive 95/46

5 La directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO 1995, L 281, p. 31), a été abrogée, avec effet au 25 mai 2018, par le règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46 (JO 2016, L 119, p. 1). L'article 3, paragraphe 2, de la directive 95/46 disposait :

« La 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, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, 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,

– effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques. »

6 L'article 22 de la directive 95/46, figurant au chapitre III de celle-ci, intitulé « Recours juridictionnels, responsabilité et sanctions », était libellé comme suit :

« Sans préjudice du recours administratif qui peut être organisé, notamment devant l'autorité de contrôle visée à l'article 28, antérieurement à la saisine de l'autorité judiciaire, les États membres prévoient que toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question. »

La directive 97/66

7 Aux termes de l'article 5 de la directive 97/66/CE du Parlement européen et du Conseil, du 15 décembre 1997, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications (JO 1997, L 24, p. 1), intitulé « Confidentialité des communications » :

« 1. Les États membres garantissent, au moyen de réglementations nationales, la confidentialité des communications effectuées au moyen d'un réseau public de télécommunications ou de services de télécommunications accessible au public. En particulier, ils interdisent à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées, conformément à l'article 14, paragraphe 1.

2. Le paragraphe 1 n'affecte pas l'enregistrement légalement autorisé de communications, dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale. »

La directive 2000/31

8 Les considérants 14 et 15 de la directive 2000/31 prévoient :

« (14) La protection des personnes physiques à l'égard du traitement des données à caractère personnel est uniquement régie par la directive [95/46] et par la directive [97/66], qui sont pleinement applicables aux services de la société de l'information. Ces directives établissent d'ores et déjà un cadre juridique communautaire dans le domaine des données à caractère personnel et, par conséquent, il n'est pas nécessaire de traiter cette question dans la présente directive afin d'assurer le bon fonctionnement du marché intérieur, et notamment la libre circulation des données à caractère personnel entre les États membres. La mise en œuvre et l'application de la présente directive devraient être conformes aux principes relatifs à la protection des données à caractère personnel, notamment pour ce qui est des communications commerciales non sollicitées et de la responsabilité des intermédiaires. La présente directive ne peut pas empêcher l'utilisation anonyme de réseaux ouverts tels qu'Internet.

(15) Le secret des communications est garanti par l'article 5 de la directive [97/66]. Conformément à cette directive, les États membres doivent interdire tout type d'interception illicite ou la surveillance de telles communications par d'autres que les expéditeurs et les récepteurs, sauf lorsque ces activités sont légalement autorisées. »

9 L'article 1er de la directive 2000/31 est libellé comme suit :

« 1. La présente directive a pour objectif de contribuer au bon fonctionnement du marché intérieur en assurant la libre circulation des services de la société de l'information entre les États membres.

2. La présente directive rapproche, dans la mesure nécessaire à la réalisation de l'objectif visé au paragraphe 1, certaines dispositions nationales applicables aux services de la société de l'information et qui concernent le marché intérieur, l'établissement des prestataires, les communications commerciales, les contrats par voie électronique, la responsabilité des intermédiaires, les codes de conduite, le règlement extrajudiciaire des litiges, les recours juridictionnels et la coopération entre États membres.

3. La présente directive complète le droit communautaire applicable aux services de la société de l'information sans préjudice du niveau de protection, notamment en matière de santé publique et des intérêts des consommateurs, établi par les instruments communautaires et la législation nationale les mettant en œuvre dans la mesure où cela ne restreint pas la libre prestation de services de la société de l'information.

[...]

5. La présente directive n'est pas applicable :

[...]

b) aux questions relatives aux services de la société de l'information couvertes par les directives [95/46] et [97/66] ;

[...] »

10 L'article 2 de la directive 2000/31 est libellé comme suit :

« Aux fins de la présente directive, on entend par :

a) "services de la société de l'information" : les services au sens de l'article 1er, paragraphe 2, de la directive 98/34/CE [du Parlement européen et du Conseil, du 22 juin 1998, prévoyant une procédure d'information dans le domaine des normes et réglementations techniques (JO 1998, L 204, p. 37)], telle que modifiée par la directive 98/48/CE [du Parlement européen et du Conseil, du 20 juillet 1998 (JO 1998, L 217, p. 18)] ;

[...] »

11 L'article 15 de la directive 2000/31 prévoit :

« 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. »

La directive 2002/21

12 Aux termes du considérant 10 de la directive 2002/21/CE du Parlement européen et du Conseil, du 7 mars 2002, relative à un cadre réglementaire commun pour les réseaux et services de communications électroniques (directive « cadre ») (JO 2002, L 108, p. 33) :

« La définition du "service de la société de l'information", qui figure à l'article 1er de la directive [98/34], telle que modifiée par la directive [98/48], se rapporte à une large gamme d'activités économiques se déroulant en ligne ; la plupart de ces activités ne sont pas couvertes par le champ d'application de la présente directive, car elles ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques ; les services de téléphonie vocale et de transmission de courrier électronique sont couverts par la présente directive. La même entreprise, par exemple un prestataire de services Internet, peut proposer à la fois un service de communications électroniques, tel que l'accès à Internet, et des services non couverts par la présente directive, tels que la fourniture de contenus sur la toile. »

13 L'article 2 de la directive 2002/21 prévoit :

« Aux fins de la présente directive, on entend par :

[...]

c) "service de communications électroniques" : le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion, mais qui exclut les services consistant à fournir des contenus à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ces contenus ; il ne comprend pas les services de la société de l'information tels que définis à l'article 1er de la directive [98/34], qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques ;

[...] »

La directive 2002/58

14 Les considérants 2, 6, 7, 11, 22, 26 et 30 de la directive 2002/58 énoncent :

« (2) La présente directive vise à respecter les droits fondamentaux et observe les principes reconnus notamment par la [Charte]. En particulier, elle vise à garantir le plein respect des droits exposés aux articles 7 et 8 de cette charte.

[...]

(6) L'Internet bouleverse les structures commerciales traditionnelles en offrant une infrastructure mondiale commune pour la fourniture de toute une série de services de communications électroniques. Les services de communications électroniques accessibles au public sur l'Internet ouvrent de nouvelles possibilités aux utilisateurs, mais présentent aussi de nouveaux dangers pour leurs données à caractère personnel et leur vie privée.

(7) Dans le cas des réseaux publics de communications, il convient d'adopter des dispositions législatives, réglementaires et techniques spécifiques afin de protéger les droits et les libertés fondamentaux des personnes physiques et les intérêts légitimes des personnes morales, notamment eu égard à la capacité accrue de stockage et de traitement automatisés de données relatives aux abonnés et aux utilisateurs.

[...]

(11) À l'instar de la directive [95/46], 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]. Elle 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 sécurité publique, de la défense, de la sûreté de l'État (y compris la prospérité économique de l'État lorsqu'il s'agit d'activités liées à la sûreté de l'État) et de l'application du droit pénal. Par conséquent, la présente directive ne porte pas atteinte à la faculté des États membres de procéder aux interceptions légales des communications électroniques ou d'arrêter d'autres mesures si cela s'avère nécessaire pour atteindre l'un quelconque des buts précités, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, [signée à Rome le 4 novembre 1050,] telle qu'interprétée par la Cour européenne des droits de l'homme dans ses arrêts. Lesdites mesures doivent être appropriées, rigoureusement proportionnées au but poursuivi et nécessaires dans une société démocratique. Elles devraient également être subordonnées à des garanties appropriées, dans le respect de la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales.

[...]

(22) L'interdiction du stockage des communications et des données relatives au trafic y afférentes par des personnes autres que les utilisateurs ou sans le consentement de ceux-ci ne vise pas à interdire tout stockage automatique, intermédiaire et transitoire de ces informations si ce stockage a lieu dans le seul but d'effectuer la transmission dans le réseau de communications électroniques, pour autant que les informations ne soient pas stockées pour une durée plus longue que le temps nécessaire à la transmission et à la gestion du trafic et qu'au cours de la période de stockage la confidentialité des informations reste garantie. [...]

[...]

(26) Les données relatives aux abonnés qui sont traitées dans des réseaux de communications électroniques pour établir des connexions et transmettre des informations contiennent des informations sur la vie privée des personnes physiques et touchent au droit au secret de leur correspondance ainsi qu'aux intérêts légitimes des personnes morales. Ces données ne peuvent être stockées que dans la mesure où cela est nécessaire à la fourniture du service, aux fins de la facturation et des paiements pour interconnexion, et ce, pour une durée limitée. Tout autre traitement de ces données [...] ne peut être autorisé que si l'abonné a donné son accord sur la base d'informations précises et complètes fournies par le fournisseur du service de communications électroniques accessible au public sur la nature des autres traitements qu'il envisage d'effectuer, ainsi que sur le droit de l'abonné de ne pas donner son consentement à ces traitements ou de retirer son consentement. Il convient également d'effacer ou de rendre anonymes les données relatives au trafic utilisées pour la commercialisation de services de communications [...]

[...]

(30) Les systèmes mis au point pour la fourniture de réseaux et de services de communications électroniques devraient être conçus de manière à limiter au strict minimum la quantité de données personnelles nécessaires. [...] »

15 L'article 1er de la directive 2002/58, intitulé « Champ d'application et objectif », dispose :

« 1. La présente directive prévoit l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques, ainsi que la libre circulation de ces données et des équipements et services de communications électroniques dans [l'Union européenne].

2. Les dispositions de la présente directive précisent et complètent la directive [95/46] aux fins énoncées au paragraphe 1. En outre, elles prévoient la protection des intérêts légitimes des abonnés qui sont des personnes morales.

3. La présente directive ne s'applique pas aux activités qui ne relèvent pas du [TFUE], telles que celles visées dans les titres V et VI du 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. »

16 Selon l'article 2 de la directive 2002/58, intitulé « Définitions » :

« Sauf disposition contraire, les définitions figurant dans la directive [95/46] et dans la directive [2002/21] s'appliquent aux fins de la présente directive.

Les définitions suivantes sont aussi applicables :

a) "utilisateur" : toute personne physique utilisant un service de communications électroniques accessible au public à des fins privées ou professionnelles sans être nécessairement abonnée à ce service ;

b) "données relatives au trafic" : toutes les données traitées en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de sa facturation ;

c) "données de localisation" : toutes les données traitées dans un réseau de communications électroniques ou par un service de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur d'un service de communications électroniques accessible au public ;

d) "communication" : toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit ;

[...] »

17 L'article 3 de la directive 2002/58, intitulé « Services concernés », prévoit :

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

18 Aux termes de l'article 5 de la directive 2002/58, intitulé « Confidentialité des communications » :

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

[...]

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

19 L'article 6 de la directive 2002/58, intitulé « Données relatives au trafic », dispose :

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

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

3. Afin de commercialiser des services de communications électroniques ou de fournir des services à valeur ajoutée, le fournisseur d'un service de communications électroniques accessible au public peut traiter les données visées au paragraphe 1 dans la mesure et pour la durée nécessaires à la fourniture ou à la commercialisation de ces services, pour autant que l'abonné ou l'utilisateur que concernent ces données ait donné son consentement préalable. Les utilisateurs ou abonnés ont la possibilité de retirer à tout moment leur consentement pour le traitement des données relatives au trafic.

[...]

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

20 L'article 9 de cette directive, intitulé « Données de localisation autres que les données relatives au trafic », prévoit, à son paragraphe 1 :

« Lorsque des données de localisation, autres que des données relatives au trafic, concernant des utilisateurs ou abonnés de réseaux publics de communications ou de services de communications électroniques accessibles au public ou des abonnés à ces réseaux ou services, peuvent être traitées, elles ne le seront qu'après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés, dans la mesure et pour la durée nécessaires à la fourniture d'un service à valeur ajoutée. Le fournisseur du service doit informer les utilisateurs ou les abonnés, avant d'obtenir leur consentement, du type de données de localisation autres que les données relatives au trafic qui sera traité, des objectifs et de la durée de ce traitement, et du fait que les données seront ou non transmises à un tiers en vue de la fourniture du service à valeur ajoutée. [...] »

21 L'article 15 de ladite directive, intitulé « Application de certaines dispositions de la directive [95/46] », énonce :

« 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]. 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 [de l'Union], y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

[...]

2. Les dispositions du chapitre III de la directive [95/46] relatif aux recours juridictionnels, à la responsabilité et aux sanctions sont applicables aux dispositions nationales adoptées en application de la présente directive ainsi qu'aux droits individuels résultant de la présente directive.

[...] »

Le règlement 2016/679

22 Le considérant 10 du règlement 2016/679 énonce :

« Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union, le niveau de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données devrait être

équivalent dans tous les États membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union. [...] »

23 L'article 2 de ce règlement dispose :

« 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 ;

[...]

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.

[...]

4. Le présent règlement s'applique sans préjudice de la directive [2000/31], et notamment de ses articles 12 à 15 relatifs à la responsabilité des prestataires de services intermédiaires. »

24 L'article 4 dudit règlement prévoit :

« Aux fins du présent règlement, on entend par :

1) "données à caractère personnel", toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée "personne concernée") ; est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

2) "traitement", toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ;

[...] »

25 L'article 5 du règlement 2016/679 dispose :

« 1. Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence) ;

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités) ;

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données) ;

d) exactes et, si nécessaire, tenues à jour ; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude) ;

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation) ;

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) ;

[...] »

26 L'article 6 de ce règlement est libellé comme suit :

« 1. Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :

[...]

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;

[...]

3. Le fondement du traitement visé au paragraphe 1, [sous] c) et e), est défini par :

a) le droit de l'Union ; ou

b) le droit de l'État membre auquel le responsable du traitement est soumis.

Les finalités du traitement sont définies dans cette base juridique [...] Cette base juridique peut contenir des dispositions spécifiques pour adapter l'application des règles du présent règlement, entre autres : les conditions générales régissant la licéité du traitement par le responsable du traitement ; les types de données qui font l'objet du traitement ; les personnes concernées ; les entités auxquelles les données à caractère personnel peuvent être communiquées et les finalités pour lesquelles elles peuvent l'être ; la limitation des finalités ; les durées de conservation ; et les opérations et procédures de traitement, y compris les mesures visant à garantir un traitement licite et loyal, telles que celles prévues dans d'autres situations particulières de traitement comme le prévoit le chapitre IX. Le droit de l'Union ou le droit des États membres répond à un objectif d'intérêt public et est proportionné à l'objectif légitime poursuivi.

[...] »

27 L'article 23 dudit règlement prévoit :

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

a) la sécurité nationale ;

b) la défense nationale ;

c) la sécurité publique ;

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

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

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

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

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

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

j) l'exécution des demandes de droit civil.

2. En particulier, toute mesure législative visée au paragraphe 1 contient des dispositions spécifiques relatives, au moins, le cas échéant :

a) aux finalités du traitement ou des catégories de traitement ;

b) aux catégories de données à caractère personnel ;

c) à l'étendue des limitations introduites ;

d) aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites ;

e) à la détermination du responsable du traitement ou des catégories de responsables du traitement ;

f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement ;

g) aux risques pour les droits et libertés des personnes concernées ; et

h) au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation. »

28 Selon l'article 79, paragraphe 1, dudit règlement :

« Sans préjudice de tout recours administratif ou extrajudiciaire qui lui est ouvert, y compris le droit d'introduire une réclamation auprès d'une autorité de contrôle au titre de l'article 77, chaque personne concernée a droit à un recours juridictionnel effectif si elle considère que les droits que lui confère le présent règlement ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation du présent règlement. »

29 Aux termes de l'article 94 du règlement 2016/679 :

« 1. La directive [95/46] est abrogée avec effet au 25 mai 2018.

2. Les références faites à la directive abrogée s'entendent comme faites au présent règlement. Les références faites au groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive [95/46] s'entendent comme faites au comité européen de la protection des données institué par le présent règlement. »

30 L'article 95 de ce règlement dispose :

« 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]. »

Le droit français

Le code de la sécurité intérieure

31 Le livre VIII de la partie législative du code de la sécurité intérieure (ci-après le « CSI »), prévoit, à ses articles L. 801-1 à L. 898-1, des règles relatives au renseignement.

32 L. 811-3 du CSI dispose :

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

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

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

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

4° La prévention du terrorisme ;

5° La prévention :
a) Des atteintes à la forme républicaine des institutions ;
b) Des actions tendant au maintien ou à la reconstitution de groupements dissous en application de l'article L. 212-1 ;
c) Des violences collectives de nature à porter gravement atteinte à la paix publique ;

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

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

33 L'article L. 811-4 du CSI énonce :

« Un décret en Conseil d'État, pris après avis de la Commission nationale de contrôle des techniques de renseignement, désigne les services, autres que les services spécialisés de renseignement, relevant des ministres de la défense, de l'intérieur et de la justice ainsi que des ministres chargés de l'économie, du budget ou des douanes, qui peuvent être autorisés à recourir aux techniques mentionnées au titre V du présent livre dans les conditions prévues au même livre. Il précise, pour chaque service, les finalités mentionnées à l'article L. 811-3 et les techniques qui peuvent donner lieu à autorisation. »

34 L'article L. 821-1, premier alinéa, du CSI précise ce qui suit :

« La mise en œuvre sur le territoire national des techniques de recueil de renseignement mentionnées aux chapitres I[er] à IV du titre V du présent livre est soumise à autorisation préalable du Premier ministre, délivrée après avis de la Commission nationale de contrôle des techniques de renseignement. »

35 L'article L. 821-2 du CSI prévoit :

« L'autorisation mentionnée à l'article L. 821-1 est délivrée sur demande écrite et motivée du ministre de la défense, du ministre de l'intérieur, du ministre de la justice ou des ministres chargés de l'économie, du budget ou des douanes. Chaque ministre ne peut déléguer cette attribution individuellement qu'à des collaborateurs directs habilités au secret de la défense nationale.

La demande précise :

1° La ou les techniques à mettre en œuvre ;

2° Le service pour lequel elle est présentée ;

3° La ou les finalités poursuivies ;

4° Le ou les motifs des mesures ;

5° La durée de validité de l'autorisation ;

6° La ou les personnes, le ou les lieux ou véhicules concernés.

Pour l'application du 6°, les personnes dont l'identité n'est pas connue peuvent être désignées par leurs identifiants ou leur qualité et les lieux ou véhicules peuvent être désignés par référence aux personnes faisant l'objet de la demande.

[…] »

36 Aux termes de l'article L. 821-3, premier alinéa, du CSI :

« La demande est communiquée au président ou, à défaut, à l'un des membres de la Commission nationale de contrôle des techniques de renseignement parmi ceux mentionnés aux 2° et 3° de l'article L. 831-1, qui rend un avis au Premier ministre dans un délai de vingt-quatre heures. Si la demande est examinée par la formation restreinte ou par la formation plénière de la commission, le Premier ministre en est informé sans délai et l'avis est rendu dans un délai de soixante-douze heures. »

37 L'article L. 821-4 du CSI dispose :

« L'autorisation de mise en œuvre des techniques mentionnées aux chapitres I[er] à IV du titre V du présent livre est délivrée par le Premier ministre pour une durée maximale de quatre mois. […] L'autorisation comporte les motivations et mentions prévues aux 1° à 6° de l'article L. 821-2. Toute autorisation est renouvelable dans les mêmes conditions que celles prévues au présent chapitre.

Lorsque l'autorisation est délivrée après un avis défavorable de la Commission nationale de contrôle des techniques de renseignement, elle indique les motifs pour lesquels cet avis n'a pas été suivi.

[...] »

38 L'article L. 833-4 du CSI figurant dans le chapitre III de ce titre dispose :

« De sa propre initiative ou lorsqu'elle est saisie d'une réclamation de toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard, la commission procède au contrôle de la ou des techniques invoquées en vue de vérifier qu'elles ont été ou sont mises en œuvre dans le respect du présent livre. Elle notifie à l'auteur de la réclamation qu'il a été procédé aux vérifications nécessaires, sans confirmer ni infirmer leur mise en œuvre. »

39 L'article L. 841-1, premier et deuxième alinéas, du CSI est libellé comme suit :

« Sous réserve des dispositions particulières prévues à l'article L. 854-9 du présent code, le Conseil d'État est compétent pour connaître, dans les conditions prévues au chapitre III bis du titre VII du livre VII du code de justice administrative, des requêtes concernant la mise en œuvre des techniques de renseignement mentionnées au titre V du présent livre.

Il peut être saisi par :

1° Toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard et justifiant de la mise en œuvre préalable de la procédure prévue à l'article L. 833-4 ;

2° La Commission nationale de contrôle des techniques de renseignement, dans les conditions prévues à l'article L. 833-8. »

40 Le titre V du livre VIII de la partie législative du CSI, relatif aux « techniques de recueil de renseignement soumises à autorisation », comporte, notamment, un chapitre Ier, intitulé « Des accès administratifs aux données de connexion », qui contient les articles L. 851-1 à L. 851-7 du CSI.

41 L'article L. 851-1 du CSI dispose :

« Dans les conditions prévues au chapitre Ier du titre II du présent livre, peut être autorisé le recueil, auprès des opérateurs de communications électroniques et des personnes mentionnées à l'article L. 34-1 du [CPCE] 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 [(JORF du 22 juin 2004, p. 11168)], 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 des numéros d'abonnement ou de connexion d'une personne désignée, à la localisation des équipements terminaux utilisés ainsi qu'aux communications d'un abonné portant sur la liste des numéros appelés et appelants, la durée et la date des communications.

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

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

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

42 L'article L. 851-2 du CSI énonce :

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

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

[...] »

43 L'article L. 851-3 du CSI prévoit :

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

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

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

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

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

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

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

[...] »

44 L'article L. 851-4 du CSI est libellé comme suit :

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

45 L'article R. 851-5 du CSI, qui figure dans la partie réglementaire de ce code, prévoit :

« I. – Les informations ou documents mentionnés à l'article L. 851-1 sont, à l'exclusion du contenu des correspondances échangées ou des informations consultées :

1° Ceux énumérés aux articles R. 10-13 et R. 10-14 du [CPCE] et à l'article 1er du décret [n° 2011-219] ;

2° Les données techniques autres que celles mentionnées au 1° :

a) Permettant de localiser les équipements terminaux ;

b) Relatives à l'accès des équipements terminaux aux réseaux ou aux services de communication au public en ligne ;

c) Relatives à l'acheminement des communications électroniques par les réseaux ;

d) Relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne ;

e) Relatives aux caractéristiques des équipements terminaux et aux données de configuration de leurs logiciels.

II. – Seuls les informations et documents mentionnés au 1° du I peuvent être recueillis en application de l'article L. 851-1. Ce recueil a lieu en temps différé.

Les informations énumérées au 2° du I ne peuvent être recueillies qu'en application des articles L. 851-2 et L. 851-3 dans les conditions et limites prévues par ces articles et sous réserve de l'application de l'article R. 851-9. »

Le CPCE

46 L'article L. 34-1 du CPCE dispose :

« 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 de ces données s'effectuent dans le respect des dispositions de la loi nº 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. »

47 L'article R. 10-13 du CPCE est libellé comme suit :

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

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

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

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

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

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

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

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

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

48 L'article R. 10-14 du CPCE prévoit :

« I. – En application du IV de l'article L. 34-1 les opérateurs de communications électroniques sont autorisés à conserver pour les besoins de leurs opérations de facturation et de paiement les données à caractère technique permettant d'identifier l'utilisateur ainsi que celles mentionnées aux b, c et d du I de l'article R. 10-13.

II. – Pour les activités de téléphonie, les opérateurs peuvent conserver, outre les données mentionnées au I, les données à caractère technique relatives à la localisation de la communication, à l'identification du ou des destinataires de la communication et les données permettant d'établir la facturation.

III. – Les données mentionnées aux I et II du présent article ne peuvent être conservées que si elles sont nécessaires à la facturation et au paiement des services rendus. Leur conservation devra se limiter au temps strictement nécessaire à cette finalité sans excéder un an.

IV. – Pour la sécurité des réseaux et des installations, les opérateurs peuvent conserver pour une durée n'excédant pas trois mois :

a) Les données permettant d'identifier l'origine de la communication ;

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

c) Les données à caractère technique permettant d'identifier le ou les destinataires de la communication ;

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

La loi n° 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique

49 L'article 6 de la loi n° 2004-575, du 21 juin 2004, pour la confiance dans l'économie numérique (JORF du 22 juin 2004, p. 11168, ci-après la « LCEN ») prévoit :

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

[...]

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

[...]

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

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

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

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

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

[...] »

Le décret nº 2011-219

50 Le chapitre Ier du décret nº 2011-219, pris sur le fondement de l'article 6, II, dernier alinéa, de la LCEN, contient les articles 1 à 4 de ce décret.

51 L'article 1er du décret nº 2011-219 dispose :

« Les données mentionnées au II de l'article 6 de la [LCEN], que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes :

1° Pour les personnes mentionnées au 1 du I du même article et pour chaque connexion de leurs abonnés :

a) L'identifiant de la connexion ;

b) L'identifiant attribué par ces personnes à l'abonné ;

c) L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;

d) Les dates et heure de début et de fin de la connexion ;

e) Les caractéristiques de la ligne de l'abonné ;

2° Pour les personnes mentionnées au 2 du I du même article et pour chaque opération de création :

a) L'identifiant de la connexion à l'origine de la communication ;

b) L'identifiant attribué par le système d'information au contenu, objet de l'opération ;

c) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ;

d) La nature de l'opération ;

e) Les date et heure de l'opération ;

f) L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni ;

3° Pour les personnes mentionnées aux 1 et 2 du I du même article, les informations fournies lors de la souscription d'un contrat par un utilisateur ou lors de la création d'un compte :

a) Au moment de la création du compte, l'identifiant de cette connexion ;

b) Les nom et prénom ou la raison sociale ;

c) Les adresses postales associées ;

d) Les pseudonymes utilisés ;

e) Les adresses de courrier électronique ou de compte associées ;

f) Les numéros de téléphone ;

g) Le mot de passe ainsi que les données permettant de le vérifier ou de le modifier, dans leur dernière version mise à jour ;

4° Pour les personnes mentionnées aux 1 et 2 du I du même article, lorsque la souscription du contrat ou du compte est payante, les informations suivantes relatives au paiement, pour chaque opération de paiement :

a) Le type de paiement utilisé ;

b) La référence du paiement ;

c) Le montant ;

d) La date et l'heure de la transaction.

Les données mentionnées aux 3° et 4° ne doivent être conservées que dans la mesure où les personnes les collectent habituellement. »

52 L'article 2 de ce décret est libellé comme suit :

« La contribution à une création de contenu comprend les opérations portant sur :

a) Des créations initiales de contenus ;

b) Des modifications des contenus et de données liées aux contenus ;

c) Des suppressions de contenus. »

53 L'article 3 dudit décret prévoit :

« La durée de conservation des données mentionnées à l'article 1er est d'un an :

a) S'agissant des données mentionnées aux 1° et 2°, à compter du jour de la création des contenus, pour chaque opération contribuant à la création d'un contenu telle que définie à l'article 2 ;

b) S'agissant des données mentionnées au 3°, à compter du jour de la résiliation du contrat ou de la fermeture du compte ;

c) S'agissant des données mentionnées au 4°, à compter de la date d'émission de la facture ou de l'opération de paiement, pour chaque facture ou opération de paiement. »

Le droit belge

54 La loi du 29 mai 2016 a modifié, notamment, la loi du 13 juin 2005 relative aux communications électroniques (*Moniteur belge* du 20 juin 2005, p. 28070, ci-après la « loi du 13 juin 2005 »), le code d'instruction criminelle et la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (*Moniteur belge* du 18 décembre 1998, p. 40312, ci-après la « loi du 30 novembre 1998 »).

55 L'article 126 de la loi du 13 juin 2005, dans sa version issue de la loi du 29 mai 2016, dispose :

« § 1er. Sans préjudice de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, les fournisseurs au public de services de téléphonie, en ce compris par internet, d'accès à l'Internet, de courrier électronique par Internet, les opérateurs fournissant des réseaux publics de communications électroniques ainsi que les opérateurs fournissant un de ces services, conservent les données visées au paragraphe 3, qui sont générées ou traitées par eux dans le cadre de la fourniture des services de communications concernés.

Le présent article ne porte pas sur le contenu des communications.

L'obligation de conserver les données visées au paragraphe 3 s'applique également aux appels infructueux, pour autant que ces données soient, dans le cadre de la fourniture des services de communications concernés :

1° en ce qui concerne les données de la téléphonie, générées ou traitées par les opérateurs de services de communications électroniques accessibles au public ou d'un réseau public de communications électroniques, ou

2° en ce qui concerne les données de l'internet, journalisées par ces fournisseurs.

§ 2. Seules les autorités suivantes peuvent obtenir, sur simple demande, des fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, des données conservées en vertu du présent article, pour les finalités et selon les conditions énumérées ci-dessous :

1° les autorités judiciaires, en vue de la recherche, de l'instruction et de la poursuite d'infractions, pour l'exécution des mesures visées aux articles 46bis et 88bis du Code d'instruction criminelle et dans les conditions fixées par ces articles ;

2° les services de renseignement et de sécurité, afin d'accomplir des missions de renseignement en ayant recours aux méthodes de recueil de données visées aux articles 16/2, 18/7 et 18/8 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et dans les conditions fixées par cette loi ;

3° tout officier de police judiciaire de l'[Institut belge des services postaux et des télécommunications], en vue de la recherche, de l'instruction et de la poursuite d'infractions aux articles 114, 124 et au présent article ;

4° les services d'urgence offrant de l'aide sur place, lorsque, à la suite d'un appel d'urgence, ils n'obtiennent pas du fournisseur ou de l'opérateur concerné les données d'identification de l'appelant à l'aide de la base de données visée à l'article 107, § 2, alinéa 3, ou obtiennent des données incomplètes ou incorrectes. Seules les données d'identification de l'appelant peuvent être demandées et au plus tard dans les 24 heures de l'appel ;

5° l'officier de police judiciaire de la Cellule des personnes disparues de la Police Fédérale, dans le cadre de sa mission d'assistance à personne en danger, de recherche de personnes dont la disparition est inquiétante et lorsqu'il existe des présomptions ou indices sérieux que l'intégrité physique de la personne disparue se trouve en danger imminent. Seules les données visées au paragraphe 3, alinéas 1 et 2, relatives à la personne disparue et conservées au cours des 48 heures précédant la demande d'obtention des données peuvent être demandées à l'opérateur ou au fournisseur concerné par l'intermédiaire d'un service de police désigné par le Roi ;

6° le Service de médiation pour les télécommunications, en vue de l'identification de la personne ayant effectué une utilisation malveillante d'un réseau ou d'un service de communications électroniques, conformément aux conditions visées à l'article 43bis, § 3, 7°, de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Seules les données d'identification peuvent être demandées.

Les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, font en sorte que les données visées au paragraphe 3, soient accessibles de manière illimitée à partir de la Belgique et que ces données et toute autre information nécessaire concernant ces données puissent être transmises sans délai et aux seules autorités visées au présent paragraphe.

Sans préjudice d'autres dispositions légales, les fournisseurs et opérateurs visés au paragraphe 1er, alinéa 1er, ne peuvent utiliser les données conservées en vertu du paragraphe 3 pour d'autres finalités.

§ 3. Les données visant à identifier l'utilisateur ou l'abonné et les moyens de communication, à l'exclusion des données spécifiquement prévues aux alinéas 2 et 3, sont conservées pendant douze mois à compter de la date à partir de laquelle une communication est possible pour la dernière fois à l'aide du service utilisé.

Les données relatives à l'accès et la connexion de l'équipement terminal au réseau et au service et à la localisation de cet équipement, y compris le point de terminaison du réseau, sont conservées pendant douze mois à partir de la date de la communication.

Les données de communication, à l'exclusion du contenu, en ce compris leur origine et leur destination, sont conservées pendant douze mois à partir de la date de la communication.

Le Roi fixe, par arrêté délibéré en Conseil des ministres, sur proposition du ministre de la Justice et du ministre [compétent pour les matières relatives aux communications électroniques], et après avis de la Commission de la protection de la vie privée et de l'Institut, les données à conserver par type de catégories visées aux alinéas 1 à 3 ainsi que les exigences auxquelles ces données doivent répondre.

[...] »

Les litiges au principal et les questions préjudicielles

L'affaire C-511/18

56 Par des requêtes introduites les 30 novembre 2015 et 16 mars 2016, jointes dans la procédure au principal, la Quadrature du Net, French Data Network et la Fédération des fournisseurs d'accès à Internet associatifs ainsi que Igwan.net ont saisi le Conseil d'État (France) de recours tendant à l'annulation des décrets nos 2015-1185, 2015-1211, 2015-1639 et 2016-67, au motif, notamment, qu'ils méconnaîtraient la Constitution française, la convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales (ci-après la « CEDH ») ainsi que les directives 2000/31 et 2002/58, lues à la lumière des articles 7, 8 et 47 de la Charte.

57 S'agissant, en particulier, des moyens tirés de la méconnaissance de la directive 2000/31, la juridiction de renvoi relève que les dispositions de l'article L. 851-3 du CSI imposent aux opérateurs de communications électroniques et aux prestataires techniques « la mise en œuvre sur leurs réseaux de traitements automatisés destinés, en fonction de paramètres précisés dans l'autorisation, à détecter des connexions susceptibles de révéler une menace terroriste ». Cette technique viserait à recueillir uniquement pendant une durée limitée, parmi l'ensemble des données de connexion traitées par ces opérateurs et ces prestataires, celles de ces données qui pourraient présenter un lien avec une telle infraction grave. Dans ces conditions, lesdites dispositions, qui n'imposeraient pas une obligation générale de surveillance active, ne méconnaîtraient pas l'article 15 de la directive 2000/31.

58 En ce qui concerne les moyens tirés de la méconnaissance de la directive 2002/58, la juridiction de renvoi considère qu'il résulte notamment des dispositions de cette directive ainsi que de l'arrêt du 21 décembre 2016, Tele2 Sverige et Watson e.a. (C-203/15 et C-698/15, ci-après l'« arrêt Tele2 », EU:C:2016:970), que les dispositions nationales imposant des obligations aux fournisseurs de services de communications électroniques, telles que la conservation généralisée et indifférenciée des données de trafic et des données de localisation de leurs utilisateurs et de leurs abonnés, aux fins mentionnées à l'article 15, paragraphe 1, de ladite directive, parmi lesquelles figurent la sauvegarde de la sécurité nationale, de la défense et de la sécurité publique, relèvent du champ d'application de la même directive dans la mesure où ces réglementations régissent l'activité desdits fournisseurs. Il en irait de même des réglementations régissant l'accès des autorités nationales aux données ainsi que leur utilisation.

59 La juridiction de renvoi en déduit que relèvent du champ d'application de la directive 2002/58 tant l'obligation de conservation résultant de l'article L. 851-1 du CSI que les accès administratifs auxdites données, y compris ceux en temps réel, prévus aux articles L. 851-1, L. 851-2 et L. 851-4 dudit code. Il en va de même, selon cette juridiction, des dispositions de l'article L. 851-3 de ce même code qui, si elles ne font pas peser sur les opérateurs concernés une obligation générale de conservation, leur imposent cependant de mettre en œuvre sur leurs réseaux des traitements automatisés destinés à détecter des connexions susceptibles de révéler une menace terroriste.

60 En revanche, cette juridiction considère que ne relèvent pas du champ d'application de la directive 2002/58 les dispositions du CSI visées par les demandes d'annulation qui portent sur des 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. Ces dispositions ne sauraient donc être regardées comme mettant en œuvre le droit de l'Union, de telle sorte que les moyens tirés de la méconnaissance par celles-ci de la directive 2002/58 ne pourraient être utilement invoqués.

61 Ainsi, en vue de trancher les litiges portant sur la légalité des décrets n^{os} 2015-1185, 2015-1211, 2015-1639 et 2016-67 au regard de la directive 2002/58 en tant qu'ils ont été pris pour la mise en œuvre des articles L. 851-1 à L. 851-4 du CSI, se poseraient trois questions d'interprétation du droit de l'Union.

62 S'agissant de l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, la juridiction de renvoi s'interroge, en premier lieu, sur le point de savoir si une obligation de conservation généralisée et indifférenciée imposée aux fournisseurs de services de communications électroniques sur le fondement des articles L. 851-1 et R. 851-5 du CSI ne doit pas être regardée, notamment eu égard aux garanties et aux contrôles dont sont assortis les accès administratifs aux données de connexion et l'utilisation de celles-ci, comme une ingérence justifiée par le droit à la sûreté garanti à l'article 6 de la Charte et les exigences de la sécurité nationale, dont la responsabilité incombe aux seuls États membres en vertu de l'article 4 TUE.

63 En ce qui concerne, en deuxième lieu, les autres obligations susceptibles d'être imposées aux fournisseurs de services de communications électroniques, la juridiction de renvoi relève que les dispositions de l'article L. 851-2 du CSI autorisent, pour les seuls besoins de la prévention du terrorisme, le recueil des informations ou des documents prévus à l'article L. 851-1 de ce code, auprès des mêmes personnes. Ce recueil, qui ne concernerait qu'un ou plusieurs individus préalablement identifiés comme étant susceptibles d'être en lien avec une menace terroriste, s'effectuerait en temps réel. Il en irait de même des dispositions de l'article L. 851-4 dudit code autorisant la transmission en temps réel par les opérateurs des seules données techniques relatives à la localisation des équipements terminaux. Ces techniques régiraient pour des finalités et selon des modalités différentes des accès administratifs en temps réel aux données conservées au titre du CPCE et de la LCEN, sans pour autant faire peser sur les fournisseurs concernés une exigence de conservation supplémentaire par rapport à ce qui serait nécessaire à la facturation et à la fourniture de leurs services. De même, les dispositions de l'article L. 851-3 du CSI, qui prévoient une obligation pour les fournisseurs de services de mettre en œuvre sur leurs réseaux une analyse automatisée des connexions, n'impliqueraient pas davantage une conservation généralisée et indifférenciée.

64 Or, d'une part, la juridiction de renvoi considère que tant la conservation généralisée et indifférenciée que les accès en temps réel aux données de connexion présentent, dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, tenant en particulier au risque terroriste, une utilité opérationnelle sans équivalent. En effet, la conservation généralisée et indifférenciée permettrait aux services de renseignement d'accéder aux données relatives aux communications avant que soient identifiées les raisons de considérer que la personne concernée présente une menace pour la sécurité publique, la défense ou la sûreté de l'État. En outre, les accès en temps réel aux données de connexion permettraient de suivre, avec une forte réactivité, les comportements d'individus susceptibles de représenter une menace immédiate pour l'ordre public.

65 D'autre part, la technique prévue à l'article L. 851-3 du CSI permettrait de détecter, sur le fondement de critères précisément définis à cette fin, les individus dont les comportements sont susceptibles, compte tenu de leurs modes de communication, de révéler une menace terroriste.

66 En troisième lieu, s'agissant de l'accès des autorités compétentes aux données conservées, la juridiction de renvoi se demande si la directive 2002/58, lue à la lumière de la Charte, doit être interprétée en ce sens qu'elle subordonne dans tous les cas la régularité des procédures de recueil des données de connexion à une exigence d'information des personnes concernées lorsqu'une telle information n'est plus susceptible de compromettre les enquêtes menées par les autorités compétentes, ou si de telles procédures peuvent être regardées comme régulières compte tenu de l'ensemble des autres garanties procédurales prévues par le droit national lorsque que celles-ci assurent l'effectivité du droit au recours.

67 S'agissant de ces autres garanties procédurales, la juridiction de renvoi précise notamment que toute personne souhaitant vérifier qu'aucune technique de renseignement n'est irrégulièrement mise en œuvre à son égard peut saisir une formation spécialisée du Conseil d'État à laquelle il appartient de vérifier, au vu des éléments qui lui sont communiqués hors procédure contradictoire si le requérant a fait l'objet d'une technique et si celle-ci a été mise en œuvre en conformité avec le livre VIII du CSI. Les pouvoirs dont cette formation serait investie pour instruire les requêtes garantiraient l'effectivité du contrôle juridictionnel qu'elle exerce. Ainsi, elle serait compétente pour instruire les requêtes, relever d'office toutes les illégalités qu'elle constate et enjoindre à l'administration de prendre toutes mesures utiles afin de remédier aux illégalités constatées. En outre, il appartiendrait à la Commission nationale de contrôle des techniques de renseignement de vérifier que les techniques de recueil de renseignement sont mises en œuvre, sur le territoire national, conformément aux exigences découlant du CSI. Ainsi, la circonstance que les dispositions législatives en cause au principal ne prévoient pas la notification aux personnes concernées des mesures de surveillance dont elles ont fait l'objet ne constituerait pas, par elle-même, une atteinte excessive au droit au respect de la vie privée.

68 C'est dans ces conditions que 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 [TUE] ?

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 ? »

L'affaire C-512/18

69 Par une requête introduite le 1er septembre 2015, French Data Network, la Quadrature du Net et la Fédération des fournisseurs d'accès à Internet associatifs ont saisi le Conseil d'État d'un recours en annulation de la décision implicite de rejet née du silence gardé par le Premier ministre sur leur demande d'abrogation de l'article R. 10-13 du CPCE ainsi que du décret nº 2011-219, au motif, notamment, que ces textes méconnaîtraient l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 de la Charte. Privacy International ainsi que le Center for Democracy and Technology ont été admises à intervenir dans la procédure au principal.

70 S'agissant de l'article R. 10-13 du CPCE et de l'obligation de conservation généralisée et indifférenciée des données relatives aux communications qui y est prévue, la juridiction de renvoi, qui exprime des considérations similaires à celles émises dans le cadre de l'affaire C-511/18, fait observer qu'une telle conservation permet à l'autorité judiciaire d'accéder aux données relatives aux communications qu'un individu a effectuées avant d'être suspecté d'avoir commis une infraction pénale, de telle sorte que cette conservation présente une utilité sans équivalent pour la recherche, la constatation et la poursuite des infractions pénales.

71 En ce qui concerne le décret nº 2011-219, la juridiction de renvoi estime que l'article 6, II, de la LCEN, qui impose une obligation de détention et de conservation des seules données relatives à la création de contenu, entre non pas dans le champ d'application de la directive 2002/58, dans la mesure où celui-ci est limité, conformément à son article 3, paragraphe 1, à la fourniture de services de communications électroniques accessibles au public sur les réseaux publics de communications dans l'Union, mais dans le champ d'application de la directive 2000/31.

72 Cette juridiction estime toutefois qu'il ressort de l'article 15, paragraphes 1 et 2, de la directive 2000/31 que celle-ci n'instaure pas une interdiction de principe de conserver des données relatives à la création de contenu, à laquelle il pourrait seulement être dérogé par exception. Ainsi, se poserait la question de savoir si les articles 12, 14 et 15 de ladite directive, lus à la lumière des articles 6 à 8 et 11 ainsi que de

l'article 52, paragraphe 1, de la Charte, doivent être interprétés en ce sens qu'ils permettent à un État membre d'instaurer une réglementation nationale, telle que l'article 6, II, de la LCEN, qui impose aux personnes concernées 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.

73 C'est dans ces conditions que 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, 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 [TUE] ?

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 ? »

L'affaire C-520/18

74 Par des requêtes introduites les 10 janvier, 16 janvier, 17 janvier et 18 janvier 2017, jointes dans le cadre de la procédure au principal, l'Ordre des barreaux francophones et germanophone, l'Académie Fiscale ASBL et UA, la Liga voor Mensenrechten ASBL et la Ligue des Droits de l'Homme ASBL ainsi que VZ, WY et XX ont saisi la Cour constitutionnelle (Belgique) de recours visant l'annulation de la loi du 29 mai 2016, au motif que celle-ci violerait les articles 10 et 11 de la Constitution belge, lue en combinaison avec les articles 5, 6 à 11, 14, 15, 17 et 18 de la CEDH, les articles 7, 8, 11 et 47 ainsi que l'article 52, paragraphe 1, de la Charte, l'article 17 du pacte international relatif aux droits civils et politiques, adopté par l'Assemblée générale des Nations unies le 16 décembre 1966 et entré en vigueur le 23 mars 1976, les principes généraux de sécurité juridique, de proportionnalité et d'autodétermination en matière d'information ainsi que l'article 5, paragraphe 4, du TUE.

75 À l'appui de leurs recours, les requérants au principal font valoir en substance que l'illégalité de la loi du 29 mai 2016 tient notamment au fait que celle-ci dépasse les limites du strict nécessaire et ne prévoit pas de garanties de protection suffisantes. En particulier, ni ses dispositions relatives à la conservation des données ni celles régissant l'accès des autorités aux données conservées ne répondraient aux exigences découlant de l'arrêt du 8 avril 2014, Digital Rights Ireland e.a. (C-293/12 et C-594/12, ci-après l'« arrêt Digital Rights », EU:C:2014:238), et de l'arrêt du 21 décembre 2016, Tele2 (C-203/15 et C-698/15, EU:C:2016:970). En effet, ces dispositions comporteraient le risque que soient établis des profils de personnalité, avec les possibles abus en découlant de la part des autorités compétentes, et ne prévoiraient pas non plus un niveau approprié de sécurisation et de protection des données conservées. Enfin, cette loi couvrirait des personnes soumises au secret professionnel ainsi que

des personnes ayant une obligation de confidentialité, et concernerait des données de communication sensibles, à caractère personnel, sans comporter de garanties spéciales aux fins de protéger ces dernières données.

76 La juridiction de renvoi relève que les données que doivent conserver les fournisseurs de services de téléphonie, en ce compris par Internet, d'accès à Internet et de courrier électronique par Internet ainsi que les opérateurs fournissant des réseaux publics de communications électroniques, en vertu de la loi du 29 mai 2016, sont identiques à celles énumérées par la directive 2006/24/CE 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), sans que soit prévue une distinction quant aux personnes concernées ou en fonction de l'objectif poursuivi. À ce dernier égard, cette juridiction précise que l'objectif poursuivi par le législateur au moyen de cette loi est non seulement de lutter contre le terrorisme et la pédopornographie, mais également de pouvoir utiliser les données conservées dans une grande variété de situations dans le cadre de l'enquête pénale. En outre, la juridiction de renvoi constate qu'il ressort de l'exposé des motifs de ladite loi que le législateur national a considéré qu'il était impossible, à la lumière de l'objectif poursuivi, de mettre en place une obligation de conservation ciblée et différenciée, et qu'il a choisi d'assortir l'obligation de conservation générale et indifférenciée de garanties strictes, tant sur le plan des données conservées que sur le plan de l'accès à celles-ci, afin de limiter à un minimum l'ingérence dans le droit au respect de la vie privée.

77 La juridiction de renvoi ajoute que l'article 126, paragraphe 2, 1° et 2°, de la loi du 13 juin 2005, dans sa version issue de la loi du 29 mai 2016, prévoit les conditions dans lesquelles, respectivement, les autorités judiciaires et les services de renseignement et de sécurité peuvent obtenir l'accès aux données conservées, de telle sorte que l'examen de la légalité de cette loi au regard des exigences du droit de l'Union devrait être suspendu jusqu'à ce que la Cour rende ses décisions dans deux procédures préjudicielles, pendantes devant elles, relatives à un tel accès.

78 Enfin, la juridiction de renvoi relève que la loi du 29 mai 2016 vise à permettre une instruction pénale efficace et des sanctions effectives en cas d'abus sexuels à l'égard de mineurs ainsi qu'à rendre possible l'identification de l'auteur d'un tel délit, même lorsqu'il est fait usage de moyens de communications électroniques. Lors de la procédure devant elle, l'attention aurait été attirée à cet égard sur les obligations positives découlant des articles 3 et 8 de la CEDH. Ces obligations pourraient également découler des dispositions correspondantes de la Charte, susceptibles d'avoir des répercussions sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58.

79 C'est dans ces conditions que la Cour constitutionnelle a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes :

« 1) L'article 15, paragraphe 1, de la directive [2002/58], lu en combinaison avec le droit à la sécurité, garanti par l'article 6 de la [Charte], et le droit au respect des données personnelles, tel que garanti par les articles 7, 8 et 52, [paragraphe] l, de la [Charte], doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle que celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la directive [2002/58], générées ou traitées par eux dans le cadre de la fourniture de ces services, réglementation nationale qui n'a pas seulement pour objectif la recherche, la détection et la poursuite de faits de criminalité grave, mais également la garantie de la sécurité nationale, de la défense du territoire et de la sécurité publique, la recherche, la détection et la poursuite d'autres faits que ceux de criminalité grave ou la prévention d'un usage interdit des systèmes de communications électroniques, ou la réalisation d'un autre objectif identifié par l'article 23, paragraphe l, du règlement [2016/679] et qui est en outre sujette à des garanties précisées dans cette réglementation sur le plan de la conservation des données et de l'accès à celles-ci ?

2) L'article 15, paragraphe l, de la directive [2002/58], combiné avec les articles 4, 7, 8, 11 et 52, paragraphe l, de la [Charte], doit-il être interprété en ce sens qu'il s'oppose à une réglementation nationale telle celle en cause, qui prévoit une obligation générale pour les opérateurs et fournisseurs de services de communications électroniques de conserver les données de trafic et de localisation au sens de la directive [2002/58], générées ou traitées par eux dans le cadre de la fourniture de ces services, si cette réglementation a notamment pour objet de réaliser les obligations positives incombant à l'autorité en vertu des articles 4 et [7] de la Charte, consistant à prévoir un cadre légal qui permette une enquête pénale effective et une répression effective de l'abus sexuel des mineurs et qui permette effectivement d'identifier l'auteur du délit, même lorsqu'il est fait usage de moyens de communications électroniques ?

3) Si, sur la base des réponses données à la première ou à la deuxième question préjudicielle, la Cour constitutionnelle devait arriver à la conclusion que la loi litigieuse méconnaît une ou plusieurs des obligations découlant des dispositions mentionnées dans ces questions, pourrait-elle maintenir provisoirement les effets de la loi du [29 mai 2016] afin d'éviter une insécurité juridique et de permettre que les données collectées et conservées précédemment puissent encore être utilisées pour les objectifs visés par la loi ? »

Sur la procédure devant la Cour

80 Par décision du président de la Cour du 25 septembre 2018, les affaires C-511/18 et C-512/18 ont été jointes aux fins des procédures écrite et orale ainsi que de l'arrêt. L'affaire C-520/18 a été jointe à ces affaires par décision du président de la Cour du 9 juillet 2020 aux fins de l'arrêt.

Sur les questions préjudicielles

Sur les premières questions dans les affaires C-511/18 et C-512/18 ainsi que sur les première et deuxième questions dans l'affaire C-520/18

81 Par les premières questions dans les affaires C-511/18 et C-512/18 ainsi que par les première et deuxième questions dans l'affaire C-520/18, qu'il convient d'examiner conjointement, les juridictions de renvoi cherchent, en substance, à savoir si l'article 15, paragraphe 1, de la directive 2002/58 doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs de services de communications électroniques, à des fins prévues à cet article 15, paragraphe 1, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation.

Observations liminaires

82 Il ressort des dossiers dont dispose la Cour que les réglementations en cause au principal couvrent l'ensemble des moyens de communications électroniques et englobent l'ensemble des utilisateurs de ces moyens, sans qu'une différenciation ou une exception ne soit faite à cet égard. En outre, les données que ces réglementations imposent aux fournisseurs de services de communications électroniques de conserver sont, en particulier, celles qui sont nécessaires pour retrouver la source d'une communication et la destination de celle-ci, déterminer la date, l'heure, la durée et le type de la communication, identifier le matériel de communication utilisé ainsi que localiser les équipements terminaux et les communications, données au nombre desquelles figurent, notamment, le nom et l'adresse de l'utilisateur, les numéros de téléphone de l'appelant et de l'appelé ainsi que l'adresse IP pour les services Internet. En revanche, lesdites données ne couvrent pas le contenu des communications concernées.

83 Ainsi, les données qui doivent, en vertu des réglementations nationales en cause au principal, être conservées pendant un an permettent, notamment, de savoir quelle est la personne avec laquelle l'utilisateur d'un moyen de communication électronique a communiqué et par quel moyen cette communication a eu lieu, de déterminer la date, l'heure et la durée des communications et des connexions à Internet ainsi que l'endroit à partir duquel celles-ci ont eu lieu, et de connaître la localisation des équipements terminaux sans qu'une communication ne soit nécessairement acheminée. En outre, elles offrent la possibilité de déterminer la fréquence des communications de l'utilisateur avec certaines personnes pendant une période donnée. Enfin, s'agissant de la réglementation nationale en cause dans les affaires C-511/18 et C-512/18, il semble que celle-ci, en ce qu'elle couvre également les données relatives à l'acheminement des communications électroniques par les réseaux, permettent également d'identifier la nature des informations consultées en ligne.

84 Quant aux finalités poursuivies, il y a lieu de relever que les réglementations en cause dans les affaires C-511/18 et C-512/18 visent, entre autres finalités, la recherche, la constatation et la poursuite des infractions pénales en général, l'indépendance nationale, l'intégrité du territoire et la défense nationale, les intérêts majeurs de la politique étrangère, l'exécution des engagements européens et internationaux de la France, les intérêts économiques, industriels et scientifiques majeurs de la France, ainsi que la prévention du terrorisme, des atteintes à la forme républicaine des institutions et des violences collectives de nature à porter gravement atteinte à la paix publique. Pour ce qui est de la réglementation en cause dans l'affaire C-520/18, celle-ci a pour objectifs, entre autres, la recherche, la détection et la poursuite d'infractions pénales ainsi que la sauvegarde de la sécurité nationale, de la défense du territoire et de la sécurité publique.

85 Les juridictions de renvoi s'interrogent, en particulier, sur les incidences éventuelles quant à l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58, du droit à la sécurité consacré à l'article 6 de la Charte. De même, elles se demandent si l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte la conservation des données prévue par les réglementations en cause au principal peut, au regard de l'existence de règles restreignant l'accès des autorités nationales aux données conservées, être regardée comme étant justifiée. En outre, selon le Conseil d'État, cette question se posant dans un contexte marqué par des menaces graves et persistantes pour la sécurité nationale, elle doit également être appréciée au regard de l'article 4, paragraphe 2, TUE. La Cour constitutionnelle, quant à elle, souligne que la réglementation nationale en cause dans l'affaire C-520/18 met également en œuvre des obligations positives découlant des articles 4 et 7 de la Charte, consistant à prévoir un cadre légal permettant la répression effective de l'abus sexuel des mineurs.

86 Si tant le Conseil d'État que la Cour constitutionnelle partent de la prémisse selon laquelle les réglementations nationales en cause au principal, qui régissent la conservation des données relatives au trafic et des données de localisation ainsi que l'accès à ces données par les autorités nationales à des fins prévues à l'article 15, paragraphe 1, de la directive 2002/58, telles que la sauvegarde de la sécurité nationale, relèvent du champ d'application de cette directive, certaines parties au principal et certains des États membres ayant soumis des observations écrites à la Cour expriment un avis divergent à cet égard, en particulier concernant l'interprétation de l'article 1er, paragraphe 3, de ladite directive. Il convient donc d'examiner, tout d'abord, si lesdites réglementations relèvent du champ d'application de cette même directive.

Sur le champ d'application de la directive 2002/58

87 La Quadrature du Net, la Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net, Privacy International et le Center for Democracy and Technology avancent en substance, en se prévalant à cet égard de la jurisprudence de la Cour portant sur le champ d'application de la directive 2002/58, que tant la conservation des données que l'accès aux données conservées relèvent de ce champ d'application, que cet accès ait lieu en temps différé ou en temps réel. En effet, l'objectif de sauvegarde

de la sécurité nationale étant expressément mentionné à l'article 15, paragraphe 1, de cette directive, la poursuite de cet objectif n'entraînerait pas l'inapplicabilité de ladite directive. L'article 4, paragraphe 2, TUE, visé par les juridictions de renvoi, n'affecterait pas cette appréciation.

88 S'agissant des mesures de renseignement que les autorités françaises compétentes mettent directement en œuvre sans régir l'activité des fournisseurs de services de communications électroniques en leur imposant des obligations spécifiques, le Center for Democracy and Technology fait observer que ces mesures relèvent nécessairement du champ d'application de la directive 2002/58 et de celui de la Charte, dès lors qu'elles constituent des dérogations au principe de confidentialité garanti à l'article 5 de cette directive. Lesdites mesures devraient donc respecter les exigences découlant de l'article 15, paragraphe 1, de celle-ci.

89 En revanche, les gouvernements français, tchèque et estonien, l'Irlande, les gouvernements chypriote, hongrois, polonais, suédois et du Royaume-Uni font, en substance, valoir que la directive 2002/58 ne s'applique pas à des réglementations nationales telles que celles en cause au principal, dans la mesure où celles-ci ont pour finalité la sauvegarde de la sécurité nationale. Les activités des services de renseignement, en ce qu'elles tiennent au maintien de l'ordre public ainsi qu'à la sauvegarde de la sécurité intérieure et de l'intégrité territoriale, relèveraient des fonctions essentielles des États membres et, par suite, seraient de la seule compétence de ces derniers, comme en témoignerait notamment l'article 4, paragraphe 2, troisième phrase, TUE.

90 Ces gouvernements ainsi que l'Irlande se réfèrent de surcroît à l'article 1er, paragraphe 3, de la directive 2002/58, qui exclurait du champ d'application de celle-ci, à l'instar de ce que prévoyait déjà l'article 3, paragraphe 2, premier tiret, de la directive 95/46, les activités concernant la sécurité publique, la défense et la sûreté de l'État. Ils prennent appui à cet égard sur l'interprétation de cette dernière disposition figurant dans l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C-317/04 et C-318/04, EU:C:2006:346).

91 À cet égard, il y a lieu d'indiquer que, aux termes de son article 1er, paragraphe 1, la directive 2002/58 prévoit, notamment, l'harmonisation des dispositions nationales nécessaires pour assurer un niveau équivalent de protection des droits et des libertés fondamentaux, et en particulier du droit à la vie privée et à la confidentialité, en ce qui concerne le traitement des données à caractère personnel dans le secteur des communications électroniques.

92 L'article 1er, paragraphe 3, de cette directive exclut du champ d'application de celle-ci les « activités de l'État » dans les domaines qui y sont visés, parmi lesquelles figurent les activités de l'État dans le domaine pénal ainsi que celles concernant la sécurité publique, la défense et 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. Les activités ainsi mentionnées à titre d'exemples sont, dans tous les cas, des activités propres aux États ou aux autorités étatiques, étrangères aux domaines d'activité des particuliers (arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 32 et jurisprudence citée).

93 En outre, l'article 3 de la directive 2002/58 énonce que cette directive s'applique au traitement des données à caractère personnel dans le cadre de la fourniture de services de communications électroniques accessibles au public sur les réseaux de communications publics dans l'Union, y compris les réseaux de communications publics qui prennent en charge les dispositifs de collecte de données et d'identification (ci-après les « services de communications électroniques »). Partant, ladite directive doit être regardée comme régissant les activités des fournisseurs de tels services (arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 33 et jurisprudence citée).

94 Dans ce cadre, l'article 15, paragraphe 1, de la directive 2002/58 autorise les États membres à adopter, dans le respect des conditions qu'il prévoit, des « mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de [cette] directive » (arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 71).

95 Or, l'article 15, paragraphe 1, de la directive 2002/58 présuppose nécessairement que les mesures législatives nationales qui y sont visées relèvent du champ d'application de celle-ci, puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit. En outre, de telles mesures régissent, aux fins mentionnées à cette disposition, l'activité des fournisseurs de services de communications électroniques (arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 34 et jurisprudence citée).

96 C'est notamment au regard de ces considérations que la Cour a jugé que l'article 15, paragraphe 1, de la directive 2002/58, lu en combinaison avec l'article 3 de celle-ci, doit être interprété en ce sens que relèvent du champ d'application de cette directive non seulement une mesure législative qui impose aux fournisseurs de services de communications électroniques de conserver les données relatives au trafic et les données de localisation, mais également une mesure législative leur imposant d'accorder aux autorités nationales compétentes l'accès à ces données. En effet, de telles mesures législatives impliquent obligatoirement un traitement, par lesdits fournisseurs, desdites données et ne sauraient, en ce qu'elles régissent les activités de ces mêmes fournisseurs, être assimilées à des activités propres aux États, visées à l'article 1er, paragraphe 3, de ladite directive (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 35 et 37 ainsi que jurisprudence citée).

97 En outre, eu égard aux considérations figurant au point 95 du présent arrêt et à l'économie générale de la directive 2002/58, une interprétation de cette directive selon laquelle les mesures législatives visées à son article 15, paragraphe 1, seraient exclues du champ d'application de ladite directive du fait que les finalités auxquelles de telles mesures doivent répondre recoupent substantiellement les finalités poursuivies par les activités visées à l'article 1er, paragraphe 3, de la même directive, priverait cet article 15, paragraphe 1, de tout effet utile (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 72 et 73).

98 La notion d'« activités » figurant à l'article 1er, paragraphe 3, de la directive 2002/58 ne saurait donc, comme l'a relevé en substance M. l'avocat général au point 75 de ses conclusions dans les affaires jointes La Quadrature du Net e.a. (C-511/18 et C-512/18, EU:C:2020:6), être interprétée comme couvrant les mesures législatives visées à l'article 15, paragraphe 1, de cette directive.

99 Les dispositions de l'article 4, paragraphe 2, TUE, auxquelles se sont référés les gouvernements mentionnés au point 89 du présent arrêt, ne sauraient infirmer cette conclusion. En effet, conformément à la jurisprudence constante de la Cour, bien qu'il appartienne aux États membres de définir leurs intérêts essentiels de sécurité et d'arrêter les mesures propres à assurer leur sécurité intérieure et extérieure, le seul fait qu'une mesure nationale a été prise aux fins de la protection de la sécurité nationale ne saurait entraîner l'inapplicabilité du droit de l'Union et dispenser les États membres du respect nécessaire de ce droit [voir, en ce sens, arrêts du 4 juin 2013, ZZ, C-300/11, EU:C:2013:363, point 38 ; du 20 mars 2018, Commission/Autriche (Imprimerie d'État), C-187/16, EU:C:2018:194, points 75 et 76, ainsi que du 2 avril 2020, Commission/Pologne, Hongrie et République tchèque (Mécanisme temporaire de relocalisation de demandeurs de protection internationale), C-715/17, C-718/17 et C-719/17, EU:C:2020:257, points 143 et 170].

100 Il est vrai que, dans l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C-317/04 et C-318/04, EU:C:2006:346, points 56 à 59), la Cour a jugé que le transfert des données à caractère personnel par des compagnies aériennes à des autorités publiques d'un État tiers à des fins de prévention ainsi que

de lutte contre le terrorisme et d'autres crimes graves ne relevait pas, en vertu de l'article 3, paragraphe 2, premier tiret, de la directive 95/46, du champ d'application de cette directive, puisque ce transfert s'insérait dans un cadre institué par les pouvoirs publics visant la sécurité publique.

101 Toutefois, eu égard aux considérations figurant aux points 93, 95 et 96 du présent arrêt, cette jurisprudence n'est pas transposable à l'interprétation de l'article 1er, paragraphe 3, de la directive 2002/58. En effet, comme l'a relevé, en substance, M. l'avocat général aux points 70 à 72 de ses conclusions dans les affaires jointes La Quadrature du Net e.a. (C-511/18 et C-512/18, EU:C:2020:6), l'article 3, paragraphe 2, premier tiret, de la directive 95/46, auquel se rapporte ladite jurisprudence, excluait du champ d'application de cette dernière directive, de manière générale, les « traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État », sans opérer de distinction en fonction de l'auteur du traitement de données concerné. En revanche, dans le cadre de l'interprétation de l'article 1er, paragraphe 3, de la directive 2002/58, une telle distinction s'avère nécessaire. En effet, ainsi qu'il ressort des points 94 à 97 du présent arrêt, l'ensemble des traitements de données à caractère personnel effectués par les fournisseurs de services de communications électroniques relève du champ d'application de ladite directive, en ce compris les traitements qui découlent d'obligations qui leur sont imposées par les pouvoirs publics, alors que ces derniers traitements pouvaient, le cas échéant, relever de l'exception prévue à l'article 3, paragraphe 2, premier tiret, de la directive 95/46, compte tenu de la formulation plus large de cette disposition, visant l'ensemble des traitements, quel qu'en soit l'auteur, ayant pour objet la sécurité publique, la défense ou la sûreté de l'État.

102 Par ailleurs, il y a lieu de relever que la directive 95/46 en cause dans l'affaire ayant conduit à l'arrêt du 30 mai 2006, Parlement/Conseil et Commission (C-317/04 et C-318/04, EU:C:2006:346), a été, en vertu de l'article 94, paragraphe 1, du règlement 2016/679, abrogée et remplacée par celui-ci, avec effet au 25 mai 2018. Or, si ledit règlement précise, à son article 2, paragraphe 2, sous d), qu'il ne s'applique pas aux traitements effectués « par les autorités compétentes » à des fins, notamment, de prévention et de détection des infractions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces, il ressort de l'article 23, paragraphe 1, sous d) et h), du même règlement que les traitements de données à caractère personnel effectués à ces mêmes fins par des particuliers relèvent du champ d'application de celui-ci. Il s'ensuit que l'interprétation de l'article 1er, paragraphe 3, de l'article 3 et de l'article 15, paragraphe 1, de la directive 2002/58 qui précède est cohérente avec la délimitation du champ d'application du règlement 2016/679 que cette directive complète et précise.

103 En revanche, lorsque les États membres mettent directement en œuvre des mesures dérogeant à la confidentialité des communications électroniques, sans imposer des obligations de traitement aux fournisseurs de services de telles communications, la protection des données des personnes concernées relève non pas de la directive 2002/58, mais du seul droit national, sous réserve de l'application de la directive (UE) 2016/680 du Parlement européen et du Conseil, du 27 avril 2016, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel 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, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO 2016, L 119, p. 89), de telle sorte que les mesures en cause doivent respecter notamment le droit national de rang constitutionnel et les exigences de la CEDH.

104 Il résulte des considérations qui précèdent qu'une réglementation nationale imposant aux fournisseurs de services de communications électroniques de conserver des données relatives au trafic et des données de localisation aux fins de la protection de la sécurité nationale et de la lutte contre la criminalité, telle que celles en cause au principal, relève du champ d'application de la directive 2002/58.

Sur l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58

105 Il convient de rappeler, à titre liminaire, qu'il est de jurisprudence constante que, afin d'interpréter une disposition du droit de l'Union, il convient non seulement de se référer aux termes de celle-ci, mais également de tenir compte de son contexte et des objectifs poursuivis par la réglementation dont elle fait partie ainsi que de prendre en considération, notamment, la genèse de cette réglementation (voir, en ce sens, arrêt du 17 avril 2018, Egenberger, C-414/16, EU:C:2018:257, point 44).

106 La directive 2002/58 a pour finalité, ainsi qu'il ressort notamment de ses considérants 6 et 7, de protéger les utilisateurs des services de communications électroniques contre les dangers pour leurs données à caractère personnel et leur vie privée résultant des nouvelles technologies et, notamment, de la capacité accrue de stockage et de traitement automatisés de données. En particulier, ladite directive vise, ainsi que l'énonce son considérant 2, à garantir le plein respect des droits énoncés aux articles 7 et 8 de la Charte. À cet égard, il ressort de l'exposé des motifs de la proposition de directive du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques [COM (2000) 385 final], à l'origine de la directive 2002/58, que le législateur de l'Union a entendu « faire en sorte qu'un niveau élevé de protection des données à caractère personnel et de la vie privée continue à être garanti pour tous les services de communications électroniques, quelle que soit la technologie utilisée ».

107 À cet effet, l'article 5, paragraphe 1, de la directive 2002/58 consacre le principe de confidentialité tant des communications électroniques que des données relatives au trafic y afférentes et implique, notamment, l'interdiction faite, en principe, à toute personne autre que les utilisateurs de stocker, sans le consentement de ceux-ci, ces communications et ces données.

108 S'agissant, en particulier, du traitement et du stockage des données relatives au trafic par les fournisseurs de services de communications électroniques, il ressort de l'article 6 ainsi que des considérants 22 et 26 de la directive 2002/58 qu'un tel traitement n'est autorisé que dans la mesure et pour la durée nécessaires à la commercialisation des services, à la facturation de ceux-ci et à la fourniture de services à valeur ajoutée. Une fois cette durée expirée, les données ayant été traitées et stockées doivent être effacées ou rendues anonymes. Quant aux données de localisation autres que les données relatives au trafic, l'article 9, paragraphe 1, de ladite directive prévoit que ces données ne peuvent être traitées que sous certaines conditions et après avoir été rendues anonymes ou moyennant le consentement des utilisateurs ou des abonnés (arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 86 et jurisprudence citée).

109 Ainsi, en adoptant cette directive, le législateur de l'Union a concrétisé les droits consacrés aux articles 7 et 8 de la Charte, de telle sorte que les utilisateurs des moyens de communications électroniques sont en droit de s'attendre, en principe, à ce que leurs communications et les données y afférentes restent, en l'absence de leur consentement, anonymes et ne puissent pas faire l'objet d'un enregistrement.

110 Toutefois, l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'introduire des exceptions à l'obligation de principe, énoncée à l'article 5, paragraphe 1, de cette directive, de garantir la confidentialité des données à caractère personnel ainsi qu'aux obligations correspondantes, mentionnées notamment aux articles 6 et 9 de ladite directive, lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, 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. 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 l'un de ces motifs.

111 Cela étant, la faculté de déroger aux droits et aux obligations prévus aux articles 5, 6 et 9 de la directive 2002/58 ne saurait justifier que la dérogation à l'obligation de principe de garantir la confidentialité des communications électroniques et des données y afférentes et, en particulier, à l'interdiction de stocker ces données, explicitement prévue à l'article 5 de cette directive, devienne la règle (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 89 et 104).

112 Quant aux objectifs susceptibles de justifier une limitation des droits et des obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58, la Cour a déjà jugé que l'énumération des objectifs figurant à l'article 15, paragraphe 1, première phrase, de cette directive revêt un caractère exhaustif, de telle sorte qu'une mesure législative adoptée au titre de cette disposition doit répondre effectivement et strictement à l'un de ces objectifs (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 52 et jurisprudence citée).

113 En outre, il ressort de l'article 15, paragraphe 1, troisième phrase, de la directive 2002/58 que les États membres ne sont autorisés à prendre des mesures législatives visant à limiter la portée des droits et des obligations visés aux articles 5, 6 et 9 de cette directive que dans le respect des principes généraux du droit de l'Union, parmi lesquels figure le principe de proportionnalité, et des droits fondamentaux garantis par la Charte. À cet égard, la Cour a déjà jugé que l'obligation imposée par un État membre aux fournisseurs de services de communications électroniques, par une réglementation nationale, de conserver les données relatives au trafic aux fins de les rendre, le cas échéant, accessibles aux autorités nationales compétentes soulève des questions relatives au respect non seulement des articles 7 et 8 de la Charte, relatifs, respectivement à la protection de la vie privée ainsi qu'à la protection des données à caractère personnel, mais également de l'article 11 de la Charte, relatif à la liberté d'expression (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 25 et 70, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 91 et 92 ainsi que jurisprudence citée).

114 Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 doit tenir compte de l'importance tant du droit au respect de la vie privée, garanti à l'article 7 de la Charte, que du droit à la protection des données à caractère personnel, garanti à l'article 8 de celle-ci, telle qu'elle ressort de la jurisprudence de la Cour, ainsi que du droit à la liberté d'expression, ce droit fondamental, garanti à l'article 11 de la Charte, constituant l'un des fondements essentiels d'une société démocratique et pluraliste et faisant partie des valeurs sur lesquelles est, conformément à l'article 2 TUE, fondée l'Union (voir, en ce sens, arrêts du 6 mars 2001, Connolly/Commission, C-274/99 P, EU:C:2001:127, point 39, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 93 et jurisprudence citée).

115 Il y a lieu de préciser, à cet égard, que la conservation des données relatives au trafic et des données de localisation constitue, par elle-même, d'une part, une dérogation à l'interdiction, prévue à l'article 5, paragraphe 1, de la directive 2002/58, faite à toute autre personne que les utilisateurs de stocker ces données et, d'autre part, une ingérence dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel, consacrés aux articles 7 et 8 de la Charte, sans qu'il importe de savoir si les informations relatives à la vie privée concernées présentent ou non un caractère sensible ou si les intéressés ont ou non subi d'éventuels inconvénients en raison de cette ingérence [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126 ainsi que jurisprudence citée ; voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 30 janvier 2020, Breyer c. Allemagne, CE:ECHR:2020:0130JUD005000112, § 81].

116 Il est également sans pertinence que les données conservées soient ou non utilisées par la suite (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 16 février 2000, Amann c. Suisse, CE:ECHR:2000:0216JUD002779895, § 69, ainsi que 13 février 2020, Trjakovski et Chipovski c. Macédonie du Nord, CE:ECHR:2020:0213JUD005320513, § 51), l'accès à de telles données constituant,

quelle que soit l'utilisation qui en est faite ultérieurement, une ingérence distincte dans les droits fondamentaux visés au point précédent [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 124 et 126].

117 Cette conclusion apparaît d'autant plus justifiée que les données relatives au trafic et les données de localisation sont susceptibles de révéler des informations sur un nombre important d'aspects de la vie privée des personnes concernées, y compris des informations sensibles, telles que l'orientation sexuelle, les opinions politiques, les convictions religieuses, philosophiques, sociétales ou autres ainsi que l'état de santé, alors que de telles données jouissent, par ailleurs, d'une protection particulière en droit de l'Union. Prises dans leur ensemble, lesdites données peuvent permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir le profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 27, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 99).

118 Dès lors, d'une part, la conservation des données relatives au trafic et des données de localisation à des fins policières est susceptible, à elle seule, de porter atteinte au droit au respect des communications, consacré à l'article 7 de la Charte, et d'entraîner des effets dissuasifs sur l'exercice par les utilisateurs des moyens de communications électroniques de leur liberté d'expression, garantie à l'article 11 de celle-ci (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 28, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 101). Or, de tels effets dissuasifs peuvent affecter en particulier les personnes dont les communications sont soumises, selon les règles nationales, au secret professionnel ainsi que les lanceurs d'alerte dont les activités sont protégées par la directive (UE) 2019/1937 du Parlement européen et du Conseil, du 23 octobre 2019, sur la protection des personnes qui signalent des violations du droit de l'Union (JO 2019, L 305, p. 17). En outre, ces effets sont d'autant plus graves que le nombre et la variété des données conservées sont élevés.

119 D'autre part, compte tenu de la quantité importante de données relatives au trafic et de données de localisation susceptibles d'être conservées de manière continue par une mesure de conservation généralisée et indifférenciée ainsi que du caractère sensible des informations que ces données peuvent fournir, la seule conservation desdites données par les fournisseurs de services de communications électroniques comporte des risques d'abus et d'accès illicite.

120 Cela étant, en ce qu'il permet aux États membres d'introduire les dérogations visées au point 110 du présent arrêt, l'article 15, paragraphe 1, de la directive 2002/58 reflète la circonstance que les droits consacrés aux articles 7, 8 et 11 de la Charte n'apparaissent pas comme étant des prérogatives absolues, mais doivent être pris en considération par rapport à leur fonction dans la société (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 172 ainsi que jurisprudence citée).

121 En effet, ainsi qu'il ressort de l'article 52, paragraphe 1, de la Charte, celle-ci admet des limitations à l'exercice de ces droits, pour autant que ces limitations soient prévues par la loi, qu'elles respectent le contenu essentiel desdits droits et que, dans le respect du principe de proportionnalité, elles soient 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.

122 Ainsi, l'interprétation de l'article 15, paragraphe 1, de la directive 2002/58 à la lumière de la Charte requiert de tenir compte également de l'importance des droits consacrés aux articles 3, 4, 6 et 7 de la Charte et de celle que revêtent les objectifs de protection de la sécurité nationale et de lutte contre la criminalité grave en contribuant à la protection des droits et des libertés d'autrui.

123 À cet égard, l'article 6 de la Charte, auquel se réfèrent le Conseil d'État et la Cour constitutionnelle, consacre le droit de toute personne non seulement à la liberté mais également à la sûreté et garantit des droits correspondant à ceux qui le sont à l'article 5 de la CEDH (voir, en ce sens, arrêts du 15 février 2016, N., C-601/15 PPU, EU:C:2016:84, point 47 ; du 28 juillet 2016, JZ, C-294/16 PPU, EU:C:2016:610, point 48, ainsi que du 19 septembre 2019, Rayonna prokuratura Lom, C-467/18, EU:C:2019:765, point 42 et jurisprudence citée).

124 En outre, il y a lieu de rappeler que l'article 52, paragraphe 3, de la Charte vise à assurer la cohérence nécessaire entre les droits contenus dans cette dernière et les droits correspondants garantis par la CEDH, sans porter atteinte à l'autonomie du droit de l'Union et de la Cour de justice de l'Union européenne. Il convient donc de tenir compte des droits correspondants de la CEDH en vue de l'interprétation de la Charte, en tant que seuil de protection minimale [voir, en ce sens, arrêts du 12 février 2019, TC, C-492/18 PPU, EU:C:2019:108, point 57, ainsi que du 21 mai 2019, Commission/Hongrie (Usufruits sur terres agricoles), C-235/17, EU:C:2019:432, point 72 et jurisprudence citée].

125 S'agissant de l'article 5 de la CEDH, qui consacre le « droit à la liberté » et le « droit à la sûreté », celui-ci vise, selon la jurisprudence de la Cour européenne des droits de l'homme, à protéger l'individu contre toute privation de liberté arbitraire ou injustifiée (voir, en ce sens, Cour EDH, 18 mars 2008, Ladent c. Pologne, CE:ECHR:2008:0318JUD001103603, §§ 45 et 46 ; 29 mars 2010, Medvedyev et autres c. France, CE:ECHR:2010:0329JUD000339403, §§ 76 et 77, ainsi que 13 décembre 2012, El-Masri v. « The former Yugoslav Republic of Macedonia », CE:ECHR:2012:1213JUD003963009, § 239). Toutefois, dans la mesure où cette disposition vise une privation de liberté commise par une autorité publique, l'article 6 de la Charte ne saurait être interprété comme imposant aux pouvoirs publics une obligation d'adopter des mesures spécifiques en vue de réprimer certaines infractions pénales.

126 En revanche, en ce qui concerne, en particulier, la lutte effective contre les infractions pénales dont sont victimes, notamment, les mineurs et les autres personnes vulnérables, évoquée par la Cour constitutionnelle, il convient de souligner que des obligations positives à la charge des pouvoirs publics peuvent résulter de l'article 7 de la Charte, en vue de l'adoption de mesures juridiques visant à protéger la vie privée et familiale [voir, en ce sens, arrêt du 18 juin 2020, Commission/Hongrie (Transparence associative), C-78/18, EU:C:2020:476, point 123 et jurisprudence citée de la Cour européenne des droits de l'homme]. De telles obligations sont également susceptibles de découler dudit article 7 en ce qui concerne la protection du domicile et des communications, ainsi que des articles 3 et 4 s'agissant de la protection de l'intégrité physique et psychique des personnes ainsi que de l'interdiction de la torture et des traitements inhumains et dégradants.

127 Or, face à ces différentes obligations positives, il convient de procéder à une conciliation nécessaire des différents intérêts et droits en cause.

128 En effet, la Cour européenne des droits de l'homme a jugé que les obligations positives découlant des articles 3 et 8 de la CEDH, dont les garanties correspondantes figurent aux articles 4 et 7 de la Charte, impliquent, notamment, l'adoption de dispositions matérielles et procédurales ainsi que de mesures d'ordre pratique permettant une lutte efficace à l'encontre des infractions contre les personnes à travers une enquête et des poursuites effectives, cette obligation étant d'autant plus importante lorsque le bien-être physique et moral d'un enfant est menacé. Cela étant, les mesures qu'il appartient aux autorités compétentes de prendre doivent pleinement respecter les voies légales et les autres garanties qui sont de nature à limiter l'étendue des pouvoirs d'investigations pénales ainsi que les

autres libertés et droits. En particulier, selon cette juridiction, il convient d'instaurer un cadre légal permettant de concilier les différentes intérêts et droits à protéger (Cour EDH, 28 octobre 1998, Osman c. Royaume-Uni, CE:ECHR:1998:1028JUD002345294, §§ 115 et 116 ; 4 mars 2004, M.C. c. Bulgarie, CE:ECHR:2003:1204JUD003927298, § 151 ; 24 juin 2004, Von Hannover c. Allemagne, CE:ECHR:2004:0624JUD005932000, §§ 57 et 58, ainsi que 2 décembre 2008, K.U. c. Finlande, CE:ECHR:2008:1202JUD 000287202, §§ 46, 48 et 49).

129 En ce qui concerne le respect du principe de proportionnalité, l'article 15, paragraphe 1, première phrase, de la directive 2002/58 dispose que les États membres peuvent adopter une mesure dérogeant au principe de confidentialité des communications et des données relatives au trafic y afférentes lorsqu'une telle mesure est « nécessaire, appropriée et proportionnée, au sein d'une société démocratique », au regard des objectifs que cette disposition énonce. Le considérant 11 de cette directive précise qu'une mesure de cette nature doit être « rigoureusement » proportionnée au but poursuivi.

130 À cet égard, il convient de rappeler que la protection du droit fondamental au respect de la vie privée exige, conformément à la jurisprudence constante de la Cour, que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire. En outre, un objectif d'intérêt général ne saurait être poursuivi sans tenir compte du fait qu'il doit être concilié avec les droits fondamentaux concernés par la mesure, ce en effectuant une pondération équilibrée entre, d'une part, l'objectif d'intérêt général et, d'autre part, les droits en cause [voir, en ce sens, arrêts du 16 décembre 2008, Satakunnan Markkinapörssi et Satamedia, C-73/07, EU:C:2008:727, point 56 ; du 9 novembre 2010, Volker und Markus Schecke et Eifert, C-92/09 et C-93/09, EU:C:2010:662, point 76, 77 et 86, ainsi que du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 52 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 140].

131 Plus particulièrement, il découle de la jurisprudence de la Cour que la possibilité pour les États membres de justifier une limitation aux droits et aux obligations prévus, notamment, aux articles 5, 6 et 9 de la directive 2002/58 doit être appréciée en mesurant la gravité de l'ingérence que comporte une telle limitation et en vérifiant que l'importance de l'objectif d'intérêt général poursuivi par cette limitation est en relation avec cette gravité (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 55 et jurisprudence citée).

132 Pour satisfaire à l'exigence de proportionnalité, une réglementation doit prévoir des règles claires et précises régissant la portée et l'application de la mesure en cause et imposant des exigences minimales, de telle sorte que les personnes dont les données à caractère personnel sont concernées disposent de garanties suffisantes permettant de protéger efficacement ces données contre les risques d'abus. Cette réglementation doit être légalement contraignante en droit interne et, en particulier, indiquer en quelles circonstances et sous quelles conditions une mesure prévoyant le traitement de telles données peut être prise, garantissant ainsi que l'ingérence soit limitée au strict nécessaire. La nécessité de disposer de telles garanties est d'autant plus importante lorsque les données à caractère personnel sont soumises à un traitement automatisé, notamment lorsqu'il existe un risque important d'accès illicite à ces données. Ces considérations valent en particulier lorsqu'est en jeu la protection de cette catégorie particulière de données à caractère personnel que sont les données sensibles [voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 54 et 55, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 117 ; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 141].

133 Ainsi, une réglementation prévoyant une conservation des données à caractère personnel doit toujours répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 191 et jurisprudence citée, ainsi que arrêt du 3 octobre 2019, A e.a., C-70/18, EU:C:2019:823, point 63].

– Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la sauvegarde de la sécurité nationale

134 Il y a lieu de faire observer que l'objectif de sauvegarde de la sécurité nationale, évoqué par les juridictions de renvoi et les gouvernements ayant présenté des observations, n'a pas encore été spécifiquement examiné par la Cour dans ses arrêts interprétant la directive 2002/58.

135 À cet égard, il convient de relever, d'emblée, que l'article 4, paragraphe 2, TUE énonce que la sécurité nationale reste de la seule responsabilité de chaque État membre. Cette responsabilité correspond à l'intérêt primordial de protéger les fonctions essentielles de l'État et les intérêts fondamentaux de la société et inclut la prévention et la répression d'activités de nature à déstabiliser gravement les structures constitutionnelles, politiques, économiques ou sociales fondamentales d'un pays, et en particulier à menacer directement la société, la population ou l'État en tant que tel, telles que notamment des activités de terrorisme.

136 Or, l'importance de l'objectif de sauvegarde de la sécurité nationale, lu à l'aune de l'article 4, paragraphe 2, TUE, dépasse celle des autres objectifs visés à l'article 15, paragraphe 1, de la directive 2002/58, notamment des objectifs de lutte contre la criminalité en général, même grave, ainsi que de sauvegarde de la sécurité publique. En effet, des menaces telles que celles visées au point précédent se distinguent, par leur nature et leur particulière gravité, du risque général de survenance de tensions ou de troubles, même graves, à la sécurité publique. Sous réserve du respect des autres exigences prévues à l'article 52, paragraphe 1, de la Charte, l'objectif de sauvegarde de la sécurité nationale est dès lors susceptible de justifier des mesures comportant des ingérences dans les droits fondamentaux plus graves que celles que pourraient justifier ces autres objectifs.

137 Ainsi, dans des situations telles que celles décrites aux points 135 et 136 du présent arrêt, 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, ne s'oppose pas, en principe, à une mesure législative qui autorise les autorités compétentes à enjoindre aux fournisseurs de services de communications électroniques de procéder à la conservation des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs des moyens de communications électroniques pendant une période limitée, dès lors qu'il existe des circonstances suffisamment concrètes permettant de considérer que l'État membre concerné fait face à une menace grave telle que celle visée aux points 135 et 136 du présent arrêt pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible. Même si une telle mesure vise, de manière indifférenciée, tous les utilisateurs de moyens de communications électroniques sans que ceux-ci paraissent, de prime abord, présenter de rapport, au sens de la jurisprudence visée au point 133 du présent arrêt, avec une menace pour la sécurité nationale de cet État membre, il y a lieu néanmoins de considérer que l'existence d'une telle menace est de nature, par elle-même, à établir ce rapport.

138 L'injonction prévoyant la conservation préventive des données de l'ensemble des utilisateurs des moyens de communications électroniques doit, néanmoins, être temporellement limitée au strict nécessaire. S'il ne peut être exclu que l'injonction faite aux fournisseurs de services de communications électroniques de procéder à la conservation des données puisse, en raison de la persistance d'une telle menace, être renouvelée, la durée de chaque injonction ne saurait dépasser un laps de temps prévisible. De surcroît, une telle conservation des données doit être sujette à des limitations et encadrée par des garanties strictes permettant de protéger efficacement les données à caractère personnel des personnes concernées contre les risques d'abus. Ainsi, cette conservation ne saurait présenter un caractère systématique.

139 Eu égard à la gravité de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte résultant d'une telle mesure de conservation généralisée et indifférenciée des données, il importe d'assurer que le recours à celle-ci soit effectivement limité aux situations dans lesquelles il existe une menace grave pour la sécurité nationale, telles que celles visées aux points 135 et 136 du

présent arrêt. À cet effet, il est essentiel qu'une décision faisant injonction aux fournisseurs de services de communications électroniques de procéder à une telle conservation des données puisse faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues.

– Sur les mesures législatives prévoyant la conservation préventive des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique

140 Pour ce qui est de l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales, conformément au principe de proportionnalité, seules la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature à justifier des ingérences graves dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, telles que celles qu'implique la conservation des données relatives au trafic et des données de localisation. Dès lors, seules des ingérences dans lesdits droits fondamentaux ne présentant pas un caractère grave peuvent être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général [voir, en ce sens, arrêts du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 102, ainsi que du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 56 et 57; avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 149].

141 Une réglementation nationale prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, en vue de lutter contre la criminalité grave, 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 (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 107).

142 En effet, compte tenu du caractère sensible des informations que peuvent fournir les données relatives au trafic et les données de localisation, la confidentialité de ces dernières est essentielle pour le droit au respect de la vie privée. Ainsi, et compte tenu, d'une part, des effets dissuasifs sur l'exercice des droits fondamentaux consacrés aux articles 7 et 11 de la Charte, visés au point 118 du présent arrêt, que la conservation de ces données est susceptible d'entraîner et, d'autre part, de la gravité de l'ingérence que comporte une telle conservation, il importe, dans une société démocratique, que celle-ci soit, comme le prévoit le système mis en place par la directive 2002/58, l'exception et non la règle et que ces données ne puissent faire l'objet d'une conservation systématique et continue. Cette conclusion s'impose même à l'égard des objectifs de lutte contre la criminalité grave et de prévention des menaces graves contre la sécurité publique ainsi que de l'importance qu'il convient de leur reconnaître.

143 En outre, la Cour a souligné qu'une réglementation prévoyant la conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation couvre les communications électroniques de la quasi-totalité de la population sans qu'aucune différenciation, limitation ni exception soient opérées en fonction de l'objectif poursuivi. Une telle réglementation, contrairement à l'exigence rappelée au point 133 du présent arrêt, concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans que ces personnes se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales. Elle s'applique donc même à des personnes pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement puisse avoir un lien, même indirect ou lointain, avec cet objectif de lutte contre des actes de criminalité grave et, en particulier, sans que soit prévue une relation entre les données dont la conservation est prévue et une menace pour la sécurité publique

(voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, points 57 et 58, ainsi que du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 105).

144 En particulier, comme l'a déjà jugé la Cour, une telle réglementation 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 grave (voir, en ce sens, arrêts du 8 avril 2014, Digital Rights, C-293/12 et C-594/12, EU:C:2014:238, point 59, et du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 106).

145 Or, même les obligations positives des États membres susceptibles de découler, selon le cas, des articles 3, 4 et 7 de la Charte et portant, ainsi qu'il a été relevé aux points 126 et 128 du présent arrêt, sur la mise en place de règles permettant une lutte effective contre les infractions pénales ne sauraient avoir pour effet de justifier des ingérences aussi graves que celles que comporte une réglementation prévoyant une conservation des données relatives au trafic et des données de localisation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte de la quasi-totalité de la population sans que les données des personnes concernées soient susceptibles de révéler un lien, au moins indirect, avec l'objectif poursuivi.

146 En revanche, conformément à ce qui a été relevé aux points 142 à 144 du présent arrêt, et eu égard à la conciliation nécessaire des droits et des intérêts en cause, les objectifs de lutte contre la criminalité grave, de prévention d'atteintes graves à la sécurité publique et, a fortiori, de sauvegarde de la sécurité nationale sont susceptibles de justifier, compte tenu de leur importance, au regard des obligations positives rappelées au point précédent et auxquelles s'est référée notamment la Cour constitutionnelle, l'ingérence particulièrement grave que comporte une conservation ciblée des données relatives au trafic et des données de localisation.

147 Ainsi, comme l'a déjà jugé la Cour, 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, ne s'oppose pas à ce qu'un État membre adopte une réglementation permettant, à titre préventif, une conservation ciblée des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, tout comme aux fins de la sauvegarde de la sécurité nationale, à condition qu'une telle conservation soit, en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue, limitée au strict nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 108).

148 S'agissant de la délimitation dont doit faire l'objet une telle mesure de conservation des données, celle-ci peut, notamment, être fixée en fonction des catégories de personnes concernées, dès lors que l'article 15, paragraphe 1, de la directive 2002/58 ne s'oppose pas à une réglementation fondée sur des éléments objectifs, permettant de viser les personnes dont les données relatives au trafic et les données de localisation sont susceptibles de révéler un lien, au moins indirect, avec des actes de criminalité grave, de contribuer d'une manière ou d'une autre à la lutte contre la criminalité grave ou de prévenir un risque grave pour la sécurité publique ou encore un risque pour la sécurité nationale (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 111).

149 À cet égard, il convient de préciser que les personnes ainsi visées peuvent notamment être celles ayant été préalablement identifiées, dans le cadre des procédures nationales applicables et sur la base d'éléments objectifs, comme présentant une menace pour la sécurité publique ou la sécurité nationale de l'État membre concerné.

150 La délimitation d'une mesure prévoyant la conservation des données relatives au trafic et des données de localisation peut également être fondée sur un critère géographique lorsque les autorités nationales compétentes considèrent, sur la base d'éléments objectifs et non discriminatoires, qu'il existe, dans une ou plusieurs zones géographiques, une situation caractérisée par un risque élevé de préparation ou de commission d'actes de criminalité grave (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 111). Ces zones peuvent être, notamment, des lieux caractérisés par un nombre élevé d'actes de criminalité grave, des lieux particulièrement exposés à la commission d'actes de criminalité grave, tels que des lieux ou infrastructures fréquentés régulièrement par un nombre très élevé de personnes, ou encore des lieux stratégiques, tels que des aéroports, des gares ou des zones de péages.

151 Afin d'assurer que l'ingérence que comportent les mesures de conservation ciblée décrites aux points 147 à 150 du présent arrêt soit conforme au principe de proportionnalité, leur durée ne saurait dépasser celle qui est strictement nécessaire au regard de l'objectif poursuivi ainsi que des circonstances les justifiant, sans préjudice d'un renouvellement éventuel en raison de la persistance de la nécessité de procéder à une telle conservation.

– Sur les mesures législatives prévoyant la conservation préventive des adresses IP et des données relatives à l'identité civile aux fins de la lutte contre la criminalité et de la sauvegarde de la sécurité publique

152 Il y a lieu de relever que les adresses IP, quoique faisant partie des données relatives au trafic, sont générées sans être rattachées à une communication déterminée et servent principalement à identifier, par l'intermédiaire des fournisseurs de services de communications électroniques, la personne physique propriétaire d'un équipement terminal à partir duquel une communication au moyen de l'Internet est effectuée. Ainsi, en matière de courrier électronique ainsi que de téléphonie par Internet, pour autant que seules les adresses IP de la source de la communication sont conservées et non celles du destinataire de celle-ci, ces adresses ne révèlent, en tant que telles, aucune information sur les tierces personnes ayant été en contact avec la personne à l'origine de la communication. Cette catégorie de données présente donc un degré de sensibilité moindre que les autres données relatives au trafic.

153 Toutefois, les adresses IP pouvant être utilisées pour effectuer notamment le traçage exhaustif du parcours de navigation d'un internaute et, par suite, de son activité en ligne, ces données permettent d'établir le profil détaillé de ce dernier. Ainsi, la conservation et l'analyse desdites adresses IP que nécessite un tel traçage constituent des ingérences graves dans les droits fondamentaux de l'internaute consacrés aux articles 7 et 8 de la Charte, pouvant avoir des effets dissuasifs tels que ceux visés au point 118 du présent arrêt.

154 Or, aux fins de la conciliation nécessaire des droits et des intérêts en cause exigée par la jurisprudence citée au point 130 du présent arrêt, il y a lieu de tenir compte du fait que, dans le cas d'une infraction commise en ligne, l'adresse IP peut constituer le seul moyen d'investigation permettant l'identification de la personne à laquelle cette adresse était attribuée au moment de la commission de cette infraction. À cela s'ajoute le fait que la conservation des adresses IP par les fournisseurs de services de communications électroniques au-delà de la durée d'attribution de ces données n'apparaît, en principe, pas nécessaire aux fins de la facturation des services en cause, de telle sorte que la détection des infractions commises en ligne peut, de ce fait, comme l'ont indiqué plusieurs gouvernements dans leurs observations soumises à la Cour, s'avérer impossible sans avoir recours à une mesure législative au titre de l'article 15, paragraphe 1, de la directive 2002/58. Tel peut notamment être le cas, ainsi que l'ont fait valoir ces gouvernements, des infractions particulièrement graves en matière de pédopornographie, telles que l'acquisition, la diffusion, la transmission ou la mise à disposition en ligne de pédopornographie, au sens de l'article 2, sous c), de la directive 2011/93/UE du Parlement

européen et du Conseil, du 13 décembre 2011, relative à la lutte contre les abus sexuels et l'exploitation sexuelle des enfants, ainsi que la pédopornographie et remplaçant la décision-cadre 2004/68/JAI du Conseil (JO 2011, L 335, p. 1).

155 Dans ces conditions, s'il est vrai qu'une mesure législative prévoyant la conservation des adresses IP de l'ensemble des personnes physiques propriétaires d'un équipement terminal à partir duquel un accès à Internet peut être effectué viserait des personnes qui ne présentent, de prime abord, pas de lien, au sens de la jurisprudence citée au point 133 du présent arrêt, avec les objectifs poursuivis et que les internautes disposent, conformément à ce qui a été constaté au point 109 du présent arrêt, du droit de s'attendre, en vertu des articles 7 et 8 de la Charte, à ce que leur identité ne soit, en principe, pas dévoilée, une mesure législative prévoyant la conservation généralisée et indifférenciée des seules adresses IP attribuées à la source d'une connexion n'apparaît pas, en principe, contraire à l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des article 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, pourvu que cette possibilité soit soumise au strict respect des conditions matérielles et procédurales devant régir l'utilisation de ces données.

156 Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte que comporte cette conservation, seule la lutte contre la criminalité grave et la prévention des menaces graves contre la sécurité publique sont de nature, à l'instar de la sauvegarde de la sécurité nationale, à justifier cette ingérence. En outre, la durée de conservation ne saurait excéder celle qui est strictement nécessaire au regard de l'objectif poursuivi. Enfin, une mesure de cette nature doit prévoir des conditions et des garanties strictes quant à l'exploitation de ces données, notamment par un traçage, à l'égard des communications et des activités effectuées en ligne par les personnes concernées.

157 En ce qui concerne, enfin, les données relatives à l'identité civile des utilisateurs des moyens de communications électroniques, ces données ne permettent pas, à elles seules, de connaître la date, l'heure, la durée et les destinataires des communications effectuées, non plus que les endroits où ces communications ont eu lieu ou la fréquence de celles-ci avec certaines personnes pendant une période donnée, de telle sorte qu'elles ne fournissent, mises à part les coordonnées de ceux-ci, telles que leurs adresses, aucune information sur les communications données et, par voie de conséquence, sur leur vie privée. Ainsi, l'ingérence que comporte une conservation de ces données ne saurait, en principe, être qualifiée de grave (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, points 59 et 60).

158 Il en découle que, conformément à ce qui a été exposé au point 140 du présent arrêt, les mesures législatives visant le traitement de ces données en tant que telles, notamment leur conservation et l'accès à celles-ci à la seule fin de l'identification de l'utilisateur concerné, et sans que lesdites données puissent être associées à des informations relatives aux communications effectuées, sont susceptibles d'être justifiées par l'objectif de prévention, de recherche, de détection et de poursuite d'infractions pénales en général, auquel se réfère l'article 15, paragraphe 1, première phrase, de la directive 2002/58 (voir, en ce sens, arrêt du 2 octobre 2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, point 62).

159 Dans ces conditions, eu égard à la conciliation nécessaire des droits et des intérêts en cause et pour les raisons figurant aux points 131 et 158 du présent arrêt, il y a lieu de considérer que, même en l'absence de lien entre l'ensemble des utilisateurs des moyens de communications électroniques et les objectifs poursuivis, 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, ne s'oppose pas à une mesure législative imposant, sans délai particulier, aux fournisseurs de services de communications électroniques la conservation des données relatives à l'identité civile de l'ensemble des utilisateurs des moyens de communications électroniques aux fins de la prévention, de la recherche, de la détection et de la poursuite d'infractions pénales ainsi que de la sauvegarde de la sécurité publique, sans qu'il soit nécessaire que les infraction pénales ou que les menaces contre ou les atteintes à la sécurité publique soient graves.

– Sur les mesures législatives prévoyant la conservation rapide des données relatives au trafic et des données de localisation aux fins de la lutte contre la criminalité grave

160 En ce qui concerne les données relatives au trafic et les données de localisation traitées et stockées par les fournisseurs de services de communications électroniques sur la base des articles 5, 6 et 9 de la directive 2002/58, ou sur celle de mesures législatives prises en vertu de l'article 15, paragraphe 1, de celle-ci, telles que décrites aux points 134 à 159 du présent arrêt, il y a lieu de relever que ces données doivent, en principe, être, selon le cas, effacées ou rendues anonymes au terme des délais légaux dans lesquels doivent intervenir, conformément aux dispositions nationales transposant cette directive, leur traitement et leur stockage.

161 Toutefois, pendant ce traitement et ce stockage, peuvent se présenter des situations dans lesquelles survient la nécessité de conserver lesdites données au-delà de ces délais aux fins de l'élucidation d'infractions pénales graves ou d'atteintes à la sécurité nationale, et ce tant dans la situation où ces infractions ou ces atteintes ont déjà pu être constatées que dans celle où leur existence peut, au terme d'un examen objectif de l'ensemble des circonstances pertinentes, être raisonnablement soupçonnée.

162 À cet égard, il y a lieu de relever que la convention sur la cybercriminalité du Conseil de l'Europe du 23 novembre 2001 (série des traités européens – n° 185), laquelle a été signée par les 27 États membres et ratifiée par 25 d'entre eux, et dont l'objectif est de faciliter la lutte contre les infractions pénales commises au moyen des réseaux informatiques, prévoit, à son article 14, que les parties contractantes adoptent aux fins d'enquêtes ou de procédures pénales spécifiques certaines mesures quant aux données relatives au trafic déjà stockées, telles que la conservation rapide de ces données. En particulier, l'article 16, paragraphe 1, de cette convention stipule que les parties contractantes adoptent les mesures législatives qui se révèlent nécessaires pour permettre à leurs autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide des données relatives au trafic stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que ces données sont susceptibles de perte ou de modification.

163 Dans une situation telle que celle visée au point 161 du présent arrêt, il est loisible aux États membres, eu égard à la conciliation nécessaire des droits et des intérêts en cause visée au point 130 du présent arrêt, de prévoir, dans une législation adoptée en vertu de l'article 15, paragraphe 1, de la directive 2002/58, la possibilité, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, d'enjoindre aux fournisseurs de services de communications électroniques de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont ils disposent.

164 Dans la mesure où la finalité d'une telle conservation rapide ne correspond plus à celles pour lesquelles les données ont été collectées et conservées initialement et où tout traitement de données doit, en vertu de l'article 8, paragraphe 2, de la Charte, répondre à des fins déterminées, les États membres doivent préciser, dans leur législation, la finalité pour laquelle la conservation rapide des données peut avoir lieu. Eu égard au caractère grave de l'ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte qu'est susceptible de comporter une telle conservation, seule la lutte contre la criminalité grave et, a fortiori, la sauvegarde de la sécurité nationale sont de nature à justifier cette ingérence. En outre, afin d'assurer que l'ingérence que comporte une mesure de ce type soit limitée au strict nécessaire, il convient, d'une part, que l'obligation de conservation porte sur les seules données de trafic et données de localisation susceptibles de contribuer à l'élucidation de l'infraction pénale grave ou de l'atteinte à la sécurité nationale concernée. D'autre part, la durée de conservation des données doit être limitée au strict nécessaire, celle-ci pouvant néanmoins être prolongée lorsque les circonstances et l'objectif poursuivi par ladite mesure le justifient.

165 À cet égard, il importe de préciser qu'une telle conservation rapide ne doit pas être limitée aux données des personnes concrètement soupçonnées d'avoir commis une infraction pénale ou une atteinte à la sécurité nationale. Tout en respectant le cadre dressé par 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, et compte tenu des considérations figurant au point 133 du présent arrêt, une telle mesure peut, selon le choix du législateur et tout en respectant les limites du strict nécessaire, être étendue aux données relatives au trafic et aux données de localisation afférentes à des personnes autres que celles qui sont soupçonnées d'avoir projeté ou commis une infraction pénale grave ou une atteinte à la sécurité nationale, pour autant que ces données peuvent, sur la base d'éléments objectifs et non discriminatoires, contribuer à l'élucidation d'une telle infraction ou d'une telle atteinte à la sécurité nationale, telles que les données de la victime de celle-ci, de son entourage social ou professionnel, ou encore de zones géographiques déterminées, telles que les lieux de la commission et de la préparation de l'infraction ou de l'atteinte à la sécurité nationale en cause. En outre, l'accès des autorités compétentes aux données ainsi conservées doit s'effectuer dans le respect des conditions résultant de la jurisprudence ayant interprété la directive 2002/58 (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, points 118 à 121 et jurisprudence citée).

166 Il convient encore d'ajouter que, ainsi qu'il ressort en particulier des points 115 et 133 du présent arrêt, l'accès à des données de trafic et à des données de localisation conservées par des fournisseurs en application d'une mesure prise au titre de l'article 15, paragraphe 1, de la directive 2002/58 ne peut en principe être justifié que par l'objectif d'intérêt général pour lequel cette conservation a été imposée à ces fournisseurs. Il s'ensuit, en particulier, qu'un accès à de telles données à des fins de poursuite et de sanction d'une infraction pénale ordinaire ne saurait en aucun cas être accordé lorsque leur conservation a été justifiée par l'objectif de lutte contre la criminalité grave ou, a fortiori, de sauvegarde de la sécurité nationale. En revanche, conformément au principe de proportionnalité tel qu'il a été précisé au point 131 du présent arrêt, un accès à des données conservées en vue de la lutte contre la criminalité grave peut, pour autant que soient respectées les conditions matérielles et procédurales entourant un tel accès visées au point précédent, être justifié par l'objectif de sauvegarde de la sécurité nationale.

167 À cet égard, il est loisible aux États membres de prévoir dans leur législation qu'un accès à des données relatives au trafic et à des données de localisation peut, dans le respect de ces mêmes conditions matérielles et procédurales, avoir lieu à des fins de lutte contre la criminalité grave ou de sauvegarde de la sécurité nationale lorsque lesdites données sont conservées par un fournisseur d'une manière conforme aux articles 5, 6 et 9 ou encore à l'article 15, paragraphe 1, de la directive 2002/58.

168 Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de répondre aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18 que 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, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, ledit article 15, paragraphe 1, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, ne s'oppose pas à des mesures législatives

– permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;

– prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et

– permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, au moyen d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services,

dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

Sur les deuxième et troisième questions dans l'affaire C-511/18

169 Par les deuxième et troisième questions dans l'affaire C-511/18, la juridiction de renvoi demande, en substance, si l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs de services de communications électroniques la mise en œuvre sur leurs réseaux de mesures permettant, d'une part, l'analyse automatisée ainsi que le recueil en temps réel des données relatives au trafic et des données de localisation et, d'autre part, le recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, sans que soit prévue l'information des personnes concernées par ces traitements et ces recueils.

170 La juridiction de renvoi précise que les techniques de recueil de renseignement prévues aux articles L. 851-2 à L. 851-4 du CSI n'impliquent pas, pour les fournisseurs de services de communications électroniques, une exigence spécifique de conservation des données relatives au trafic et des données de localisation. S'agissant, en particulier, de l'analyse automatisée visée à l'article L. 851-3 du CSI, cette juridiction relève que ce traitement a pour objet de détecter, en fonction de critères définis à cette fin, des connexions susceptibles de révéler une menace terroriste. Quant au recueil en temps réel visé à l'article L. 851-2 du CSI, ladite juridiction constate qu'il ne concerne qu'une ou plusieurs personnes préalablement identifiées comme étant susceptibles d'être en lien avec une menace terroriste. Selon la même juridiction, ces deux techniques ne peuvent être mises en œuvre qu'en vue de la prévention du terrorisme et portent sur les données visées aux articles L. 851-1 et R. 851-5 du CSI.

171 À titre liminaire, il convient de préciser que la circonstance que, selon l'article L. 851-3 du CSI, l'analyse automatisée qu'il prévoit ne permet pas, en tant que telle, l'identification des utilisateurs dont les données sont soumises à cette analyse ne fait pas obstacle à la qualification de telles données en

tant que « données à caractère personnel ». En effet, dès lors que la procédure prévue au point IV de cette même disposition permet, à un stade ultérieur, l'identification de la ou des personnes concernées par des données dont l'analyse automatisée a révélé qu'elles étaient susceptibles de caractériser l'existence d'une menace terroriste, toutes les personnes dont les données font l'objet de l'analyse automatisée demeurent identifiables à partir de ces données. Or, selon la définition des données à caractère personnel contenue à l'article 4, point 1, du règlement 2016/679, constituent de telles données les informations se rapportant, notamment, à une personne identifiable.

Sur l'analyse automatisée des données relatives au trafic et des données de localisation

172 Il ressort de l'article L. 851-3 du CSI que l'analyse automatisée qu'il prévoit correspond, en substance, à un filtrage de la totalité des données relatives au trafic et des données de localisation conservées par les fournisseurs de services de communications électroniques, effectué par ces derniers à la demande des autorités nationales compétentes et en application des paramètres que celles-ci ont déterminés. Il s'ensuit que les données des utilisateurs des moyens de communications électroniques sont toutes vérifiées si elles correspondent à ces paramètres. Dès lors, une telle analyse automatisée doit être considérée comme impliquant, pour les fournisseurs de services de communications électroniques concernés, de pratiquer, pour le compte de l'autorité compétente, un traitement généralisé et indifférencié, prenant la forme d'une utilisation à l'aide d'un procédé automatisé, au sens de l'article 4, point 2, du règlement 2016/679, couvrant l'ensemble des données relatives au trafic et des données de localisation de tous les utilisateurs de moyens de communications électroniques. Ce traitement est indépendant du recueil subséquent des données afférentes aux personnes identifiées à la suite de l'analyse automatisée, recueil qui est autorisé sur le fondement de l'article L. 851-3, IV, du CSI.

173 Or, une réglementation nationale qui autorise une telle analyse automatisée des données relatives au trafic et des données de localisation déroge à l'obligation de principe, posée à l'article 5 de la directive 2002/58, de garantir la confidentialité des communications électroniques et des données y afférentes. Une telle réglementation est également constitutive d'une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, quelle que soit l'utilisation ultérieure qui est faite de ces données. Enfin, ladite réglementation est, conformément à la jurisprudence citée au point 118 du présent arrêt, susceptible d'entraîner des effets dissuasifs sur l'exercice de la liberté d'expression consacrée à l'article 11 de la Charte.

174 En outre, l'ingérence résultant d'une analyse automatisée des données relatives au trafic et des données de localisation, telle que celle en cause au principal, s'avère particulièrement grave dès lors qu'elle couvre de manière généralisée et indifférenciée les données des personnes faisant usage des moyens de communications électroniques. Ce constat s'impose d'autant plus lorsque, ainsi qu'il ressort de la réglementation nationale en cause au principal, les données faisant l'objet de l'analyse automatisée sont susceptibles de révéler la nature des informations consultées en ligne. Au surplus, une telle analyse automatisée s'applique de manière globale à l'ensemble des personnes faisant usage des moyens de communications électroniques et, par suite, également à celles pour lesquelles il n'existe aucun indice de nature à laisser croire que leur comportement pourrait avoir un lien, même indirect ou lointain, avec des activités de terrorisme.

175 S'agissant de la justification d'une telle ingérence, il convient de préciser que l'exigence, posée à l'article 52, paragraphe 1, de la Charte, selon laquelle toute limitation de l'exercice des droits fondamentaux doit être prévue par la loi implique que la base légale qui permet celle-ci doit définir elle-même la portée de la limitation de l'exercice du droit concerné (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 175 ainsi que jurisprudence citée).

176 En outre, pour satisfaire à l'exigence de proportionnalité rappelée aux points 130 et 131 du présent arrêt, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celle-ci doivent s'opérer dans les limites du strict nécessaire, une réglementation nationale régissant l'accès des autorités compétentes à des données relatives au trafic et à des données de localisation conservées doit respecter les exigences résultant de la jurisprudence citée au point 132 du présent arrêt. En particulier, une telle réglementation ne saurait se limiter à exiger que l'accès des autorités aux données réponde à la finalité poursuivie par cette réglementation, mais elle doit également prévoir les conditions matérielles et procédurales régissant cette utilisation [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 192 et jurisprudence citée].

177 À cet égard, il y a lieu de rappeler que l'ingérence particulièrement grave que comporte une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, visée par les considérations figurant aux points 134 à 139 du présent arrêt, ainsi que l'ingérence particulièrement grave que constitue leur analyse automatisée ne peuvent satisfaire à l'exigence de proportionnalité que dans des situations dans lesquelles un État membre se trouve face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, et à la condition que la durée de cette conservation soit limitée au strict nécessaire.

178 Dans des situations telles que celles visées au point précédent, la mise en œuvre d'une analyse automatisée des données relatives au trafic et des données de localisation de l'ensemble des utilisateurs de moyens de communications électroniques, pendant une période strictement limitée, peut être considérée comme étant justifiée au regard des exigences découlant de 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.

179 Cela étant, afin de garantir que le recours à une telle mesure se limite effectivement à ce qui est strictement nécessaire à la protection de la sécurité nationale, et plus particulièrement à la prévention du terrorisme, il est essentiel, conformément à ce qui a été constaté au point 139 du présent arrêt, que la décision autorisant l'analyse automatisée puisse faire l'objet d'un contrôle effectif soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une situation justifiant ladite mesure ainsi que le respect des conditions et des garanties devant être prévues.

180 À cet égard, il convient de préciser que les modèles et les critères préétablis sur lesquels se fonde ce type de traitement de données doivent être, d'une part, spécifiques et fiables, permettant d'aboutir à des résultats identifiant des individus à l'égard desquels pourrait peser un soupçon raisonnable de participation à des infractions terroristes et, d'autre part, non discriminatoires [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 172].

181 En outre, il importe de rappeler que toute analyse automatisée effectuée en fonction de modèles et de critères fondés sur le postulat selon lequel l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, l'état de santé ou la vie sexuelle d'une personne pourraient, par eux-mêmes et indépendamment du comportement individuel de cette personne, être pertinents au regard de la prévention du terrorisme méconnaîtrait les droits garantis aux articles 7 et 8 de la Charte, lus en combinaison avec l'article 21 de celle-ci. Ainsi, les modèles et les critères préétablis aux fins d'une analyse automatisée visant à prévenir des activités de terrorisme présentant une menace grave pour la sécurité nationale ne sauraient être fondés sur ces seules données sensibles [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, point 165].

182 Par ailleurs, les analyses automatisées des données relatives au trafic et des données de localisation comportant nécessairement un certain taux d'erreur, tout résultat positif obtenu à la suite d'un traitement automatisé doit être soumis à un réexamen individuel par des moyens non automatisés avant l'adoption d'une mesure individuelle produisant des effets préjudiciables à l'égard des personnes

concernées, tel le recueil subséquent des données relatives au trafic et des données de localisation en temps réel, une telle mesure ne pouvant en effet être fondée de manière décisive sur le seul résultat d'un traitement automatisé. De même, aux fins de garantir, en pratique, que les modèles et les critères préétablis, l'usage qui en est fait ainsi que les bases de données utilisées ne présentent pas un caractère discriminatoire et soient limités au strict nécessaire au regard de l'objectif de prévenir des activités de terrorisme présentant une menace grave pour la sécurité nationale, la fiabilité et l'actualité de ces modèles et de ces critères préétablis ainsi que des bases de données utilisées doivent faire l'objet d'un réexamen régulier [voir, en ce sens, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 173 et 174]

Sur le recueil en temps réel des données relatives au trafic et des données de localisation

183 S'agissant du recueil en temps réel des données relatives au trafic et des données de localisation visé à l'article L. 851-2 du CSI, il y a lieu de relever que celui-ci peut être individuellement autorisé en ce qui concerne « une personne préalablement identifiée susceptible d'être en lien avec une menace [terroriste] ». De même, selon cette disposition, « lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations au titre de la finalité qui motive l'autorisation, celle-ci peut être également accordée individuellement pour chacune de ces personnes ».

184 Les données faisant l'objet d'une mesure de cette nature permettent aux autorités nationales compétentes de surveiller, pendant la durée de l'autorisation, de manière continue et en temps réel, les interlocuteurs avec lesquels les personnes concernées communiquent, les moyens qu'elles utilisent, la durée des communications qu'elles passent, ainsi que leurs lieux de séjours et leurs déplacements. De même, elles semblent susceptibles de révéler la nature des informations consultées en ligne. Prises dans leur ensemble, ces données permettent, ainsi qu'il ressort du 117 point du présent arrêt, de tirer des conclusions très précises concernant la vie privée des personnes concernées et fournissent les moyens d'établir le profil de celles-ci, une telle information étant tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications.

185 Quant au recueil de données en temps réel visé à l'article L. 851-4 du CSI, cette disposition autorise le recueil des données techniques relatives à la localisation des équipements terminaux et la transmission en temps réel à un service du Premier ministre. Il apparaît que de telles données permettent au service compétent, à tout moment pendant la durée de l'autorisation, de localiser, de manière continue et en temps réel, des équipements terminaux utilisés, tels des téléphones mobiles.

186 Or, une réglementation nationale autorisant de tels recueils en temps réel déroge, à l'instar de celle qui autorise l'analyse automatisée des données, à l'obligation de principe, posée à l'article 5 de la directive 2002/58, de garantir la confidentialité des communications électroniques et des données y afférentes. Elle est dès lors également constitutive d'une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte et est susceptible d'entraîner des effets dissuasifs sur l'exercice de la liberté d'expression garantie à l'article 11 de la Charte.

187 Il y a lieu de souligner que l'ingérence que comporte le recueil en temps réel des données permettant de localiser un équipement terminal apparaît particulièrement grave, dès lors que ces données fournissent aux autorités nationales compétentes le moyen d'un suivi précis et permanent des déplacements des utilisateurs des téléphones mobiles. Dans la mesure où ces données doivent ainsi être considérées comme étant particulièrement sensibles, l'accès en temps réel des autorités compétentes à de telles données doit être distingué d'un accès en temps différé à celles-ci, le premier étant davantage intrusif en ce qu'il permet une surveillance quasiment parfaite de ces utilisateurs (voir, par analogie, en ce qui concerne l'article 8 de la CEDH, Cour EDH, 8 février 2018, Ben Faiza c.

France, CE:ECHR:2018:0208JUD003144612, § 74). L'intensité de cette ingérence est en outre aggravée lorsque le recueil en temps réel s'étend également aux données relatives au trafic des personnes concernées.

188 Si l'objectif de prévention du terrorisme que poursuit la réglementation nationale en cause au principal est susceptible, eu égard à son importance, de justifier l'ingérence que comporte le recueil en temps réel des données relatives au trafic et des données de localisation, une telle mesure ne saurait être mise en œuvre, compte tenu de son caractère particulièrement intrusif, qu'à l'égard des personnes pour lesquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme. Quant aux données des personnes ne relevant pas de cette catégorie, elles peuvent seulement faire l'objet d'un accès en temps différé, celui-ci ne pouvant avoir lieu, conformément à la jurisprudence de la Cour, que dans des situations particulières, telles que celles dans lesquelles sont en cause des activités de terrorisme, et lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre le terrorisme (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 119 et jurisprudence citée).

189 En outre, une décision autorisant le recueil en temps réel des données relatives au trafic et des données de localisation doit être fondée sur des critères objectifs prévus dans la législation nationale. En particulier, cette législation doit définir, conformément à la jurisprudence citée au point 176 du présent arrêt, les circonstances et les conditions dans lesquelles un tel recueil peut être autorisé et prévoir que, ainsi qu'il a été précisé au point précédent, seules peuvent être concernées les personnes présentant un lien avec l'objectif de prévention du terrorisme. En outre, une décision autorisant le recueil en temps réel des données relatives au trafic et des données de localisation doit être fondée sur des critères objectifs et non discriminatoires prévus dans la législation nationale. Aux fins de garantir, en pratique, le respect de ces conditions, il est essentiel que la mise en œuvre de la mesure autorisant le recueil en temps réel soit soumise à un contrôle préalable effectué soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, cette juridiction ou cette entité devant notamment s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire (voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 120). En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais.

Sur l'information des personnes dont les données ont été recueillies ou analysées

190 Il importe que les autorités nationales compétentes procédant au recueil en temps réel des données relatives au trafic et des données de localisation en informent les personnes concernées, dans le cadre des procédures nationales applicables, pour autant que et dès le moment où cette communication n'est pas susceptible de compromettre les missions qui incombent à ces autorités. En effet, cette information est, de fait, nécessaire pour permettre à ces personnes d'exercer leurs droits, découlant des articles 7 et 8 de la Charte, de demander l'accès à leurs données à caractère personnel faisant l'objet de ces mesures et, le cas échéant, la rectification ou la suppression de celles-ci, ainsi que d'introduire, conformément à l'article 47, premier alinéa, de la Charte, un recours effectif devant un tribunal, un tel droit étant d'ailleurs explicitement garanti à l'article 15, paragraphe 2, de la directive 2002/58, lu en combinaison avec l'article 79, paragraphe 1, du règlement 2016/679 [voir, en ce sens, arrêt du 21 décembre 2016, Tele2, C-203/15 et C-698/15, EU:C:2016:970, point 121 et jurisprudence citée, ainsi que avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 219 et 220].

191 S'agissant de l'information requise dans le contexte d'une analyse automatisée des données relatives au trafic et des données de localisation, l'autorité nationale compétente est tenue de publier des renseignements de nature générale relatifs à cette analyse, sans devoir procéder à une information individuelle des personnes concernées. En revanche, dans l'hypothèse où les données répondent aux paramètres précisés dans la mesure autorisant l'analyse automatisée et où cette autorité procède à

l'identification de la personne concernée aux fins d'analyser plus en profondeur les données la concernant, l'information individuelle de cette personne s'avère nécessaire. Une telle information ne doit toutefois intervenir que pour autant que et qu'à partir du moment où elle n'est pas susceptible de compromettre les missions incombant à ladite autorité [voir, par analogie, avis 1/15 (Accord PNR UE-Canada), du 26 juillet 2017, EU:C:2017:592, points 222 à 224].

192 Eu égard à l'ensemble des considérations qui précèdent, il y a lieu de répondre aux deuxième et troisième questions dans l'affaire C-511/18 que 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, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée ainsi qu'au recueil en temps réel, notamment, des données relatives au trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, lorsque

– le recours à l'analyse automatisée est limité à des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le recours à cette analyse pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une situation justifiant ladite mesure ainsi que le respect des conditions et des garanties devant être prévues, et que

– le recours à un recueil en temps réel des données relatives au trafic et des données de localisation est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme et est soumis à un contrôle préalable, effectué, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais.

Sur la seconde question dans l'affaire C-512/18

193 Par la seconde question dans l'affaire C-512/18, la juridiction de renvoi cherche, en substance, à savoir si les dispositions de la directive 2000/31, lues à la lumière des articles 6 à 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doivent être interprétées en ce sens qu'elles s'opposent à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.

194 Tout en considérant que de tels services relèvent du champ d'application de la directive 2000/31, et non de celui de la directive 2002/58, la juridiction de renvoi est d'avis que l'article 15, paragraphes 1 et 2, de la directive 2000/31, lu en combinaison avec les articles 12 et 14 de celle-ci, n'instaure pas, par lui-même, une interdiction de principe de conserver des données relatives à la création de contenu à laquelle il pourrait seulement être dérogé de manière exceptionnelle. Cette juridiction se demande néanmoins si cette appréciation doit être retenue, compte tenu du respect nécessaire des droits fondamentaux consacrés aux articles 6 à 8 et 11 de la Charte.

195 En outre, la juridiction de renvoi précise que sa question vise l'obligation de conservation prévue à l'article 6 de la LCEN, lu en combinaison avec le décret nº 2011-219. Les données que doivent conserver les fournisseurs de services concernés à ce titre incluent, notamment, les données relatives à l'identité civile des personnes ayant fait usage de ces services, tels que leurs nom, prénom, leurs

adresses postales associées, leurs adresses de courrier électronique ou de compte associées, leurs mots de passe et, lorsque la souscription du contrat ou du compte est payante, le type de paiement utilisé, la référence du paiement, le montant ainsi que la date et l'heure de la transaction.

196 De même, les données visées par l'obligation de conservation couvrent les identifiants des abonnés, des connexions et des équipements terminaux utilisés, les identifiants attribués aux contenus, les dates et heures de début et de fin des connexions et des opérations ainsi que les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus. L'accès à ces données, dont la durée de conservation s'élève à un an, peut être sollicité dans le cadre des procédures pénales et civiles, en vue de faire respecter les règles relatives à la responsabilité civile ou pénale, ainsi que dans le cadre de mesures de recueil de renseignement auxquelles l'article L. 851-1 du CSI s'applique.

197 À cet égard, il y a lieu de relever que, conformément à son article 1er, paragraphe 2, la directive 2000/31 rapproche certaines dispositions nationales applicables aux services de la société de l'information visés à son article 2, sous a).

198 De tels services englobent, certes, ceux qui sont fournis à distance au moyen d'équipements électroniques de traitement et de stockage de données, à la demande individuelle d'un destinataire de services et, normalement, contre rémunération, tels que des services d'accès à Internet ou à un réseau de communication ainsi que des services d'hébergement (voir, en ce sens, arrêts du 24 novembre 2011, Scarlet Extended, C-70/10, EU:C:2011:771, point 40 ; du 16 février 2012, SABAM, C-360/10, EU:C:2012:85, point 34 ; du 15 septembre 2016, Mc Fadden, C-484/14, EU:C:2016:689, point 55, ainsi que du 7 août 2018, SNB-REACT, C-521/17, EU:C:2018:639, point 42 et jurisprudence citée).

199 Toutefois, l'article 1er, paragraphe 5, de la directive 2000/31 dispose que celle-ci n'est pas applicable aux questions relatives aux services de la société de l'information qui sont couvertes par les directives 95/46 et 97/66. À cet égard, il ressort des considérants 14 et 15 de la directive 2000/31 que la protection de la confidentialité des communications ainsi que des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information est uniquement régie par les directives 95/46 et 97/66, cette dernière interdisant, à son article 5, aux fins de la protection de la confidentialité des communications, toute forme d'interception ou de surveillance des communications.

200 Ainsi, des questions liées à la protection de la confidentialité des communications et des données à caractère personnel doivent être appréciées à l'aune de la directive 2002/58 et du règlement 2016/679, ceux-ci ayant remplacé respectivement la directive 97/66 et la directive 95/46, étant précisé que la protection que vise à assurer la directive 2000/31 ne peut en tout état de cause pas porter atteinte aux exigences résultant de la directive 2002/58 et du règlement 2016/679 (voir, en ce sens, arrêt du 29 janvier 2008, Promusicae, C-275/06, EU:C:2008:54, point 57).

201 L'obligation imposée par la réglementation nationale visée au point 195 du présent arrêt aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement de conserver des données à caractère personnel afférentes à ces services doit donc, comme l'a relevé en substance M. l'avocat général au point 141 de ses conclusions dans les affaires jointes La Quadrature du Net e.a. (C-511/18 et C-512/18, EU:C:2020:6), être appréciée à l'aune de la directive 2002/58 ou du règlement 2016/679.

202 Ainsi, selon que la fourniture des services couverts par cette réglementation nationale relève ou non de la directive 2002/58, elle sera régie soit par cette dernière directive, en particulier par l'article 15, paragraphe 1, de celle-ci, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, soit par le règlement 2016/679, en particulier par l'article 23, paragraphe 1, dudit règlement, lu à la lumière des mêmes dispositions de la Charte.

203 En l'occurrence, il ne saurait être exclu, comme l'a relevé la Commission européenne dans ses observations écrites, que certains des services auxquels s'applique la réglementation nationale visée au point 195 du présent arrêt constituent des services de communications électroniques, au sens de la directive 2002/58, ce qu'il appartient à la juridiction de renvoi de vérifier.

204 À cet égard, il convient de relever que la directive 2002/58 couvre les services de communications électroniques qui remplissent les conditions énoncées à l'article 2, sous c), de la directive 2002/21, auquel renvoie l'article 2 de la directive 2002/58 et qui définit le service de communications électroniques comme étant « le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques, y compris les services de télécommunications et les services de transmission sur les réseaux utilisés pour la radiodiffusion ». S'agissant des services de la société de l'information, tels que visés aux points 197 et 198 du présent arrêt et couverts par la directive 2000/31, ceux-ci constituent des services de communications électroniques dès lors qu'ils consistent entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques (voir, en ce sens, arrêt du 5 juin 2019, Skype Communications, C-142/18, EU:C:2019:460, points 47 et 48).

205 Ainsi, les services d'accès à Internet, lesquels paraissent être couverts par la réglementation nationale visée au point 195 du présent arrêt, constituent, comme le confirme le considérant 10 de la directive 2002/21, des services de communications électroniques, au sens de cette directive (voir, en ce sens, arrêt du 5 juin 2019, Skype Communications, C-142/18, EU:C:2019:460, point 37). Tel est également le cas des services de messageries sur Internet, dont il ne semble pas exclu qu'ils relèvent également de cette réglementation nationale, dès lors que, sur le plan technique, ils impliquent entièrement ou principalement la transmission de signaux sur des réseaux de communications électroniques (voir, en ce sens, arrêt du 13 juin 2019, Google, C-193/18, EU:C:2019:498, points 35 et 38).

206 S'agissant des exigences découlant de 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, il convient de renvoyer à l'ensemble des constatations et des appréciations faites dans le cadre de la réponse apportée aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18.

207 Quant aux exigences découlant du règlement 2016/679, il convient de rappeler que celui-ci vise, notamment, ainsi qu'il ressort de son considérant 10, à assurer un niveau élevé de protection des personnes physiques au sein de l'Union et, à cette fin, à assurer une application cohérente et homogène des règles de protection des libertés et des droits fondamentaux de ces personnes à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union (voir, en ce sens, arrêt du 16 juillet 2020, Facebook Ireland et Schrems, C-311/18, EU:C:2020:559, point 101).

208 À cette fin, tout traitement de données à caractère personnel doit, sous réserve des dérogations admises à l'article 23 du règlement 2016/679, respecter les principes régissant les traitements des données à caractère personnel ainsi que les droits de la personne concernée énoncés respectivement dans les chapitres II et III de ce règlement. En particulier, tout traitement de données à caractère personnel doit, d'une part, être conforme aux principes énoncés à l'article 5 dudit règlement et, d'autre part, satisfaire aux conditions de licéité énumérées à l'article 6 de ce même règlement (voir, par analogie, en ce qui concerne la directive 95/46, arrêt du 30 mai 2013, Worten, C-342/12, EU:C:2013:355, point 33 et jurisprudence citée).

209 Pour ce qui est, plus particulièrement, de l'article 23, paragraphe 1, du règlement 2016/679, il y a lieu de relever que celui-ci, à l'instar de ce qui est prévu à l'article 15, paragraphe 1, de la directive 2002/58, permet aux États membres de limiter, au regard des finalités qu'il prévoit et au moyen de mesures législatives, la portée des obligations et des droits qui y sont visés « lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et

proportionnée dans une société démocratique pour garantir » la finalité poursuivie. Toute mesure législative prise sur ce fondement doit, en particulier, respecter les exigences spécifiques posées à l'article 23, paragraphe 2, de ce règlement.

210 Ainsi, l'article 23, paragraphes 1 et 2, du règlement 2016/679 ne saurait être interprété comme pouvant conférer aux États membres le pouvoir de porter atteinte au respect de la vie privée, en méconnaissance de l'article 7 de la Charte, tout comme aux autres garanties prévues par celle-ci (voir, par analogie, en ce qui concerne la directive 95/46, arrêt du 20 mai 2003, Österreichischer Rundfunk e.a., C-465/00, C-138/01 et C-139/01, EU:C:2003:294, point 91). En particulier, à l'instar de ce qui vaut pour l'article 15, paragraphe 1, de la directive 2002/58, le pouvoir que confère l'article 23, paragraphe 1, du règlement 2016/679 aux États membres ne saurait être exercé que dans le respect de l'exigence de proportionnalité, selon laquelle les dérogations à la protection des données à caractère personnel et les limitations de celles-ci doivent s'opérer dans les limites du strict nécessaire (voir, par analogie, s'agissant de la directive 95/46, arrêt du 7 novembre 2013, IPI, C-473/12, EU:C:2013:715, point 39 et jurisprudence citée).

211 Il s'ensuit que les constatations et les appréciations faites dans le cadre de la réponse apportée aux premières questions dans les affaires C-511/18 et C-512/18 ainsi qu'aux première et deuxième questions dans l'affaire C-520/18 s'appliquent mutatis mutandis à l'article 23 du règlement 2016/679.

212 Au regard des considérations qui précèdent, il convient de répondre à la seconde question dans l'affaire C-512/18 que la directive 2000/31 doit être interprétée en ce sens qu'elle n'est pas applicable en matière de protection de la confidentialité des communications et des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information, cette protection étant, selon le cas, régie par la directive 2002/58 ou par le règlement 2016/679. L'article 23, paragraphe 1, du règlement 2016/679, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.

Sur la troisième question dans l'affaire C-520/18

213 Par la troisième question dans l'affaire C-520/18, la juridiction de renvoi cherche, en substance, à savoir si une juridiction nationale peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, entre autres, de la poursuite des objectifs de sauvegarde de la sécurité nationale et de lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, résultant de son caractère incompatible avec 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.

214 Le principe de primauté du droit de l'Union consacre la prééminence du droit de l'Union sur le droit des États membres. Ce principe impose dès lors à toutes les instances des États membres de donner leur plein effet aux différentes normes de l'Union, le droit des États membres ne pouvant affecter l'effet reconnu à ces différentes normes sur le territoire desdits États [arrêts du 15 juillet 1964, Costa, 6/64, EU:C:1964:66, p. 1159 et 1160, ainsi que du 19 novembre 2019, A. K. e.a. (Indépendance de la chambre disciplinaire de la Cour suprême), C-585/18, C-624/18 et C-625/18, EU:C:2019:982, points 157 et 158 et jurisprudence citée].

215 En vertu du principe de primauté, à défaut de pouvoir procéder à une interprétation de la réglementation nationale conforme aux exigences du droit de l'Union, le juge national chargé d'appliquer, dans le cadre de sa compétence, les dispositions du droit de l'Union a l'obligation d'assurer le plein effet de celles-ci en laissant au besoin inappliquée, de sa propre autorité, toute disposition contraire de la législation nationale, même postérieure, sans qu'il ait à demander ou à attendre l'élimination préalable de celle-ci par voie législative ou par tout autre procédé constitutionnel [arrêts du 22 juin 2010, Melki et Abdeli, C-188/10 et C-189/10, EU:C:2010:363, point 43 et jurisprudence citée ; du 24 juin 2019, Popławski, C-573/17, EU:C:2019:530, point 58, ainsi que du 19 novembre 2019, A. K. e.a. (Indépendance de la chambre disciplinaire de la Cour suprême), C-585/18, C-624/18 et C-625/18, EU:C:2019:982, point 160].

216 Seule la Cour peut, à titre exceptionnel et pour des considérations impérieuses de sécurité juridique, accorder une suspension provisoire de l'effet d'éviction exercé par une règle du droit de l'Union à l'égard du droit national contraire à celle-ci. Une telle limitation dans le temps des effets de l'interprétation de ce droit donnée par la Cour ne peut être accordée que dans l'arrêt même qui statue sur l'interprétation sollicitée [voir, en ce sens, arrêts du 23 octobre 2012, Nelson e.a., C-581/10 et C-629/10, EU:C:2012:657, points 89 et 91 ; du 23 avril 2020, Herst, C-401/18, EU:C:2020:295, points 56 et 57, ainsi que du 25 juin 2020, A e.a. (Éoliennes à Aalter et à Nevele), C-24/19, EU:C:2020:503, point 84 et jurisprudence citée].

217 Il serait porté atteinte à la primauté et à l'application uniforme du droit de l'Union si des juridictions nationales avaient le pouvoir de donner aux dispositions nationales la primauté par rapport au droit de l'Union auquel ces dispositions contreviennent, serait-ce même à titre provisoire (voir, en ce sens, arrêt du 29 juillet 2019, Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, point 177 ainsi que jurisprudence citée).

218 Toutefois, la Cour a jugé, dans une affaire où était en cause la légalité de mesures adoptées en méconnaissance de l'obligation édictée par le droit de l'Union d'effectuer une évaluation préalable des incidences d'un projet sur l'environnement et sur un site protégé, qu'une juridiction nationale peut, si le droit interne le permet, exceptionnellement maintenir les effets de telles mesures lorsque ce maintien est justifié par des considérations impérieuses liées à la nécessité d'écarter une menace réelle et grave de rupture de l'approvisionnement en électricité de l'État membre concerné, à laquelle il ne pourrait être fait face par d'autres moyens et alternatives, notamment dans le cadre du marché intérieur, ledit maintien ne pouvant couvrir que le laps de temps strictement nécessaire pour remédier à cette illégalité (voir, en ce sens, arrêt du 29 juillet 2019, Inter-Environnement Wallonie et Bond Beter Leefmilieu Vlaanderen, C-411/17, EU:C:2019:622, points 175, 176, 179 et 181).

219 Or, contrairement à l'omission d'une obligation procédurale telle que l'évaluation préalable des incidences d'un projet dans le domaine spécifique de la protection de l'environnement, une méconnaissance de 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, ne saurait faire l'objet d'une régularisation par voie d'une procédure comparable à celle mentionnée au point précédent. En effet, le maintien des effets d'une législation nationale, telle que celle en cause au principal, signifierait que cette législation continue à imposer aux fournisseurs de services de communications électroniques des obligations qui sont contraires au droit de l'Union et qui comportent des ingérences graves dans les droits fondamentaux des personnes dont les données ont été conservées.

220 Partant, la juridiction de renvoi ne saurait faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, de la législation nationale en cause au principal.

221 Cela étant, dans leurs observations soumises à la Cour, VZ, WY et XX font valoir que la troisième question soulève, implicitement mais nécessairement, le point de savoir si le droit de l'Union s'oppose à une exploitation, dans le cadre d'une procédure pénale, des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec ce droit.

222 À cet égard et afin de donner une réponse utile à la juridiction de renvoi, il y a lieu de rappeler que, en l'état actuel du droit de l'Union, il appartient, en principe, au seul droit national de déterminer les règles relatives à l'admissibilité et à l'appréciation, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité grave, d'informations et d'éléments de preuve qui ont été obtenus par une telle conservation de données contraire au droit de l'Union.

223 En effet, il est de jurisprudence constante que, en l'absence de règles de l'Union en la matière, il appartient à l'ordre juridique interne de chaque État membre, en vertu du principe d'autonomie procédurale, de régler les modalités procédurales des recours en justice destinés à assurer la sauvegarde des droits que les justiciables tirent du droit de l'Union, à condition toutefois qu'elles ne soient pas moins favorables que celles régissant des situations similaires soumises au droit interne (principe d'équivalence) et qu'elles ne rendent pas impossible en pratique ou excessivement difficile l'exercice des droits conférés par le droit de l'Union (principe d'effectivité) (voir, en ce sens, arrêts du 6 octobre 2015, Târşia, C-69/14, EU:C:2015:662, points 26 et 27 ; du 24 octobre 2018, XC e.a., C-234/17, EU:C:2018:853, points 21 et 22 ainsi que jurisprudence citée, et du 19 décembre 2019, Deutsche Umwelthilfe, C-752/18, EU:C:2019:1114, point 33).

224 En ce qui concerne le principe d'équivalence, il appartient au juge national saisi d'une procédure pénale fondée sur des informations ou des éléments de preuve obtenus en méconnaissance des exigences résultant de la directive 2002/58 de vérifier si le droit national régissant cette procédure prévoit des règles moins favorables en ce qui concerne l'admissibilité et l'exploitation de telles informations et de tels éléments de preuve que celles régissant les informations et les éléments de preuve obtenus en violation du droit interne.

225 Quant au principe d'effectivité, il convient de relever que les règles nationales relatives à l'admissibilité et à l'exploitation des informations et des éléments de preuve ont pour objectif, en vertu des choix opérés par le droit national, d'éviter que des informations et des éléments de preuve qui ont été obtenus de manière illégale portent indûment préjudice à une personne soupçonnée d'avoir commis des infractions pénales. Or, cet objectif peut, selon le droit national, être atteint non seulement par une interdiction d'exploiter de telles informations et de tels éléments de preuve, mais également par des règles et des pratiques nationales régissant l'appréciation et la pondération des informations et des éléments de preuve, voire par une prise en considération de leur caractère illégal dans le cadre de la détermination de la peine.

226 Cela étant, il ressort de la jurisprudence de la Cour que la nécessité d'exclure des informations et des éléments de preuve obtenus en méconnaissance des prescriptions du droit de l'Union doit être appréciée au regard, notamment, du risque que l'admissibilité de tels informations et éléments de preuve comporte pour le respect du principe du contradictoire et, partant, du droit à un procès équitable (voir, en ce sens, arrêt du 10 avril 2003, Steffensen, C-276/01, EU:C:2003:228, points 76 et 77). Or, une juridiction qui considère qu'une partie n'est pas en mesure de commenter efficacement un moyen de preuve qui ressortit à un domaine échappant à la connaissance des juges et qui est susceptible d'influencer de manière prépondérante l'appréciation des faits doit constater une violation du droit à un procès équitable et exclure ce moyen de preuve afin d'éviter une telle violation (voir, en ce sens, arrêt du 10 avril 2003, Steffensen, C-276/01, EU:C:2003:228, points 78 et 79).

227 Partant, le principe d'effectivité impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus au moyen d'une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le

cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

228 Eu égard aux considérations qui précèdent, il y a lieu de répondre à la troisième question dans l'affaire C-520/18 qu'une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec 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. Cet article 15, paragraphe 1, interprété à la lumière du principe d'effectivité, impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.

Sur les dépens

229 La procédure revêtant, à l'égard des parties au principal, le caractère d'un incident soulevé devant les juridictions de renvoi, il appartient à celles-ci de statuer sur les dépens. Les frais exposés pour soumettre des observations à la Cour, autres que ceux desdites parties, ne peuvent faire l'objet d'un remboursement.

Par ces motifs, la Cour (grande chambre) dit pour droit :

1) **L'article 15, paragraphe 1, de la directive 2002/58/CE du Parlement européen et du Conseil, du 12 juillet 2002, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), telle que modifiée par la directive 2009/136/CE du Parlement européen et du Conseil, du 25 novembre 2009, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne, doit être interprété en ce sens qu'il s'oppose à des mesures législatives prévoyant, aux fins prévues à cet article 15, paragraphe 1, à titre préventif, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation. En revanche, l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, ne s'oppose pas à des mesures législatives**

   — **permettant, aux fins de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques de procéder à une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation, dans des situations où l'État membre concerné fait face à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, la décision prévoyant cette injonction pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une de ces situations ainsi que le respect des**

conditions et des garanties devant être prévues, et ladite injonction ne pouvant être émise que pour une période temporellement limitée au strict nécessaire, mais renouvelable en cas de persistance de cette menace ;

— **prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation ciblée des données relatives au trafic et des données de localisation qui soit délimitée, sur la base d'éléments objectifs et non discriminatoires, en fonction de catégories de personnes concernées ou au moyen d'un critère géographique, pour une période temporellement limitée au strict nécessaire, mais renouvelable ;**

— **prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité grave et de la prévention des menaces graves contre la sécurité publique, une conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion, pour une période temporellement limitée au strict nécessaire ;**

— **prévoyant, aux fins de la sauvegarde de la sécurité nationale, de la lutte contre la criminalité et de la sauvegarde de la sécurité publique, une conservation généralisée et indifférenciée des données relatives à l'identité civile des utilisateurs de moyens de communications électroniques, et**

— **permettant, aux fins de la lutte contre la criminalité grave et, a fortiori, de la sauvegarde de la sécurité nationale, le recours à une injonction faite aux fournisseurs de services de communications électroniques, par le biais d'une décision de l'autorité compétente soumise à un contrôle juridictionnel effectif, de procéder, pour une durée déterminée, à la conservation rapide des données relatives au trafic et des données de localisation dont disposent ces fournisseurs de services,**

dès lors que ces mesures assurent, par des règles claires et précises, que la conservation des données en cause est subordonnée au respect des conditions matérielles et procédurales y afférentes et que les personnes concernées disposent de garanties effectives contre les risques d'abus.

2) **L'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il ne s'oppose pas à une réglementation nationale imposant aux fournisseurs de services de communications électroniques de recourir, d'une part, à l'analyse automatisée ainsi qu'au recueil en temps réel, notamment, des données relatives au trafic et des données de localisation et, d'autre part, au recueil en temps réel des données techniques relatives à la localisation des équipements terminaux utilisés, lorsque**

— **le recours à l'analyse automatisée est limité à des situations dans lesquelles un État membre se trouve confronté à une menace grave pour la sécurité nationale qui s'avère réelle et actuelle ou prévisible, le recours à cette analyse pouvant faire l'objet d'un contrôle effectif, soit par une juridiction, soit par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, visant à vérifier l'existence d'une situation justifiant ladite mesure ainsi que le respect des conditions et des garanties devant être prévues, et que**

— **le recours à un recueil en temps réel des données relatives au trafic et des données de localisation est limité aux personnes à l'égard desquelles il existe une raison valable de soupçonner qu'elles sont impliquées d'une manière ou d'une autre dans des activités de terrorisme et est soumis à un contrôle préalable, effectué, soit par une juridiction, soit**

par une entité administrative indépendante, dont la décision est dotée d'un effet contraignant, afin de s'assurer qu'un tel recueil en temps réel n'est autorisé que dans la limite de ce qui est strictement nécessaire. En cas d'urgence dûment justifiée, le contrôle doit intervenir dans de brefs délais.

3) **La directive 2000/31/CE du Parlement européen et du Conseil, du 8 juin 2000, relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), doit être interprétée en ce sens qu'elle n'est pas applicable en matière de protection de la confidentialité des communications et des personnes physiques à l'égard du traitement des données à caractère personnel dans le cadre des services de la société de l'information, cette protection étant, selon le cas, régie par la directive 2002/58, telle que modifiée par la directive 2009/136, ou par le règlement (UE) 2016/679 du Parlement européen et du Conseil, du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46. L'article 23, paragraphe 1, du règlement 2016/679, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux, doit être interprété en ce sens qu'il s'oppose à une réglementation nationale imposant aux fournisseurs d'accès à des services de communication au public en ligne et aux fournisseurs de services d'hébergement la conservation généralisée et indifférenciée, notamment, des données à caractère personnel afférentes à ces services.**

4) **Une juridiction nationale ne peut faire application d'une disposition de son droit national qui l'habilite à limiter dans le temps les effets d'une déclaration d'illégalité lui incombant, en vertu de ce droit, à l'égard d'une législation nationale imposant aux fournisseurs de services de communications électroniques, en vue, notamment, de la sauvegarde de la sécurité nationale et de la lutte contre la criminalité, une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la charte des droits fondamentaux. Cet article 15, paragraphe 1, interprété à la lumière du principe d'effectivité, impose au juge pénal national d'écarter des informations et des éléments de preuve qui ont été obtenus par une conservation généralisée et indifférenciée des données relatives au trafic et des données de localisation incompatible avec le droit de l'Union, dans le cadre d'une procédure pénale ouverte à l'encontre de personnes soupçonnées d'actes de criminalité, si ces personnes ne sont pas en mesure de commenter efficacement ces informations et ces éléments de preuve, provenant d'un domaine échappant à la connaissance des juges et qui sont susceptibles d'influencer de manière prépondérante l'appréciation des faits.**

Signatures